HUBSOFT · SEGURANÇA DA INFORMAÇÃO

Boletim de Segurança para Provedores

Vulnerabilidades em equipamentos e sistemas de provedores

REFERÊNCIA	DESTINATÁRIO	ELABORAÇÃO
Falhas divulgadas até 24/11/2026	Responsáveis técnicos de provedores de internet	Bianca Couto, Head de Tecnologia e Produto

Material elaborado pela Hubsoft para provedores de internet. Pode ser compartilhado na íntegra, com a fonte.

Como usar este boletim

Este boletim reúne as vulnerabilidades divulgadas até 24/11/2026 nos equipamentos e sistemas mais usados por provedores de internet. Encaminhe ao responsável técnico da sua empresa (NOC, redes, infraestrutura, TI e desenvolvimento) para conferir cada versão e atualizar o que estiver defasado.

Escopo. Cobre a rede do provedor (roteadores, OLTs, rádios, equipamentos de assinante, gerência de CPE, núcleo da rede, servidores, virtualização, firewalls, datacenter, hospedagem, câmeras, telefonia e IPTV) e o que roda dentro da empresa (estações, celulares, VPN, servidores Windows e backup, site, ERP de backoffice, ferramentas internas e soluções próprias com Docker, IA e chatbots). O servidor do HubSoft não entra aqui: o sistema, o firewall e as atualizações dele são gerenciados pela Hubsoft.

Como ler a prioridade.

Prioridade	Significado	Prazo sugerido
Crítica	Já explorada, ou com código de ataque público	Imediato
Alta	Falha grave, sem exploração conhecida até a data	Próxima janela de manutenção
Atenção	Sem correção do fabricante ou fora de suporte	Mitigar e planejar a troca

Regra geral, válida para tudo que está neste boletim. A maior parte destas falhas só é explorável quando a interface de gerência do equipamento está acessível pela internet.

- Nenhuma gerência aberta para a internet: Winbox, SSH, Telnet, interface web, SNMP, API e a porta do ACS (TR-069/NBI). Acesso só por VPN ou por lista de IPs autorizados.
- Trocar todas as senhas e communities SNMP de fábrica.
- Ativar autenticação em dois fatores onde o equipamento oferecer.
- Manter um inventário de modelo e firmware dos equipamentos, para responder rápido a cada alerta.

Nas tabelas, a etiqueta **EXPLORADA** marca o que já foi usado em ataques reais e deve ser tratado primeiro. A etiqueta **SEM CORREÇÃO** marca o que depende de mitigação e isolamento.

Comece por aqui: dez itens para conferir hoje

Se o tempo for curto, comece por estes dez. São os que mais aparecem em provedores e os que mais têm sido usados em ataques.

#	O que conferir	Como resolver
1	Gerência aberta para a internet: Winbox, SSH, Telnet, interface web, SNMP, API, NBI do ACS e painel do hypervisor	Fechar. Acesso só por VPN ou lista de IPs autorizados. É o que torna explorável a maior parte das falhas deste boletim
2	MikroTik RouterOS	Atualizar para 6.49.23, 7.24.6 (long-term) ou 7.25.1 (stable). Há falhas exploradas desde setembro (seção 2)
3	Servidores Linux com nginx e PHP	nginx 1.30.8 ou 1.31.10; PHP 8.2.36, 8.3.37, 8.4.28 ou 8.5.13; kernel atualizado, com reinício (seção 8)
4	OLTs, em especial a V-SOL série 1600	Gerência isolada da internet e da rede dos assinantes; trocar a senha do admin e as communities SNMP. A V-SOL tem falha sem correção (seção 3)
5	Ubiquiti	UniFi OS 5.1.31 e airMAX M 6.3.26 ou superiores; console nunca exposto direto à internet (seção 4)
6	ACS e equipamentos de assinante	No GenieACS, porta da NBI liberada só para os sistemas que integram. Firmware dos equipamentos atualizado pelo ACS e gerência pela WAN bloqueada (seções 5 e 6)
7	Virtualização: VMware e Proxmox	Painel só por VPN, com 2FA. vCenter com o patch de 19/11/2026 e ESXi com os patches de 2026; Proxmox VE 7 e 8 com migração para o 9 (seção 9)
8	Firewall de borda e VPN: Fortinet, SonicWall, Ivanti, NetScaler, Check Point, pfSense	Conferir a versão mínima de cada um, que mudou em outubro e novembro, e exigir 2FA em todo acesso (seções 13 e 14)
9	Computadores da equipe	Chrome 157.0.8103.50 ou superior, atualização de novembro do Windows e do Office, e ninguém com perfil de administrador no uso diário (seção 15)
10	Soluções próprias e site: n8n, chatbots, Docker, WordPress	Nenhum painel aberto para a internet, versões corrigidas e porta 2375 do Docker fechada (seções 18 e 21)

Antes de qualquer atualização: backup da configuração e janela de manutenção. E, sempre, backup testado e guardado fora do servidor de origem.

Material elaborado pela Hubsoft para provedores de internet. Pode ser compartilhado na íntegra, com a fonte.

Sumário

Parte 1 · O que já está sendo explorado **4**
1. Resumo: o que conferir primeiro 4
Parte 2 · Rede do provedor **8**
2. Roteadores e concentradores 8
MikroTik RouterOS — prioridade crítica 8
Juniper Junos OS — prioridade alta 9
Cisco — prioridade alta, com um item crítico 10
Huawei, Nokia e ZTE 10
3. OLTs e gerência da rede óptica 11
V-SOL (V-Solution) série 1600 — prioridade crítica, sem correção 11
Huawei MA5600T / MA5800 e ZTE C300 / C350 11
Demais OLTs integradas ao HubSoft 12
4. Rádios e Wi-Fi 12
Ubiquiti UniFi (UniFi OS, Network, Protect, Talk, Access) — prioridade crítica 12
Ubiquiti airMAX, airFiber e bridges (UBB/UDB) — prioridade alta 13
Cambium Networks 14
Intelbras (APC 5A e linha de rádios) e Deliberant 14
5. CPEs, ONUs e roteadores de assinante 14
6. Gerência de CPE (ACS / TR-069) 17
7. Núcleo da rede: CGNAT, BNG, roteamento e DNS recursivo 17
Parte 3 · Servidores e datacenter **20**
8. Servidores e serviços do provedor 20
Servidor web e linguagem 20
Sistema operacional 21
DNS, RADIUS, e-mail, monitoramento e telefonia 23
9. Virtualização, firewalls e switches 25
10. Datacenter e POP: gerência de servidor, storage e energia 28
11. Hospedagem, e-mail e banco de dados 29
12. Ferramentas de operação: documentação de rede, monitoramento e cofres de senha 31
Parte 4 · Borda e acesso remoto **32**
13. Outros firewalls, Wi-Fi corporativo e impressoras 32
14. Acesso remoto e VPN 33
Parte 5 · Dentro da empresa **37**
15. Estações de trabalho 37
16. Celulares e aplicativos 38
17. Servidores Windows, colaboração e backup 39
18. Site institucional, ERP de backoffice e ferramentas internas 40
19. Câmeras e telefonia IP 43
20. IPTV, TV box e equipamentos de voz 44
Parte 6 · Soluções próprias **45**
21. Soluções próprias: Docker, IA e chatbots 45
Contêineres e orquestração 45
Automação, IA e chatbots 46
Aplicações próprias e pipeline 48
Parte 7 · Sem correção, checklist e fontes **50**
22. Falhas divulgadas sem correção disponível 50
23. Checklist para o responsável técnico 52
24. Fontes e limites deste levantamento 54

Material elaborado pela Hubsoft para provedores de internet. Pode ser compartilhado na íntegra, com a fonte.

Parte 1 · O que já está sendo explorado

1. Resumo: o que conferir primeiro

Na rede e nos servidores do provedor, os itens abaixo têm exploração confirmada em ataques reais ou código de ataque público. Comece por eles.

Sistema	Falha	Situação	Ação
MikroTik RouterOS	CVE-2026-67276, 67277, 67279, 86060 (SSH, btest); CVE-2026-84411 (serviço web)	Exploração ativa desde setembro	Atualizar para 6.49.23, 7.24.6 (long-term) ou 7.25.1 (stable)
nginx	“nginx2root”: CVE-2026-123007 e mais quatro	Corrigida em 18/11; prova de conceito pública, sem exploração relatada até 24/11	Atualizar para 1.30.8 ou 1.31.10, de 23/11 (o mínimo para o nginx2root é 1.30.7 ou 1.31.9), e reiniciar o serviço
PHP	“PHP2Shell”: CVE-2026-109618 e 109619	Exploração ativa, encadeada com falha de kernel para obter root	PHP 8.2.36, 8.3.37, 8.4.28 ou 8.5.13, de 19/11 (ou superior)
Brotli	CVE-2026-111497	Exploração confirmada (CISA, 27/10)	Brotli 1.0.10, 1.1.1 ou 1.2.1; Node.js 22.23.4, 24.22.1 ou 26.12.1
Kernel Linux	Copy Fail (CVE-2026-31431), Fragnesia (CVE-2026-46300), CVE-2026-53362 e outras	Exploração ativa: usuário comum vira root	Atualizar o kernel da distribuição e reiniciar
Switches Zyxel GS1900	CVE-2026-107441 e CVE-2026-7273	Cerca de mil switches invadidos	Firmware Patch 3, de outubro/2026, ou posterior
Ubiquiti UniFi OS	CVE-2026-34908, 34909, 34910	Exploração ativa (CISA, 23/06)	UniFi OS 5.1.31 ou superior
VMware vCenter e ESXi	CVE-2026-123890 e 59310 (vCenter); CVE-2026-41709 e CVE-2025-22224, 22225, 22226 (ESXi)	Exploração ativa, com uso por ransomware	vCenter 8.0 U3m, 9.0.2.0200 ou 9.1.1.0200 (de 19/11); ESXi 8.0 U3k, 9.0.2.0100 ou 9.1.0.0200
Fortinet FortiOS	CVE-2026-24858 (login por FortiCloud SSO)	Exploração ativa desde janeiro	FortiOS 7.6.6, 7.4.11, 7.2.13 ou 7.0.19 no mínimo; para cobrir também as falhas críticas de 10/11: 8.0.2, 7.6.8, 7.4.13 ou 7.2.14; desativar o FortiCloud

Material elaborado pela Hubsoft para provedores de internet. Pode ser compartilhado na íntegra, com a fonte.

Sistema	Falha	Situação	Ação
			SSO se não usar
Roundcube	CVE-2025-49113, CVE-2025-68461	Exploração ativa (CISA, 20/02)	1.6.16 ou 1.7.1 no mínimo (as atuais são 1.6.21 e 1.7.6, de 09/11), que corrigem também a CVE-2026-48842 (injeção de SQL sem autenticação)
Zimbra	CVE-2026-73570	Exploração ativa, sem autenticação	10.1.20 ou superior
FreePBX	CVE-2025-57819, CVE-2025-64328, CVE-2026-46376	Mais de 900 centrais invadidas, 51 no Brasil	Atualizar módulos; painel administrativo fora da internet
GenieACS	CVE-2025-56015 (API NBI sem autenticação)	Exploit público	Fechar a porta da NBI no firewall
OLT V-SOL série 1600	Execução de comandos sem login (SNMP e web)	Divulgada, sem correção conhecida	Isolar a gerência; trocar senhas e communities
Câmeras Dahua e Hikvision	CVE-2021-33044, 33045; CVE-2017-7921, CVE-2021-36260	Mais de 14.500 câmeras Dahua invadidas em 2026	Atualizar firmware; desativar P2P se não usar
Cisco Catalyst SD-WAN e firewalls ASA/FTD	CVE-2026-76504 e outras quatro (SD-WAN); CVE-2026-20349 e 76418 (ASA/FTD)	Exploração ativa (CISA)	Versões corrigidas na seção de roteadores
OpenSSH em Alpine Linux (contêineres e VMs)	CVE-2026-123158	Exploração ativa (CISA, 09/11)	Atualizar o pacote openssh e reiniciar o sshd

Dentro da empresa (computadores, sistemas internos e soluções próprias), estes itens estão sendo usados em ataques:

Sistema	Falha	Situação	Ação
Google Chrome e navegadores baseados em Chromium	CVE-2026-125350	Exploração ativa (CISA, 10/11)	Chrome 157.0.8103.50 ou superior; reiniciar o navegador
Windows e Outlook	CVE-2026-124194 (roubo de hash NTLM)	Exploração ativa	Atualização cumulativa de novembro/2026

Material elaborado pela Hubsoft para provedores de internet. Pode ser compartilhado na íntegra, com a fonte.

Sistema	Falha	Situação	Ação
WordPress (núcleo)	CVE-2026-119977	Exploração ativa (CISA, 03/11)	Atualizar e conferir os administradores do site
Plugins de WordPress	Elementor Pro, Everest Forms Pro, WP Maps Pro	Exploração ativa	Atualizar; remover plugins sem uso
ConnectWise ScreenConnect	CVE-2026-84869	Catálogo da CISA desde 11/09	Cliente 26.6.5 ou superior
VPNs de borda (SonicWall SMA 1000, Ivanti, NetScaler, GlobalProtect, Check Point)	Várias	Exploração ativa, parte por grupos de ransomware	Versões mínimas na seção de acesso remoto (várias mudaram em outubro e novembro); 2FA em todo acesso
Atlassian Data Center (Jira, Confluence, Bitbucket)	CVE-2026-21589	Exploração ativa (CISA, 15/10)	Versões corrigidas de outubro/2026
Microsoft SharePoint (local)	CVE-2026-45659, 58644, 50522, 65660 e outras	Oito falhas exploradas em 2026 (CISA), uma delas por ransomware	Atualização de agosto/2026 ou posterior; migrar o 2016 e o 2019
n8n	CVE-2026-21858 e outras	Exploração ativa	1.123.101, 2.48.8 ou 2.49.5 em diante; painel fora da internet
Langflow e Flowise	Mais de uma dezena de falhas em 2026	Exploração ativa	Langflow 1.13.3 ou superior; o Flowise foi descontinuado: migrar. Painel fora da internet
LiteLLM	CVE-2026-42208, 42271, 59822, 40217	As quatro no catálogo da CISA (a 40217 desde 18/11)	1.100.4 ou superior; não usar a master key de exemplo
Docker (API na porta 2375)	Exposição sem autenticação	Botnets ativas em 2026	Fechar a porta para a internet
Microsoft Exchange (local)	CVE-2026-42897	Exploração ativa (CISA, 15/05)	Atualizações de junho e julho/2026; o 2016 e o 2019 não recebem mais correção: migrar
SAP NetWeaver	CVE-2025-42884 (Enterprise Portal)	Exploração ativa (CISA, 20/11)	Nota SAP 3660969 e as notas de 10/11/2026 aplicadas; portal fora da internet

No datacenter, na hospedagem e na borda da rede, estes:

Sistema	Falha	Situação	Ação
cPanel e WHM	CVE-2026-41940;	Explorada desde	Última build da sua linha (no

Sistema	Falha	Situação	Ação
	CVE-2026-87899 e outras	fevereiro/2026	mínimo 11.110.0.159, 11.134.0.72, 11.136.0.52 ou 11.138.0.25); painel restrito por IP
Synology DSM	CVE-2024-10441 e duas de 2026	Ransomware C3RB3R desde outubro/2026	Atualizar o DSM; NAS fora da internet
F5 BIG-IP (APM)	CVE-2026-94127, CVE-2025-53521	Exploradas (CISA)	Hotfix do fabricante
WatchGuard Firebox	CVE-2025-14733	Usada por grupos de ransomware	Atualizar o Fireware
Gerência de servidor (iLO, iDRAC, IPMI)	CVE-2013-4786, CVE-2024-54085	24.650 BMCs expostas em julho/2026	Tirar da internet; trocar a senha de fábrica
TV box Android não certificada	Botnets BadBox 2.0 e Kimwolf	Milhões de aparelhos infectados	Usar só modelo certificado
Firewalls e gateways de e-mail (SonicWall SonicOS, Barracuda ESG, FortiMail, PAN-OS, Cisco Secure Email Gateway)	Várias, de outubro e novembro/2026	Exploração ativa (CISA)	Versões corrigidas na seção de outros firewalls
HPE Aruba (AOS-8 e AOS-10)	CVE-2026-79844 a 79851 (nota 10)	Sem exploração conhecida, mas oito falhas de gravidade máxima sem login	AOS-10.8.1.2, 10.7.2.7 ou 10.4.1.14; AOS-8.13.3.1 ou 8.10.0.24

Os detalhes de cada item, com versões e condições de exploração, estão nas seções seguintes.

Material elaborado pela Hubsoft para provedores de internet. Pode ser compartilhado na íntegra, com a fonte.

Parte 2 · Rede do provedor

2. Roteadores e concentradores

MikroTik é o item mais urgente desta seção: quatro falhas do RouterOS estão sendo usadas para tomar o controle de roteadores. A Juniper publicou um lote grande de correções críticas, ainda sem exploração conhecida. Na Cisco, o SD-WAN e os firewalls ASA e FTD têm falhas exploradas.

MikroTik RouterOS — prioridade crítica

Seis falhas divulgadas em 05/09/2026 pelo CERT da Polônia. As de SSH e btest (67276, 67277, 67279 e 86060) têm exploração ativa, com indícios desde 02/09, um dia antes da correção. Depois vieram mais três: uma crítica no serviço web (06/10), uma no SNMP (20/10) e uma do kernel Linux (03/11).

CVE	Componente	O que permite	Versões afetadas	Corrigido em
• EXPLORADA **CVE-2026-67276**	SSH (chave RSA)	Entrar como um usuário existente sem ter a chave privada	7.9 a 7.23.3; 7.24 a 7.24.1 (o aviso da MikroTik lista também a 6.49.21 como correção)	7.23.4, 7.24.2
• EXPLORADA **CVE-2026-67279**	SSH (rekey)	Executar comandos sem autenticação, ler e sobrescrever arquivos	6.x até 6.49.20; 7.0 a 7.23.3; 7.24 a 7.24.1	6.49.21, 7.23.4, 7.24.2
• EXPLORADA **CVE-2026-86060**	SSH (login)	Escalar privilégio; combinada com a 67276 dá controle total	6.x até 6.49.20; 7.0 a 7.23.3; 7.24 a 7.24.1	6.49.21, 7.23.4, 7.24.2
• EXPLORADA **CVE-2026-67277**	btest (UDP)	Vazar memória e reiniciar o roteador, sem autenticação	6.x até 6.49.20; 7.0 a 7.23.3; 7.24 a 7.24.1	6.49.21, 7.23.4, 7.24.2
CVE-2026-67281	WebFig (/jsproxy)	Ler arquivos com credenciais, sem autenticação	7.20 a 7.23.3; 7.24 a 7.24.1	7.23.4, 7.24.2
CVE-2026-67278	Verificação de assinatura RSA (TLS, SSH)	Forjar certificados e se passar por servidor	7.0 a 7.23.5; 7.24 a 7.24.2	7.23.6, 7.24.3
CVE-2026-84411 (nota 9,8)	Serviço web (WebFig, www e www-ssl)	Uma única requisição HTTP, sem autenticação, executa código como root ou derruba o serviço. Aviso de 06/10/2026, sem exploração conhecida	RouterOS 6 e 7 anteriores às versões corrigidas	6.49.23, 7.23.8, 7.24
CVE-2026-88464	SNMP	Uma requisição SNMP com community válida (a "public" de fábrica serve) derruba o SNMP. Aviso de 20/10/2026	7.20 em diante (o RouterOS 6 não é afetado)	7.23.3, 7.24

Material elaborado pela Hubsoft para provedores de internet. Pode ser compartilhado na íntegra, com a fonte.

CVE	Componente	O que permite	Versões afetadas	Corrigido em
CVE-2026-98432	Kernel Linux (TCP IPv4)	Tráfego TCP IPv4 destinado ao próprio roteador pode travá-lo ou reiniciá-lo. Aviso de 03/11/2026	RouterOS 7 (o 6 não é afetado)	7.24.6, 7.25.1
CVE-2026-63887, 64320, 68431	Kernel Linux (iSCSI, NVMe sobre rede e servidor SMB)	Corrupção e vazamento de memória do kernel pela rede, sem autenticação, nos serviços de armazenamento e de compartilhamento de arquivos. Corrigidas em 19 e 20/11/2026, sem aviso próprio da MikroTik	RouterOS 7 usado como servidor de arquivos ou de armazenamento (SMB, iSCSI, NVMe sobre TCP)	7.24.7, 7.25.2

Ação: RouterOS 6 em 6.49.23; RouterOS 7 em 7.24.6 (long-term) ou 7.25.1 (stable), ou superiores. Em 19 e 20/11/2026 saíram a 7.24.7 (long-term) e a 7.25.2 (stable), com mais três correções de kernel (última linha da tabela), que só importam para quem usa o roteador como servidor de arquivos ou de armazenamento. Há relatos no fórum da MikroTik de lentidão em OpenVPN depois da 7.24.7: testar em poucos equipamentos antes de aplicar em massa. Quem não puder ir direto: o mínimo que cobre as falhas críticas (as de setembro e a CVE-2026-84411) é 6.49.23, 7.23.8 ou 7.24.3. As versões 7.23.4 e 7.24.2 trouxeram correção incompleta da CVE-2026-67278. Enquanto não atualizar: fechar SSH, WebFig (serviços www e www-ssl), SNMP e btest para a internet. Como houve exploração antes do patch, vale revisar usuários, scripts e agendamentos em roteadores que ficaram expostos.

Juniper Junos OS — prioridade alta

Os boletins de 14/10/2026 corrigem dezenas de falhas no Junos OS e no Junos OS Evolved, ao menos nove delas críticas (nota 9,8). A Juniper declarou não ter conhecimento de exploração.

CVE	Afeta	O que permite
CVE-2026-101954, 101986, 101956, 101983	J-Web	Controle total do equipamento sem autenticação, quando o J-Web está ativo
CVE-2026-102182	Série MX	Execução de código como root via pacotes IKE com certificado
CVE-2026-102178, 101990, 101982, CVE-2026-33789	BGP / EVPN	Derrubar o daemon de roteamento ou comprometer a Routing Engine
CVE-2026-33796	BMP	Comandos como root quando o monitoramento BMP está ativo
CVE-2026-102175	Daemon de service-deployment (SDX/SRC)	Execução de código ou negação de serviço

Versões corrigidas do Junos OS: 23.2R2-S7.7, 23.4R2-S8.13, 24.2R2-S5.5, 24.4R2-S5, 25.2R2-S2, 25.4R1-S3, 25.4R2, 26.2R1-S2, 26.2R2 e 26.4R1. Ação: atualizar; desativar o J-Web onde não for usado;

Material elaborado pela Hubsoft para provedores de internet. Pode ser compartilhado na íntegra, com a fonte.

restringir sessões BGP a vizinhos conhecidos.

Cisco — prioridade alta, com um item crítico

Sistema	CVE	Situação	Corrigido em
• EXPLORADA **IOS e IOS XE (SNMP)**	CVE-2025-20352	Exploração ativa: estouro de pilha no SNMP, com execução de código como root para quem tem credenciais	Releases de setembro/2025 em diante
IOS XE	CVE-2026-20267 a 20273 (a pior com nota 9,8)	Pacote de agosto/2026, sem exploração conhecida	17.9.10, 17.12.8, 17.15.6, 17.18.4, 26.1.2
IOS XR	CVE-2026-20274 a 20280 (duas críticas, nota 9,8)	Pacote de 02/09/2026	Conforme o advisory de hardening do IOS XR
IOS XR	CVE-2026-20040, CVE-2026-20046	Usuário autenticado vira root (março/2026)	25.2.21 ou 25.4.2 (CVE-2026-20040); 25.2.2 (CVE-2026-20046); demais trens: migrar
Nexus 9000 (Silicon One)	CVE-2026-20212 (nota 9,8)	Execução de código como root sem autenticação	Patch de 02/09/2026
• EXPLORADA **Catalyst SD-WAN (Manager, Controller, Validator)**	CVE-2026-20127, 20182, 76504 (críticas); CVE-2026-20245, 20262	Exploração ativa (as cinco no catálogo da CISA): acesso administrativo sem login e comandos como root	20.9.10.1, 20.12.8.2, 20.15.6.1, 20.18.4.1, 26.1.2.1 ou 26.2.1
• EXPLORADA **ASA e FTD (VPN SSL)**	CVE-2026-20349 (nota 8,6)	Exploração ativa desde agosto/2026: uma requisição HTTP sem login reinicia o firewall	ASA 9.16.4.103, 9.18.4.94, 9.20.4.49, 9.22.3.26, 9.23.1.47 ou 9.24.1.26; FTD 7.0.10, 7.2.12, 7.4.8, 7.6.6, 7.7.13 ou 10.0.2. Uma segunda falha do mesmo tipo (CVE-2026-76418, no catálogo da CISA desde 29/10/2026) tem correção mais nova: conferir no Cisco Software Checker

Ação: conferir a release no Cisco Software Checker; restringir SNMP a IPs do NMS e trocar communities; não expor a interface web (HTTP Server) do IOS XE.

Huawei, Nokia e ZTE

Não localizamos falha nova de 2026 com exploração conhecida para Huawei NetEngine, Nokia 7750 SR ou ZTE ZXR10. A Huawei publicou avisos de segurança ao longo de 2026, mas sem detalhe público de modelo nas fontes consultadas. Ação: consultar o PSIRT de cada fabricante com o modelo e a versão em mãos e

Material elaborado pela Hubsoft para provedores de internet. Pode ser compartilhado na íntegra, com a fonte.

manter a release recomendada.

3. OLTs e gerência da rede óptica

A OLT V-SOL série 1600 tem falhas divulgadas que permitem executar comandos sem login, e o artigo que as descreve não aponta correção do fabricante. Para as demais marcas, o risco principal continua sendo gerência exposta com senha ou community de fábrica.

V-SOL (V-Solution) série 1600 — prioridade crítica, sem correção

Pesquisa da Quarkslab publicada em 19/05/2026 (“How OLTs may have exposed entire ISP networks”).

Falha	Modelos	Exige login?	O que permite
Injeção de comandos no traceroute via SNMP	V1600GS-O32, GS-F, GS-ZF, G0-B, G1-B, G2-B, G1WEO-B, V1600GT, V1600XG02	Não	Executar comandos na OLT
Injeção de comandos em /action/tracert.html	Os mesmos	Não	Executar comandos na OLT
Injeção de comandos no login TACACS+ (/action/main.html)	Séries GS, G0-B, G1-B, G2-B e G1WEO-B	Não (exige TACACS+ ativo e web exposta)	Executar comandos pelos campos de usuário e senha
Credenciais de fábrica no admin web	Todos	—	Acesso administrativo
Cloud EMS (gerenciador da frota)	Versão mais recente à época	Não	Envio de arquivo sem autenticação, com execução de código como root

O artigo não traz números de CVE nem versão de firmware corrigida. Ação: tirar a gerência (web, SNMP, Telnet/SSH) de qualquer rede alcançável pela internet ou pelos assinantes; trocar a senha do admin e as communities SNMP; restringir SNMP ao IP do sistema de gerência; consultar a V-SOL sobre firmware novo.

Huawei MA5600T / MA5800 e ZTE C300 / C350

Não localizamos falha nova de 2026 para essas OLTs. Duas antigas continuam relevantes para quem roda firmware defasado:

Equipamento	CVE	O que permite	Versões afetadas
Huawei SmartAX MA5600T,	CVE-2020-9067	Execução remota de código por estouro de buffer	MA5600T V800R013C10 a V800R018C10; MA5800

Equipamento	CVE	O que permite	Versões afetadas
MA5800, EA5800			V100R017C00 a V100R019C10
ZTE ZXA10 C300M / C350M	CVE-2022-39070 (nota 9,8)	Acesso remoto ao equipamento por falha de controle de acesso	Firmware 2.1.0 anterior à correção indicada pela ZTE

Ação: confirmar a versão em uso contra o boletim do fabricante e atualizar se estiver na faixa afetada.

Demais OLTs integradas ao HubSoft

Fiberhome, Nokia 7360, Datacom, Parks, Intelbras, C-Data, TP-Link, Ubiquiti UFiber, Furukawa, Raisecom, Zhone, Zyxel, Digistar, Cianet, Think, BDCom, Phyhome, Hioso, HSGQ, Chima, Tenda e GigaTelco: não temos CVE pública de 2026 mapeada para a OLT, e para parte desses fabricantes a busca não foi exaustiva. Isso não significa que não existam falhas. Vários desses fabricantes não publicam boletins de segurança, e a pesquisa da Quarkslab mostra o padrão comum em OLTs de baixo custo: injeção de comandos por SNMP e pela interface web, e senha de fábrica.

Ação para todas: aplicar a regra geral (gerência isolada, senhas e communities trocadas), manter o firmware mais recente do fabricante e isolar também o software de gerência (EMS/NMS, U2000, NetNumen, UNM2000 e equivalentes).

4. Rádios e Wi-Fi

A Ubiquiti concentrou os alertas do ano: mais de dez boletins para a linha UniFi, um deles com exploração ativa, e falhas que atingem os rádios airMAX, LTU e airFiber.

Ubiquiti UniFi (UniFi OS, Network, Protect, Talk, Access) — prioridade crítica

Boletim	Data	Principais CVEs	Situação
062	Março/2026	CVE-2026-22557 (nota máxima, tomada de conta), CVE-2026-22558	UniFi Network; sem exploração conhecida
● EXPLORADA **064**	21/05/2026	CVE-2026-34908, 34909, 34910 (sem autenticação), CVE-2026-33000	Exploração ativa; incluídas no catálogo da CISA em 23/06
066	02/07/2026	25 falhas, entre elas CVE-2026-50746 (nota 10), 50747, 50748, 54400, 54402	Sem exploração conhecida
067	26/08/2026	22 falhas, entre elas CVE-2026-77550 (nota 10, burla a autenticação), 77537 (Protect) e 77554 (Talk), ambas sem autenticação	Sem exploração conhecida
065	10/06/2026	CVE-2026-47367, 47369, 47370 (nota 9,9), 47368,	UniFi OS: injeção de comandos por usuário de baixo privilégio;

Material elaborado pela Hubsoft para provedores de internet. Pode ser compartilhado na íntegra, com a fonte.

Boletim	Data	Principais CVEs	Situação
		48610	sem exploração conhecida
069	22/09/2026	CVE-2026-77544 e mais cinco (nota 7,5)	Negação de serviço sem autenticação em consoles e gateways; sem exploração conhecida
073	18/11/2026	CVE-2026-132802 a 132808 (quatro com nota 9,9)	UniFi Access: comandos como root por usuário de baixo privilégio, duas falhas sem autenticação; sem exploração conhecida

Versões que cobrem até o boletim 073:

Produto	Versão mínima
UniFi OS (consoles e gateways)	5.1.31 (UniFi Express: 4.0.21)
UniFi OS Server	5.1.37
UniFi Network	10.5.67
UniFi Protect	7.2.105
UniFi Talk	5.3.2
UniFi Access	4.3.24

A versão corrigida varia por família de hardware: confirme o build do seu modelo. Ação: atualizar; não expor o console UniFi diretamente à internet.

Ubiquiti airMAX, airFiber e bridges (UBB/UDB) — prioridade alta

CVE	Produtos	O que permite	Correção
CVE-2026-21638 (nota 8,8)	UBB-XG até 1.2.2; UDB-Pro e UDB-Pro-Sector até 1.4.1; UBB até 3.1.5	Quem está no alcance do rádio executa código no equipamento, sem autenticação	UDB-Pro 1.4.2; UBB 3.1.7; UBB-XG 1.2.3
CVE-2026-21639 (nota 8,8)	airMAX AC, airMAX M, airFiber AF60 e AF60-XG	Quem está no alcance do rádio executa código no equipamento, sem autenticação	airMAX AC 8.7.21; airMAX M 6.3.26; AF60 2.6.8; AF60-XG 1.2.3
CVE-2026-116837 (nota 8,8) e mais três, de 26/10/2026	airMAX M até 6.3.24; LTU PTMP até 2.4.1; LTU PTP até 1.5.6	Quem alcança o rádio pela rede local executa código no equipamento, sem autenticação	airMAX M 6.3.26; LTU PTMP 2.4.2; LTU PTP 1.5.7
CVE-2026-77532	EdgeSwitch até 1.12.1	Execução de código por rede adjacente, sem autenticação, quando o DHCPv6 está ativo	EdgeSwitch 1.12.2

Material elaborado pela Hubsoft para provedores de internet. Pode ser compartilhado na íntegra, com a fonte.

As duas primeiras foram divulgadas em 06/01/2026. Nenhuma das quatro tem exploração conhecida. O UISP não aparece nos boletins de 2026 que consultamos, mas deve seguir a regra geral: nunca exposto sem VPN.

Cambium Networks

Produto	Falha	Situação
PMP 450b High Gain	CVE-2026-37243 (XSS armazenado na interface web)	Corrigida no firmware 25.0.1, de março/2026
ePMP 1000 e 2000 com firmware 3.5 ou anterior	Injeção de comandos (CVE-2017-5255 e relacionadas)	Antiga, com módulos prontos no Metasploit; usa as credenciais de fábrica (admin, installer, home, readonly). Corrigida no 3.5.1
ePMP Force 300-25, versão 4.7.0.1	CVE-2023-6691: usuário local com credencial vira root; não é explorável remotamente, segundo a CISA (alerta ICSA-23-348-01)	A Cambium não respondeu à CISA e não há firmware corrigido indicado: gerência isolada, contas de fábrica trocadas e consulta ao suporte

Ação: firmware atual em toda a base ePMP e troca das quatro contas de fábrica.

Intelbras (APC 5A e linha de rádios) e Deliberant

Não localizamos CVE pública de 2026 para esses rádios. Vale a regra geral.

5. CPEs, ONUs e roteadores de assinante

Equipamentos de assinante acumulam falhas de execução de comandos, várias sem autenticação e algumas em modelos que não recebem mais firmware. O caminho prático é empurrar firmware novo pelo ACS e bloquear o acesso à gerência pela WAN.

Fabricante	Modelos	CVE	O que permite	Correção
TP-Link	Archer VX1800v	CVE-2026-15427, 15428, 15429	Injeção de comandos, inclusive pela interface TR-069/CWMP	Firmware 0.16.0 2.0.0 v6092.0 Build 260521 (aviso de 14/07/2026)
TP-Link	Produtos gerenciados por ISP	CVE-2025-30237 a 30241	Várias falhas (advisory 5239)	Firmware indicado no advisory
TP-Link	TL-WR940N	CVE-2026-12935; CVE-2026-11409, 11410	Execução remota de código quando um aparelho da rede local acessa um servidor RTSP malicioso; injeção de comandos por	Firmware V6_260528 (EN e US) ou V6_260527 (JP). Modelo em fim de vida: planejar

Fabricante	Modelos	CVE	O que permite	Correção
			administrador autenticado	a troca
TP-Link	TL-WR841N	CVE-2026-76649, 76650, 76651	Queda do UPnP e estouro de buffer no HTTP, sem autenticação, a partir da rede local (nota 5,3; aviso 5270)	V14: firmware 4.19 Build 260820 (US) ou Build 260821 (EU)
TP-Link	Vários roteadores	CVE-2026-12001; CVE-2026-75118; CVE-2026-11834	Credencial fixa no firmware; estouro de pilha antes do login; injeção de comandos por opção DHCP	Firmware indicado em cada advisory
TP-Link	Archer NX200, NX210, NX500, NX600	CVE-2025-15517 e outras três	Envio de firmware sem autenticação	Firmware de março/2026
• SEM CORREÇÃO **Tenda**	HG9, HG3 2.0, HG10 (ONTs GPON)	CVE-2026-2907, CVE-2026-7096, CVE-2026-86167	Estouro de buffer e injeção de comandos em /boaform/formgponConf, por usuário autenticado; exploits públicos	Sem correção no registro da CVE: trocar a senha de fábrica e bloquear a gerência pela WAN
• SEM CORREÇÃO **Tenda**	G103	CVE-2026-5339	Injeção de comandos na configuração GPON, por administrador autenticado	Sem correção no registro da CVE: trocar a senha de fábrica e bloquear a gerência pela WAN
Zyxel	CPEs DSL/Ethernet, ONTs de fibra, extensores	CVE-2025-13942 (nota 9,8)	Execução de comandos sem autenticação via UPnP, quando o acesso pela WAN e o UPnP estão habilitados	Firmware de fevereiro e março/2026
Zyxel	Os mesmos	CVE-2026-1459, CVE-2026-0711, CVE-2026-1460, CVE-2026-6952	Injeção de comandos após login	Firmware indicado nos avisos de 24/02, 28/04 e 21/07/2026
• EXPLORADA	CPEs DSL	CVE-2024-40890,	Exploração ativa;	Não será

Fabricante	Modelos	CVE	O que permite	Correção
Zyxel	legados	CVE-2024-40891, CVE-2025-0890	credenciais padrão no Telnet	corrigida: substituir
Fiberhome	HG6145F1	CVE-2025-63353 (nota 9,8)	Senha Wi-Fi de fábrica previsível a partir do nome da rede (SSID), no firmware RP4423	Trocar a senha Wi-Fi padrão em todas as unidades (pelo ACS, se possível)
Fiberhome	AN5506-01A	CVE-2025-1614, 1615, 1616	Injeção de comandos no diagnóstico e XSS	Conferir com o fabricante
Huawei	EG8141A5, EG8145V5, EG8145V5-V2	CVE-2025-49599	A conta Epuser consegue desativar o firewall da ONT e liberar SSH/Telnet	Afeta versões até V5R019C00S100 / V5R021C00S184 ; conferir com a Huawei
ZTE	ZXHN H188A	CVE-2026-34472	Vazamento de credenciais sem autenticação, pela rede local	Conferir com a ZTE
ZTE	ZXHN F660T / F660A	CVE-2025-53558	Mesma credencial em todas as unidades	V1.0.10P17N4 / V1.0.10P14N4
• EXPLORADA **GL.iNet**	Roteadores (GL-MT3000, GL-MT6000, GL-AXT1800 e outros) e KVM IP ligados à nuvem GoodCloud	Sem CVE divulgada (aviso de 20/11/2026)	Invasores exploraram uma falha na nuvem de gerência do fabricante e instalaram malware em parte dos equipamentos conectados a ela	A nuvem foi corrigida, mas o aparelho infectado continua infectado: instalar o firmware de segurança de 22/11/2026 do modelo, procurar o processo crond -i /tmp/.log e trocar as senhas e chaves que passaram pelo equipamento

Ação:

- Levantar no ACS os modelos e versões em campo e atualizar em lote.
- Bloquear acesso à interface web, Telnet/SSH e TR-069 pela WAN; liberar a porta do CWMP só para

Material elaborado pela Hubsoft para provedores de internet. Pode ser compartilhado na íntegra, com a fonte.

o IP do ACS.
- Trocar a senha padrão de administração por uma única por equipamento.
- Planejar a troca dos modelos que o fabricante não atualiza mais.

6. Gerência de CPE (ACS / TR-069)

O GenieACS 1.2.13 deixa a API NBI acessível sem autenticação, e já existe exploit público. Quem alcança essa porta lê os dados de todos os equipamentos de assinante gerenciados, que podem incluir credenciais de PPPoE e de Wi-Fi.

Componente	CVE	O que permite	Ação
GenieACS (API NBI)	CVE-2025-56015 (nota 7,5), publicada em 07/04/2026	Acesso sem autenticação à NBI	Liberar a porta da NBI (padrão 7557) apenas para os IPs dos sistemas que integram com o ACS, como o HubSoft
• EXPLORADA **Node.js (base do GenieACS)**	CVE-2026-111497 (Brotli)	Execução remota de código; exploração confirmada	Node.js 22.23.4, 24.22.1 ou 26.12.1
MongoDB (banco do GenieACS e do UniFi Network)	CVE-2026-118383 (nota 9,5)	Derrubar membros de um replica set sem autenticação; lote de novembro/2026 com 26 falhas	7.0.48, 8.0.37, 8.3.16 ou 9.0.7; porta 27017 nunca exposta
genieacs-mcp (ferramenta de terceiros)	CVE-2026-55637	DNS rebinding por falta de validação de origem	genieacs-mcp 0.3.2 ou superior; remover se não usar

Para os ACS comerciais integrados ao HubSoft (Anlix/Flashman, ACS Plus, Int6, Made4IT, OLT Cloud), não localizamos CVE pública. Vale consultar o fornecedor e aplicar a mesma regra.

Ação para qualquer ACS:

- Interface de administração e API acessíveis só por VPN ou IPs autorizados.
- Porta do CWMP (padrão 7547) aberta apenas para as redes dos assinantes, com autenticação entre CPE e ACS.
- Sistema operacional, Node.js e MongoDB do servidor do ACS atualizados.

7. Núcleo da rede: CGNAT, BNG, roteamento e DNS recursivo

Concentradores, roteadores em software e resolvedores DNS ficam no caminho de todo o tráfego do provedor. A maior parte das falhas abaixo derruba o serviço em vez de invadir, mas para um provedor isso já é parar a operação.

Produto	CVE	Risco	Situação e correção
accel-ppp (PPPoE, IPoE,	CVE-2026-123205 e mais onze, segundo	Derrubar o concentrador sem autenticação, por estouro de	Corrigidas no accel-ppp 1.15.0 (29/10/2026). Como mitigação da

Produto	CVE	Risco	Situação e correção
L2TP)	a VyOS	memória	123205, manter verbose=0 na seção de log
VyOS	Treze falhas: as doze do accel-ppp e uma no update-check	Execução remota de código pelo mecanismo de verificação de atualização	VyOS 1.5.1 ou 1.4.5 LTS (07/09/2026)
FRRouting	CVE-2026-37459, 37460, 37457; CVE-2026-129456	Um UPDATE de BGP derruba o bgpd, e todas as sessões caem. A falha mais recente (129456) é disparada por um vizinho com sessão estabelecida e só afeta vizinhos com soft-reconfiguration inbound	FRR 10.6.2, 10.5.4, 10.4.4, 10.3.4 ou 10.7.0 em diante; a 10.6.1 não corrige a 129456. Os pacotes do Debian 12 e 13 constavam como vulneráveis à 37460 e à 129456 no rastreador do Debian. Aceitar TCP 179 só dos vizinhos configurados
● EXPLORADA **F5 BIG-IP (APM)**	CVE-2026-94127 (nota 9,8); CVE-2025-53521	Execução remota de código sem login	As duas exploradas (catálogo da CISA em 22/09/2026 e em 27/03/2026). A 94127 só afeta quem usa APM como servidor de autorização OAuth: hotfix 21.1.0.2.0.30.22, 17.5.1.9.0.160.12 ou 17.1.3.5.0.41.14 (aviso K000162605). A 53521: 17.5.1.3, 17.1.3, 16.1.6.1 ou 15.1.10.8
Unbound	CVE-2026-81642 (nota 9,1), CVE-2026-82717 (nota 8,4); CVE-2026-96405 e mais quatro	Uma zona maliciosa consultada pelo resolvedor pode derrubá-lo e, possivelmente, executar código; consultas forjadas consomem a CPU	1.26.2 ou superior (21/10/2026); as duas primeiras foram corrigidas na 1.26.1. Sem exploração relatada
PowerDNS Recursor e dnsdist	CVE-2026-73206, CVE-2026-52682 e outras	Negação de serviço; envenenamento de cache em cenários específicos	Recursor 5.3.12 ou 5.4.8; dnsdist 1.9.16, 2.0.8 ou 2.1.1
FastNetMon Community	CVE-2026-48692 (API gRPC), CVE-2026-48687 (plugin Juniper) e outras	Quem alcança a porta 50052 bane ou libera IPs, dispara anúncios BGP de blackhole e executa scripts, sem autenticação; injeção de comandos no plugin de integração com Juniper	Atualizar para a 1.2.9, que refez o plugin Juniper. A API gRPC continua sem autenticação: bloquear a porta 50052 no firewall

Ação:

- Resolvedor DNS respondendo só para os blocos de IP dos assinantes, nunca aberto para a internet.
- Sessões BGP com filtro de origem, senha ou TCP-AO quando o vizinho suportar, e limite de prefixos.

Material elaborado pela Hubsoft para provedores de internet. Pode ser compartilhado na íntegra, com a fonte.

- Gerência do concentrador (BNG, CGNAT) fora da rede de assinantes.
- Servidor de logs de CGNAT isolado e com acesso restrito: ele guarda os registros de conexão que o provedor é obrigado a preservar.

Material elaborado pela Hubsoft para provedores de internet. Pode ser compartilhado na íntegra, com a fonte.

Parte 3 · Servidores e datacenter

8. Servidores e serviços do provedor

Servidores Linux com nginx e PHP expostos são o alvo mais provável hoje: as duas famílias de falhas permitem invadir sem login, e foram encadeadas com falhas de kernel para chegar a root (em ataques reais, no caso do PHP; em demonstração de pesquisadores, no caso do nginx). Vale para Zabbix, portais, hotspots, webmail, sites e qualquer sistema próprio.

Servidor web e linguagem

Componente	CVE	Condição para explorar	Corrigido em
nginx	CVE-2026-123007	HTTP/2 ativo (presente desde a versão 1.9.5, de 2015)	1.30.7, 1.31.9
nginx	CVE-2026-123633	HTTP/2 com encaminhamento para upstream	1.30.7, 1.31.9
nginx	CVE-2026-123634	resolver + proxy_pass derivado da requisição + mirror	1.30.7, 1.31.9
nginx	CVE-2026-121810	HTTP/3 com encaminhamento para upstream	1.30.7, 1.31.9
nginx	CVE-2026-113425	Proxy de e-mail com auth_http	1.30.7, 1.31.9
● EXPLORADA **nginx**	CVE-2026-42945 (rewrite) e CVE-2026-42055 (cabeçalhos HTTP/2)	Falhas de maio e junho/2026; a 42945 foi explorada dias após a divulgação	1.30.1 e 1.30.3 em diante
● EXPLORADA **PHP**	CVE-2026-109618, CVE-2026-109619 (nota 9,2)	Qualquer PHP que atenda requisições web, sem login; exploração ativa (catálogo da CISA, 26/10/2026)	8.2.36, 8.3.37, 8.4.28 ou 8.5.13 (de 19/11/2026). O mínimo para o PHP2Shell é 8.2.35, 8.3.36, 8.4.27 ou 8.5.12
PHP	CVE-2026-129474, 129496, 126714, 115560 e outras (lote de 19/11/2026)	Execução remota de código em configurações fora do padrão; falhas também no PHP-FPM e no PHP-CGI. Sem exploração relatada	8.2.36, 8.3.37, 8.4.28 ou 8.5.13
● EXPLORADA **Brotli**	CVE-2026-111497 (nota 9,2)	Biblioteca usada por Node.js, Python, .NET, Envoy e	1.0.10, 1.1.1, 1.2.1

Material elaborado pela Hubsoft para provedores de internet. Pode ser compartilhado na íntegra, com a fonte.

Componente	CVE	Condição para explorar	Corrigido em
		outros; exploração confirmada (catálogo da CISA, 27/10/2026)	
Java (OpenJDK)	CVE-2026-114938, “Java4Shell” (nota 9,2)	Java 17.0.6 em diante em CPU x86-64 com AVX-512 VBMI; afeta Keycloak, Jira, Confluence, Jenkins e outros sem autenticação	17.0.21.1, 21.0.13.1, 25.0.5.1, 27.0.1.1 (já nos pacotes do Ubuntu, Debian, RHEL e Amazon Linux; há prova de conceito pública, sem exploração confirmada)
Ruby	CVE-2026-132825, “Ruby2Shell”	Aplicações Rails e Sinatra, sem autenticação; os autores anunciaram a publicação da prova de conceito para 25/11/2026, e a partir dela é de esperar tentativas de ataque; a falha não constava no catálogo de falhas exploradas da CISA em 23/11/2026	3.3.14, 3.4.13, 4.0.10 (3.2 e anteriores não terão correção)

Para o nginx, desativar o HTTP/2 bloqueia apenas duas das cinco falhas; o mesmo pacote corrige outras cinco (dez ao todo). Em 23/11/2026 saíram a 1.30.8 e a 1.31.10, que corrigem mais uma falha, a CVE-2026-132779 (consumo excessivo de CPU em TLS 1.3 com ssl_early_data ativo, gravidade média): preferir essas versões. Depois de atualizar, reinicie o serviço: o reload não troca o binário. O PHP de versões fora de suporte não recebe release oficial: migrar. O PHP 8.2 chega ao fim de vida em 31/12/2026.

Sistema operacional

Componente	CVE	O que permite	Situação e correção
• EXPLORADA **Kernel Linux**	CVE-2026-31431 (Copy Fail)	Usuário comum vira root; atravessa contêineres	Exploração ativa; kernels 6.18.22, 6.19.12, 7.0 ou o pacote corrigido da distribuição
• EXPLORADA **Kernel Linux**	CVE-2026-46300 (Fragnesia); CVE-2026-43284 e 43500 (DirtyFrag)	Escalada para root	Fragnesia usada junto com o PHP2Shell para instalar webshell como root; no catálogo da CISA desde 28/10/2026. Corrigida em 5.10.257, 5.15.208, 6.1.174, 6.6.141, 6.12.91, 6.18.33 e 7.0.10
• EXPLORADA **Kernel Linux**	CVE-2026-53362; CVE-2026-53266, CVE-2025-39682, CVE-2025-39964	Escalada de privilégio e negação de serviço	No catálogo da CISA desde 27/08/2026 (53362) e 18/09/2026 (as outras três). A 53362 está corrigida em 6.1.177, 6.6.144, 6.12.95, 6.18.38 e 7.1.3; a 53266, em 5.10.259, 5.15.210, 6.1.176, 6.6.143, 6.12.94, 6.18.36 e 7.0.13

Material elaborado pela Hubsoft para provedores de internet. Pode ser compartilhado na íntegra, com a fonte.

Componente	CVE	O que permite	Situação e correção
● SEM CORREÇÃO **Kernel Linux (SCTP)**	Sem CVE divulgada (parte do nginx2root)	Transforma uma invasão do nginx em root no servidor	Sem correção até a publicação; ver seção de falhas sem correção
Kernel Debian	CVE-2026-80521	Uso de memória já liberada no tratamento de sockets locais (AF_UNIX)	Corrigida nos repositórios de segurança: Debian 13 com linux 6.12.111-1 ou superior (DSA-6528-1); Debian 12 com linux 6.1.190-1 ou superior (DLA-4841-1). Conferir se o repositório security está habilitado, atualizar e reiniciar
OpenSSH	CVE-2026-35414, CVE-2026-35385 a 35388	Burla de controle de acesso em cenários com certificados, e outras	10.3 (abril/2026); novas correções nas 10.4, 10.5 e 10.6 e nas atualizações das distribuições
apt (Debian, Ubuntu)	CVE-2026-109518	Quem intercepta tráfego HTTP do repositório (espelho ou proxy malicioso) instala pacote falso como root	Corrigida em 04/11/2026: apt 2.6.2 (Debian 12), 3.0.4 (Debian 13), 2.4.15ubuntu0.1 (Ubuntu 22.04) e 2.8.4ubuntu0.1 (Ubuntu 24.04). Atualizar o apt e preferir espelhos HTTPS
Kernel Linux (SCTP)	CVE-2026-64564 (SCTPhantom)	Usuário comum vira root e pode sair do contêiner; um par SCTP remoto pode derrubar o servidor	Corrigida em 5.10.265, 5.15.216, 6.1.183, 6.6.148, 6.12.101, 6.18.42 e 7.1.6. Não confundir com a falha de SCTP do nginx2root, que segue sem correção
Kernel Linux (TCP)	CVE-2026-98432	Uso de memória já liberada no TCP IPv4, que pode travar ou reiniciar o equipamento	Corrigida em 5.10.272, 5.15.223, 6.1.190, 6.6.159, 6.12.113, 6.18.56 e 7.2.10. Vale também para o que embarca o kernel, como o RouterOS 7 e o Proxmox
● EXPLORADA **OpenSSH em Alpine Linux e outros sistemas com musl sem PAM (contêineres, VMs e appliances)**	CVE-2026-123158 (nota 8,1)	Login por senha sem conhecer a senha: uma senha muito longa é aceita em contas sem senha definida, como o root do Alpine	Explorada (catálogo da CISA, 09/11/2026). Atualizar o pacote openssh do Alpine (ou OpenSSH 10.6p2) e reiniciar o sshd; se não der, PasswordAuthentication no. Debian e Ubuntu padrão (glibc com PAM) não são atingidos

Material elaborado pela Hubsoft para provedores de internet. Pode ser compartilhado na íntegra, com a fonte.

DNS, RADIUS, e-mail, monitoramento e telefonia

Sistema	CVE	O que permite	Correção
BIND 9	CVE-2026-5946, 5947 (maio); CVE-2026-11331, 11605 (julho); CVE-2026-3104, 1519	Derrubar ou esgotar o servidor DNS remotamente; sem exploração conhecida	9.20.26 ou superior. Na série 9.18, a 9.18.49 cobre as falhas até maio; para as de julho o registro só indica correção na 9.20.26: confirmar com a ISC ou migrar para a 9.20
FreeRADIUS	CVE-2026-127030 (EAP-FAST), CVE-2026-127029 (EAP-SIM), de 12/11/2026	Derrubar o serviço sem autenticação; só afeta quem habilitou esses módulos EAP	Pacote corrigido da distribuição; desabilitar EAP-FAST e EAP-SIM se não usar
Roundcube	CVE-2026-48842 (nota 8,1)	Injeção de SQL sem autenticação no plugin virtuser_query; sem exploração confirmada até 24/11/2026	1.6.16, 1.7.1 (as atuais, com novas correções de segurança, são 1.6.21 e 1.7.6, de 09/11/2026)
● EXPLORADA **Roundcube**	CVE-2025-49113, CVE-2025-68461	Execução de código e XSS; exploração ativa (catálogo da CISA, 20/02/2026)	Versão atual da série 1.6
● EXPLORADA **Zimbra**	CVE-2026-73570	Comandos sem autenticação quando o pacote zimbra-snmp está instalado e as notificações SNMP estão ativas; exploração ativa (catálogo da CISA, 21/08/2026)	10.1.20
Zabbix	CVE-2026-23921, 23920, 23919	Injeção de SQL cega na API, com extração de dados (23921); injeção de comandos em scripts por usuário autenticado (23920); vazamento de dados entre hosts (23919)	7.0.22, 7.2.15 ou 7.4.6 para a 23921 e a 23920. Para a 23919: 6.0.42, 7.0.19, 7.2.13 ou 7.4.3
Zabbix	CVE-2026-23926, 23928; CVE-2026-23937	XSS armazenado; extração de chave PSK por usuário autenticado	7.0.24 e 7.4.8 (XSS); 6.0.47, 7.0.28 e 7.4.12 (PSK)
Grafana	CVE-2026-27876 (nota 9,1)	Escrita de arquivos que leva a execução de código	11.6.14, 12.1.10, 12.2.8, 12.3.6, 12.4.2
Grafana	CVE-2026-81841 (nota 5,3); CVE-2026-28381	Falha de autorização em dashboards públicos; leitura e escrita de arquivos pelo	12.4.12, 13.0.10, 13.1.7 ou 13.2.3 (a 81841 não tem correção indicada na série 11.6). Plugin

Material elaborado pela Hubsoft para provedores de internet. Pode ser compartilhado na íntegra, com a fonte.

Sistema	CVE	O que permite	Correção
	(nota 9,6, no plugin Snowflake Datasource)	plugin Snowflake	Snowflake: atualizar para a última versão
Grafana	CVE-2026-33379	Qualquer usuário autenticado cria, publica externamente e apaga snapshots de dashboards	Afeta só da 12.4.0 à 12.4.3; corrigida na 12.4.4. Sem exploração conhecida
Grafana MCP (conector de IA)	CVE-2026-19516 (nota 9,1), CVE-2026-15583 (nota 8,6)	Requisições forjadas a partir do servidor (SSRF) pelo cabeçalho X-Grafana-URL	Última versão do servidor MCP do Grafana; não expor à internet
LibreNMS	CVE-2026-26988 (nota 9,3), CVE-2026-6204, CVE-2026-84189 (nota 9,2)	Injeção de SQL sem login; execução de código por usuário autenticado; XSS armazenado pela URL do Oxidized	26.7.0 ou superior
Wazuh	CVE-2026-25769 (nota 9,1), CVE-2026-30893 (crítica)	Execução remota de código em instalações em cluster, com exploit público, e escrita de arquivos fora do diretório na sincronização. As duas exigem um nó já autenticado no cluster	4.14.4 ou superior
Asterisk	CVE-2026-57160; CVE-2026-57185 a 57202; CVE-2026-23741	Estouro de buffer em cabeçalho SIP e outras	20.20.1, 21.12.3, 22.10.1 ou 23.4.1
• EXPLORADA **FreePBX**	CVE-2025-57819 (nota 10)	Execução de código sem autenticação com o painel administrativo exposto; exploração ativa	Módulo endpoint 15.0.66, 16.0.89 ou 17.0.3 em diante
• EXPLORADA **FreePBX**	CVE-2025-64328; CVE-2026-46376 (nota 9,3)	Injeção de comandos após login no módulo filestore, explorada ativamente (catálogo da CISA, 03/02/2026); credencial fixa no painel de usuário (UCP)	Atualizar todos os módulos; conferir se há webshell instalado
• EXPLORADA **FreeSWITCH**	CVE-2026-116779 (nota 9,8)	Uma mensagem SIP executa comandos da API e do sistema; exploração ativa (catálogo da CISA, 09/11/2026)	1.11.3 ou superior

Centrais baseadas em Asterisk de terceiros (Issabel e similares) herdam as falhas do Asterisk: consulte o

fornecedor.

9. Virtualização, firewalls e switches

O painel de virtualização é o ponto mais sensível da infraestrutura: quem entra nele pode desligar ou apagar todos os servidores do provedor. VMware tem falhas usadas por grupos de ransomware, e o Proxmox VE 7 tem uma burla de autenticação que não será corrigida.

Sistema	CVE	O que permite	Situação e correção
• EXPLORADA **VMware vCenter**	CVE-2026-59310; CVE-2026-59309 (nota 9,8)	Execução de código sem autenticação pelo servidor Syslog do vCenter; burla de autenticação	Exploração ativa, inclusive por ransomware (catálogo da CISA, 18/08/2026). Aviso VMSA-2026-0006, de 29/07/2026: vCenter 8.0 U3k (ou U2f), 9.0.2.0100 ou 9.1.0.0300. Essas versões já não bastam: a falha de 19/11/2026, na linha seguinte, exige atualizar de novo
• EXPLORADA **VMware vCenter (falha nova, de 19/11/2026)**	CVE-2026-123890 (nota 9,8)	Burla de autenticação sem login no serviço de diretório do vCenter: o invasor assume a administração do ambiente. Usada como zero-day desde setembro/2026 por um grupo de espionagem, que criou contas de administrador e plantou chaves SSH nos hosts ESXi	Catálogo da CISA desde 20/11/2026. Aviso VMSA-2026-0009: vCenter 8.0 U3m, 9.0.2.0200 ou 9.1.1.0200. Não há solução de contorno, e quem aplicou o patch de julho precisa atualizar de novo. O vCenter 7.0 não tem correção pública: migrar. O mesmo aviso corrige o VMware Tools para Windows (13.1.5 ou 12.5.5). Depois de atualizar, revisar contas administrativas e chaves SSH
• EXPLORADA **VMware ESXi**	CVE-2025-22224, 22225, 22226	Escapar da máquina virtual para o hypervisor	Exploradas ativamente (catálogo da CISA, 04/03/2025), com uso por ransomware reportado; patch de março/2025 (VMSA-2025-0004)
• EXPLORADA **Proxmox VE 7**	PSA-2026-00043 (CVE-2023-54391, nota 9,8)	Login como qualquer usuário sem 2FA, inclusive root, sem senha, pela API na porta 8006 (libpve-access-control de 7.0-7 até antes de 8.0.4)	Exploração ativa confirmada pela Proxmox, com prova de conceito pública. Versão fora de suporte desde julho/2024: migrar para o Proxmox VE 9 (o 8 saiu de suporte em agosto/2026). Contas com 2FA não são afetadas, e a Proxmox publicou um paliativo no fórum para quem não consegue migrar já

Material elaborado pela Hubsoft para provedores de internet. Pode ser compartilhado na íntegra, com a fonte.

Sistema	CVE	O que permite	Situação e correção
Proxmox VE 8 e 9 (kernel)	CVE-2026-31431, 43284, 43500, 46300	Usuário local vira root no host	Atualizar o proxmox-kernel e reiniciar
Proxmox VE 8 e 9 (kernel)	CVE-2026-64564 (SCTPhantom); CVE-2026-98432 (TCP)	Escalada de privilégio; uso de memória liberada na pilha TCP	SCTPhantom: proxmox-kernel 6.8.12-41 (PVE 8) ou 7.0.14-10 (PVE 9). CVE-2026-98432: só o proxmox-kernel 7.0.14-25, do PVE 9
KVM em servidor AMD (Proxmox VE e outros)	CVE-2026-99312, divulgada em 18/11/2026	Quem é root dentro de uma VM lê e altera a memória do host e, com isso, a das outras VMs. Só afeta hosts AMD com virtualização aninhada ligada; Intel não é afetado	Sem exploração conhecida. Kernel 7.3.5, 6.18.64 ou 6.12.118; no Proxmox VE 9, usuários do fórum apontam o proxmox-kernel 7.0.14-30 como corrigido, ainda sem confirmação oficial da Proxmox: conferir o changelog do pacote e reiniciar o host. Até atualizar, ou no PVE 8: desligar a virtualização aninhada (options kvm_amd nested=0). Prioridade para quem hospeda VMs de clientes
Proxmox VE 8 e 9	PSA-2026-00039, 00042, 00072 a 00081	Falhas de validação e de permissão em migração, backup e console	No PVE 9, apt full-upgrade até qemu-server 9.2.11, pve-manager 9.2.24, pve-xtermjs 6.0.0-3 e libpve-common-perl 9.2.5 ou superiores. O Proxmox VE 8 saiu de suporte em agosto/2026 e só recebeu correção para os dois primeiros avisos: migrar para o 9
• EXPLORADA **Fortinet FortiOS, FortiManager, FortiAnalyzer, FortiProxy**	CVE-2026-24858 (nota 9,4)	Entrar em equipamentos de outros clientes pelo login FortiCloud SSO	Exploração ativa desde janeiro/2026 (catálogo da CISA, 27/01/2026). FortiOS 7.6.6, 7.4.11, 7.2.13 ou 7.0.19 e versões corrigidas dos demais produtos; desativar o FortiCloud SSO se não usar
Fortinet FortiOS, FortiManager e FortiAnalyzer (avisos de 10/11/2026)	CVE-2026-126253 (nota 9,3), CVE-2026-126261 (nota 9,0) e outras	No FortiOS, um atacante sem login faz o firewall anunciar rotas falsas por OSPF. No FortiManager, execução de código sem login pelo canal de gerência FGFM; outros avisos do mesmo dia atingem também o FortiAnalyzer	Sem exploração conhecida. FortiOS 8.0.2, 7.6.8, 7.4.13 ou 7.2.14. FortiManager: 8.0.1, 7.6.8, 7.4.6 ou 7.2.9 para a falha do FGFM (aviso FG-IR-26-275); para cobrir os demais avisos de novembro do FortiManager e do FortiAnalyzer, 8.0.2, 7.6.8, 7.4.12 ou 7.2.13 (conferir o aviso de

Material elaborado pela Hubsoft para provedores de internet. Pode ser compartilhado na íntegra, com a fonte.

Sistema	CVE	O que permite	Situação e correção
			cada falha). Porta do FGFM (541) fechada para a internet
• EXPLORADA **Fortinet FortiOS, FortiProxy e FortiWeb**	CVE-2025-59718, CVE-2025-59719	Burla de autenticação em equipamentos expostos: a 59718 no FortiOS, FortiProxy e FortiSwitchManager; a 59719 no FortiWeb	A 59718 tem exploração ativa (catálogo da CISA, 16/12/2025): FortiOS 7.6.4, 7.4.9, 7.2.12 ou 7.0.18 em diante. FortiWeb: 8.0.1, 7.6.5 ou 7.4.10
• EXPLORADA **Zyxel GS1900 (switches)**	CVE-2026-107441 (nota 8,8)	Execução de comandos por requisição HTTP à interface web	Zero-day usado para invadir 996 switches em 48 países. Firmware Patch 3, de outubro/2026 (aviso de 03/11/2026), por exemplo GS1900-8 2.90(AAHH.3)C0
• EXPLORADA **Zyxel GS1900 (switches)**	CVE-2026-7273 (nota 8,8)	Estouro de pilha na interface web, sem autenticação, a partir da rede local	No catálogo da CISA desde 21/09/2026. O firmware de junho/2026 corrige esta falha, mas não a da linha de cima: instalar direto o Patch 3, o mesmo da linha de cima
Cisco Nexus 9000	CVE-2026-20212 (nota 9,8)	Execução de código como root sem autenticação	Patch de 02/09/2026
• EXPLORADA **VMware ESXi**	CVE-2026-47876 (nota 9,3); CVE-2026-41709	Escapar da máquina virtual para o hypervisor pelo adaptador de rede VMXNET3 (47876); administrador executa operações sem registro em log (41709)	A 41709 está no catálogo da CISA desde 28/10/2026. Mesmo aviso do vCenter (VMSA-2026-0006): ESXi 8.0 U3k (build 25595708) ou U2f (25626445), 9.0.2.0100 ou 9.1.0.0200
Proxmox VE 9	PSA-2026-00068, PSA-2026-00046	Escape da VM para o host pela rede virtio; comandos como root no host a partir de imagem OCI maliciosa	proxmox-kernel 7.0.14-24 e pve-container 6.1.14 ou superiores
• EXPLORADA **Fortinet FortiOS e FortiProxy**	CVE-2025-61624; CVE-2025-25249, CVE-2025-68686	Escrita e remoção de arquivos por administrador autenticado (61624); as outras duas também têm exploração confirmada	No catálogo da CISA desde 16/10, 09/09 e 27/07/2026. A 61624 está corrigida no FortiOS 7.6.5 e 7.4.10; para as demais, seguir o aviso da Fortinet para a sua série

Ação:

- Painel do hypervisor (vCenter, ESXi, Proxmox na porta 8006) acessível só por VPN, com senha forte e 2FA.
- Backup das máquinas virtuais guardado fora do próprio hypervisor.

Material elaborado pela Hubsoft para provedores de internet. Pode ser compartilhado na íntegra, com a fonte.

- Firewall de borda sem administração exposta na WAN; revisar contas de administrador criadas sem o seu conhecimento.
- Switches gerenciáveis com a interface web em VLAN de gerência separada.

10. Datacenter e POP: gerência de servidor, storage e energia

A placa de gerência do servidor (BMC), o storage e o nobreak costumam ser instalados uma vez e esquecidos. Quem chega neles controla a máquina mesmo desligada, os backups e a energia do POP.

Produto	CVE	Risco	Situação e correção
● SEM CORREÇÃO **Gerência de servidor por IPMI (HPE iLO, Supermicro, Dell iDRAC)**	CVE-2013-4786	O protocolo IPMI 2.0 entrega o hash da senha a quem pedir. A senha de fábrica do iLO foi quebrada em menos de um minuto	24.650 BMCs expostas em julho/2026, com nota de resgate encontrada em um iLO 4. É falha de projeto, sem patch: desativar IPMI sobre LAN e tirar a porta de gerência da internet
● EXPLORADA **AMI MegaRAC (Supermicro, Gigabyte, ASRock, Huawei e outros)**	CVE-2024-54085 (nota 10)	Burla de autenticação pela interface Redfish: controle total do servidor	Explorada (catálogo da CISA, junho/2025). Firmware da placa com MegaRAC SPx 12.7 ou 13.5 em diante
● SEM CORREÇÃO **HPE iLO, Supermicro, Dell iDRAC 10, OpenBMC**	Pesquisa da runZero (DEF CON, agosto/2026)	Conjunto de falhas em grande parte ainda sem correção	Tratar toda BMC como não confiável: VLAN de gerência isolada e firmware atual
● EXPLORADA **Synology DSM**	CVE-2024-10441, CVE-2026-13639, CVE-2026-13684 (nota 9,8)	Leitura e gravação de arquivos sem login (as duas de 2026) e execução de código sem login (a de 2024); o ransomware C3RB3R criptografa os arquivos	Ataques desde outubro/2026 em equipamentos desatualizados (a falha de 2024 entrou no catálogo da CISA em 18/11/2026); a Synology aponta a falha de 2024 como porta de entrada, e pesquisadores, as de 2026. DSM 7.4-90075, 7.3.2-86009-4, 7.2.2-72806-9 ou 7.2.1-69057-12 em diante
QNAP (QTS, QuTS hero, QVR Pro)	CVE-2026-22898 (QVR Pro) e os avisos de fevereiro e março/2026	Execução de código e acesso a dados	QVR Pro 2.7.4.1485 e Qsync Central 5.0.0.4 ou superiores; manter o QTS e o QuTS hero atualizados
● SEM CORREÇÃO **Nobreaks e PDUs com placa de rede (Vertiv, APC, Eaton,**	CVE-2025-46412, CVE-2025-41426 (Vertiv, nota 9,8); CVE-2024-58310 (APC)	Vertiv: burla de autenticação e execução de código na placa, o que permite desligar a energia do POP. APC: leitura de arquivos do	Vertiv: RDU101 1.9.1.2_0000001 e IS-UNITY 8.4.3.1_00160 ou superiores. APC: o registro não indica versão corrigida; firmware atual e placa fora de rede

Produto	CVE	Risco	Situação e correção
Minuteman)		sistema sem autenticação	exposta. A placa Minuteman 1.60.3 tem falha crítica (CVE-2026-88560) divulgada em 31/08/2026, sem correção conhecida

Ação:

- BMC, nobreak, PDU, retificadora e controle de acesso em VLAN de gerência, sem rota para a internet.
- Trocar as senhas de fábrica de BMCs e placas de nobreak.
- NAS fora da internet, com snapshots imutáveis e uma cópia dos dados em outro local.
- Conferir no roteador de borda se alguma porta de gerência (623/UDP do IPMI, 443 da BMC, 5000 e 5001 do Synology, 8080 e 443 do QNAP) está redirecionada.

11. Hospedagem, e-mail e banco de dados

Vale para o provedor que hospeda sites e e-mails de clientes ou mantém os próprios.

Produto	CVE	Risco	Situação e correção
● EXPLORADA **cPanel e WHM**	CVE-2026-41940 (nota 9,8)	Burla de autenticação: acesso administrativo ao painel e a todos os sites hospedados	Explorada desde 23/02/2026, com uso para ransomware. Corrigida em 28/04/2026
cPanel e WHM	CVE-2026-58048 e CVE-2026-87899 (nota 9,4), CVE-2026-68490; CVE-2026-67401 e CVE-2026-93698 (nota 9,9)	Um cliente de hospedagem executa SQL como administrador do banco (58048), executa código como root pelo CalDAV/CardDAV (87899) e altera bancos de outras contas pelo WP Toolkit (CVE-2026-87900)	O mínimo subiu a cada aviso. Builds que cobrem até o aviso de 29/09/2026: 11.110.0.148, 11.134.0.61, 11.136.0.45 ou 11.138.0.11. Em 18/11/2026 saiu nova release de segurança (11.110.0.159, 11.134.0.72, 11.136.0.52 e 11.138.0.25) e, em 19/11, mais duas atualizações (pacotes internos de PHP e manutenção de segurança): usar a build mais recente da sua linha, igual ou superior a essas. As linhas 118, 126 e 132 não recebem mais builds: migrar. WP Toolkit 6.11.3 ou superior
Plesk	CVE-2026-68488 e 68487 (Backup Manager, nota 9,9); CVE-2026-64637, CVE-2026-67394,	Um cliente ou revendedor de hospedagem assume o servidor inteiro como root	Plesk Obsidian 18.0.82 Update 3 ou 18.0.81 Update 8 (12/11/2026) em diante, com as extensões atualizadas (RESTful API 2.4.7, Site Import 1.12.2). As primeiras

Material elaborado pela Hubsoft para provedores de internet. Pode ser compartilhado na íntegra, com a fonte.

Produto	CVE	Risco	Situação e correção
	CVE-2026-68492, CVE-2026-87898		falhas já estavam corrigidas em 10/09/2026, mas houve correções críticas depois
• EXPLORADA **Plugin LiteSpeed para cPanel**	CVE-2026-48172	Escalada de privilégio, possivelmente até root	Explorada em maio/2026; plugin 2.4.5 ou superior
Exim	CVE-2026-45185 (nota 9,8)	Execução de código sem login em instalações compiladas com GnuTLS	4.99.3. O Exim é o servidor de e-mail padrão do Debian
Dovecot	Aviso de 26/08/2026: 25 falhas, entre elas a CVE-2026-42007 (nota 9,1)	Usuário de e-mail autenticado corrompe memória com um script Sieve (extensão editheader), com possível execução de código; quedas do ManageSieve e do IMAP sem login	Dovecot CE 2.4.5; desativar a extensão Sieve editheader e o ManageSieve se não forem usados
MariaDB	CVE-2026-49261 (nota 10); CVE-2026-85746, 85748, 92262 (nota 9,9)	Comprometimento do servidor de banco; usuário de baixo privilégio executa código	10.6.28, 10.11.19, 11.4.13, 11.8.9 ou superior. A 49261 só afeta clusters Galera com wsrep_notify_cmd; a 85748, só as séries 12.3 e 13.0 (12.3.3 e 13.0.2)
• EXPLORADA **Plugin Acronis Backup (cPanel, Plesk, DirectAdmin)**	CVE-2026-87886 (nota 7,8)	Um usuário comum do servidor vira root	Explorada (catálogo da CISA, 16/09/2026). Plugin cPanel 1.9.3.1021, extensão Plesk 1.8.11.638 ou plugin DirectAdmin 1.2.3.238, ou superiores
• EXPLORADA **N-able Mail Assure / SpamExperts (filtro de e-mail)**	CVE-2026-134624 (nota 9,3)	Um usuário da API faz o servidor acessar sistemas internos (SSRF). A falha foi usada na invasão da própria N-able, que deixou o painel e a API fora do ar de 16 a 21/11/2026	Catálogo da CISA desde 23/11/2026. A nuvem do fabricante já foi corrigida; quem opera instalação própria (Local Cloud) deve confirmar a build 20261121.1943 ou superior. Os tokens de API e OAuth foram revogados pela N-able: integrações precisam ser refeitas

Ação:

- Portas dos painéis de hospedagem (2083, 2087, 8443, 10000) restritas por IP ou VPN.
- Banco de dados (3306, 27017) nunca exposto à internet.
- Microsoft 365 e Google Workspace: 2FA obrigatório para todas as contas, protocolos legados bloqueados e revisão periódica das regras de encaminhamento e dos aplicativos de terceiros

Material elaborado pela Hubsoft para provedores de internet. Pode ser compartilhado na íntegra, com a fonte.

autorizados.

- SPF, DKIM e DMARC configurados no domínio, para dificultar e-mail falso em nome do provedor.

12. Ferramentas de operação: documentação de rede, monitoramento e cofres de senha

Essas ferramentas concentram as credenciais e o mapa da rede. Uma falha nelas vale mais para o atacante do que uma falha em um único equipamento.

Produto	CVE	Risco	Situação e correção
● SEM CORREÇÃO **NetBox**	CVE-2026-29514 (nota 8,8); CVE-2026-86175	Execução de código por usuário com permissão de modelos; usuário só de leitura obtém pela API as senhas de Git e S3	A 29514: 4.6.1 ou superior. A 86175 afeta até a 4.7.0 e foi divulgada em 05/09/2026; segue sem correção até a 4.7.6, de 24/11/2026 (as notas de versão não registram correção)
phpIPAM	CVE-2026-12194	Inclusão de arquivos por usuário da API, que vem desativada por padrão	Atualizar; manter a API desligada se não for usada
Cacti	CVE-2026-39938 (nota 9,8); CVE-2026-39949, CVE-2026-40079	Execução de código sem login (inclusão de arquivo local) e por usuário autenticado	1.2.31 ou superior
Nagios XI	CVE-2026-2042, CVE-2026-2043	Injeção de comandos pelos assistentes de configuração	Nagios XI 2026R1.0.1 ou superior
Vaultwarden	CVE-2026-26012, CVE-2026-27801, CVE-2026-31835	Membro da organização lê todas as senhas; burla do 2FA em ações protegidas	1.36.0 ou superior

Ação:

- Oxidized, RANCID e ferramentas parecidas guardam a configuração, e muitas vezes a senha, de todos os equipamentos: acesso só por VPN, repositório privado e usuário de coleta somente de leitura.
- Cofre de senhas com 2FA, fora da internet e com backup próprio.
- Monitoramento com SNMPv3 onde o equipamento suportar; onde não suportar, community trocada e restrita ao IP do servidor.

Material elaborado pela Hubsoft para provedores de internet. Pode ser compartilhado na íntegra, com a fonte.

Parte 4 · Borda e acesso remoto

13. Outros firewalls, Wi-Fi corporativo e impressoras

Produto	CVE	Risco	Situação e correção
OPNsense	CVE-2026-44193 (nota 9,1), CVE-2026-45158, CVE-2026-57155 (nota 9,9), CVE-2026-119409	Execução de código como root por usuário autenticado com privilégio, parte com código de ataque público	26.7.8 ou superior
pfSense	CVE-2026-111224, CVE-2026-111225	Execução de comandos pela autenticação remota do OpenVPN (exige conta válida no RADIUS ou LDAP) e pelo nome do certificado do cliente OpenVPN	Avisos de 17/11/2026. Afetam o Plus até a 26.07 e o CE até a 2.9.0: atualizar para o pfSense Plus 26.07.1 ou o CE 2.9.1 (17/11/2026), ou aplicar os Recommended System Patches
• EXPLORADA **SonicWall SMA 1000**	CVE-2026-83548 (nota 10), CVE-2026-83549; CVE-2026-102255 (nota 10) a 102258	Segunda e terceira levas de falhas do ano no mesmo equipamento (setembro e outubro), após a de julho	A leva de setembro foi explorada (catálogo da CISA, 02/09/2026). Instalar 12.4.3-03670 ou 12.5.0-03082 ou superior; ver também a seção de acesso remoto
• EXPLORADA **WatchGuard Firebox**	CVE-2025-14733	Execução de código pelo serviço de VPN IKEv2	No catálogo da CISA desde 19/12/2025, com uso por ransomware confirmado em 2026. Atualizar o Fireware
TP-Link Omada (gateways, switches, APs e controladora)	CVE-2026-19586; CVE-2025-15627 a 15631	Injeção de comandos sem login no servidor OpenVPN dos gateways; chaves fixas no protocolo de adoção	Firmware mais recente de cada modelo e controladora atualizada (avisos de 11/08 e 20/08/2026)
HPE Aruba (AOS-8 e AOS-10)	CVE-2026-79844 a 79851 (nota 10); CVE-2026-23825	Execução de código e burla de autenticação sem login (aviso de 22/10/2026); sem exploração conhecida	AOS-10.8.1.2, 10.7.2.7 ou 10.4.1.14; AOS-8.13.3.1 ou 8.10.0.24. Gerência e PAPI (UDP 8211) só em VLAN de gerência
Impressoras Brother, Fujifilm, Ricoh, Konica Minolta e Toshiba	CVE-2024-51978	A senha de administrador de fábrica pode ser calculada a partir do número de série	Atinge 695 modelos (748 somando as outras falhas da mesma pesquisa) e não é totalmente corrigível por firmware: trocar a senha de administrador
• EXPLORADA **SonicWall SonicOS**	CVE-2026-19868	Quem tem senha válida de outro método (por exemplo, usuário local) entra na VPN	Explorada (catálogo da CISA, 06/11/2026). SonicOS 7.3.4-7013 (Gen7) ou 8.2.3-8015 (Gen8);

Material elaborado pela Hubsoft para provedores de internet. Pode ser compartilhado na íntegra, com a fonte.

Produto	CVE	Risco	Situação e correção
(firewalls Gen7 e Gen8) com SSL-VPN e SAML		sem passar pelo SAML nem pelo MFA	revisar logins de VPN sem registro no provedor de identidade
• EXPLORADA **Barracuda Email Security Gateway (e ADC, WAF, Web Security Gateway, Message Archiver)**	CVE-2026-116606 (nota 9,3), CVE-2026-111560 (nota 8,6)	Quem alcança a interface de administração importa uma configuração forjada sem login e, em seguida, executa comandos como root	Exploradas (catálogo da CISA, 10/11/2026). Conferir se o patch automático foi aplicado e atualizar o firmware (ESG 9.4.0.030 ou superior); interface de administração fora da internet
• EXPLORADA **Fortinet FortiMail**	CVE-2026-104286 (nota 9,8)	Gravação de arquivos sem login por HTTP ou HTTPS	Explorada (catálogo da CISA, 01/10/2026). FortiMail 8.0.2, 7.6.7, 7.4.9 ou 7.2.10
• EXPLORADA **Palo Alto PAN-OS (interface de gerência)**	CVE-2026-0322	Execução de código como root por usuário autenticado na interface de gerência	Explorada (catálogo da CISA, 14/10/2026). PAN-OS 12.2.4, 12.1.10-h2, 11.2.16 ou o hotfix da sua série; gerência fora da internet
• EXPLORADA **Cisco Secure Email Gateway**	CVE-2026-76519 (nota 9,8)	Um anexo malicioso grava arquivos e executa comandos como root, sem login	Explorada (catálogo da CISA, 14/10/2026). Aplicar a release corrigida indicada pela Cisco

Ação:

- Gerência do firewall (web e SSH) só pela LAN ou por VPN, nunca pela WAN.
- Wi-Fi corporativo separado da rede de gerência e da rede de visitantes.
- Impressoras e smart TVs em VLAN própria, sem acesso aos servidores e com a senha de fábrica trocada.

14. Acesso remoto e VPN

Ferramentas de acesso remoto e concentradores de VPN são hoje a porta de entrada preferida dos grupos de ransomware: ficam expostos à internet por definição e dão acesso direto à rede interna.

Produto	CVE	Risco	Situação e correção
• EXPLORADA **ConnectWise ScreenConnect**	CVE-2026-84869 (nota 9,9)	Falha crítica no cliente (agente) instalado nas máquinas	No catálogo de falhas exploradas da CISA desde 11/09/2026. A falha está no cliente (agente) anterior à 26.6.5. Em instalação própria: atualizar o servidor para a 26.6.5 ou superior e, em seguida, os agentes; na nuvem, basta atualizar os agentes

Material elaborado pela Hubsoft para provedores de internet. Pode ser compartilhado na íntegra, com a fonte.

Produto	CVE	Risco	Situação e correção
• EXPLORADA **SonicWall SMA 1000**	CVE-2026-15409 e 15410 (julho), CVE-2026-83548 e 83549 (setembro), CVE-2026-102255 a 102258 (outubro)	Três levas no ano: em cada uma, um atacante sem login alcança funções internas do equipamento (nota 10) e, com a segunda falha, executa comandos. As duas primeiras foram exploradas, a de julho também por grupos de ransomware	Cada correção não cobre a leva seguinte: instalar 12.4.3-03670 ou 12.5.0-03082 ou superior. Se o equipamento ficou exposto sem patch: reinstalar a imagem, trocar as senhas e redefinir os tokens TOTP
• EXPLORADA **Ivanti Connect Secure**	CVE-2026-104935 (nota 8,6), CVE-2026-111357, CVE-2026-118527	Encadeadas, dão controle total (root) do concentrador de VPN sem login; usadas para roubar credenciais e consultar o Active Directory	Exploradas desde 03/10/2026 (catálogo da CISA em 13/10 e 30/10). O patch de 13/10 não basta: atualizar para 22.8R2.6, 25.1.1.3 ou 25.1.3.0 em diante. O verificador de integridade pode não acusar invasão: revisar logs e trocar credenciais se o equipamento ficou exposto
• EXPLORADA **Palo Alto GlobalProtect**	CVE-2026-0257	Burla de autenticação no portal e no gateway GlobalProtect, para quem usa cookies de "authentication override"; explorada por operadores de ransomware (Qilin, Inc) desde junho/2026	PAN-OS 12.1.4-h6 ou 12.1.7; 11.2.4-h17, 11.2.7-h14, 11.2.10-h7 ou 11.2.12; 11.1.4-h33, 11.1.6-h32, 11.1.7-h6, 11.1.10-h25, 11.1.13-h5 ou 11.1.15; 10.2.7-h34, 10.2.10-h36, 10.2.13-h21, 10.2.16-h7 ou 10.2.18-h6. Mitigação: desativar a opção de cookie ou usar certificado dedicado
• EXPLORADA **Check Point VPN (IKEv1)**	CVE-2026-50751	Conexão na VPN de acesso remoto sem a senha do usuário; explorada por operadores de ransomware (catálogo da CISA, 08/06/2026)	Corrigida desde junho (sk185033). O Jumbo Hotfix de novembro, indicado na linha do Check Point mais abaixo, é posterior e cobre também esta falha. Preferir IKEv2
• EXPLORADA **Citrix NetScaler**	CVE-2026-8452 (junho), CVE-2026-19490, CVE-2026-88771 e 88772 (setembro), CVE-2026-88779 (outubro) e mais 28 falhas em 12/11/2026	Execução de código e burla de autenticação sem login em equipamentos usados como gateway de VPN ou AAA; seis falhas do NetScaler entraram no catálogo de exploradas da CISA em 2026	Atualizar para 14.1-73.57 ou 13.1-64.39 ou superior, que cobrem tudo até o boletim de 12/11/2026, e procurar webshells no equipamento. Por precaução, encerrar as sessões ativas depois do patch
• SEM CORREÇÃO **RustDesk**	CVE-2026-30783 (nota 9,8 no NVD;	O cliente consegue ignorar comandos e políticas do	A 57850 está corrigida na 1.4.9. Para a 30783 (cliente até a 1.4.8)

Material elaborado pela Hubsoft para provedores de internet. Pode ser compartilhado na íntegra, com a fonte.

Produto	CVE	Risco	Situação e correção
	4,8 segundo quem a registrou), CVE-2026-57850	administrador; mensagens de controle fora do escopo da sessão	o projeto não declarou versão corrigida: usar a mais recente (1.5.0) e não contar com políticas aplicadas só no cliente
• SEM CORREÇÃO **AnyDesk**	CVE-2026-15681, CVE-2026-15682	Negação de serviço local, de baixo impacto	Sem correção do fabricante na divulgação (13/07/2026). O risco maior do AnyDesk é o uso em golpes de falso suporte
Fortinet (SSL-VPN)	Ver a seção de firewalls		
• EXPLORADA **Check Point (gateways com Mobile Access, SSL VPN, Captive Portal ou UserCheck)**	CVE-2026-109618 e 109619 (PHP2Shell, nota 9,2), CVE-2026-123039 (Gaia OS)	Execução de código sem login pelo portal web do firewall e, em seguida, escalada para root; nos ataques, o invasor instalou backdoor, passou para o VMware ESXi e apagou dados	Exploradas de 30/10 a 04/11/2026 (catálogo da CISA em 26/10 e 13/11). Jumbo Hotfix de novembro: R82.20 Take 14, R82.10 Take 52, R82 Take 132 ou R81.20 Take 174, ou superior. R81.10 e anteriores: sem correção completa, migrar. Em 23/11/2026 a GreyNoise divulgou uma campanha que invadiu 24 servidores de gerência Check Point em 22 organizações, de outubro ao início de novembro, por falhas já conhecidas, entre elas a CVE-2026-16232 (burla de autenticação do SmartConsole, no catálogo da CISA desde 22/07/2026): a 16232 está corrigida desde julho (R82.10 Take 36, R82 Take 118 ou R81.20 Take 158, todos anteriores ao Jumbo Hotfix de novembro). Manter o servidor de gerência atualizado, sem acesso pela internet e com a lista de Trusted Clients restrita a IPs conhecidos
• EXPLORADA **BeyondTrust Remote Support**	CVE-2026-102764 (nota 9,3)	Operações de arquivo no appliance sem autenticação válida	Explorada (catálogo da CISA, 16/10/2026). Afeta até a 26.2.3: aplicar o patch BT26-05 ou atualizar para a 26.3.1. O mesmo grupo usou esta falha como porta de entrada para chegar ao vCenter (CVE-2026-123890)

Ação:

Material elaborado pela Hubsoft para provedores de internet. Pode ser compartilhado na íntegra, com a fonte.

- VPN e acesso remoto sempre com 2FA e sem conta compartilhada.
- RDP (3389), Winbox (8291), SSH e painéis de hypervisor nunca abertos para a internet: só por VPN ou IP liberado.
- Levantar quais ferramentas de acesso remoto existem nas máquinas (AnyDesk, TeamViewer, RustDesk, ScreenConnect) e remover as que ninguém usa. Ferramenta esquecida é acesso esquecido.
- Appliance de VPN que ficou exposto sem patch durante exploração ativa: além de atualizar, trocar senhas e certificados e revisar as contas criadas.
- Acesso de terceiros (fornecedor, consultor) com usuário próprio, prazo de validade e liberação só quando necessário.

Material elaborado pela Hubsoft para provedores de internet. Pode ser compartilhado na íntegra, com a fonte.

Parte 5 · Dentro da empresa

15. Estações de trabalho

Boa parte das invasões começa no computador de um funcionário, não no roteador. Em novembro/2026 há duas falhas com exploração ativa que atingem praticamente qualquer estação: uma no Chrome e uma no Outlook.

Sistema	CVE	O que permite	Situação e correção
• EXPLORADA **Google Chrome**	CVE-2026-125350	Execução de código ao abrir uma página maliciosa (falha no componente XML)	Exploração ativa; oitavo zero-day do Chrome em 2026. Versão 157.0.8103.50 ou superior (Windows, macOS, Linux)
Microsoft Edge, Brave, Opera e outros baseados em Chromium	A mesma base de código do Chrome	Herdam as falhas do Chromium	Manter a atualização automática ligada e reiniciar o navegador
• EXPLORADA **Microsoft Outlook**	CVE-2026-124194; CVE-2026-110043, 110068, 111309 (nota 8,8)	Roubo do hash de senha do Windows (NTLM) ao abrir um arquivo malicioso; o atacante pode usar o hash para entrar como o usuário. As outras três executam código só de exibir o e-mail no painel de leitura	A 124194 tem exploração ativa (catálogo da CISA, 10/11/2026). Todas corrigidas no Patch Tuesday de 10/11/2026: atualizar o Windows e o Office
Windows 10 e 11	CVE-2026-116928 (nota 9,8) e as demais correções do Patch Tuesday de 10/11/2026	Mais de mil falhas corrigidas, 63 críticas e cerca de 30 com potencial de propagação em rede; entre elas, execução remota no Windows Search	Instalar a atualização cumulativa de novembro. O Windows 11 23H2 recebeu suas últimas atualizações em 10/11/2026, e o 24H2 Home e Pro saiu de suporte em 13/10/2026: migrar para o 25H2
• EXPLORADA **Windows**	CVE-2026-96951	Burla do aviso de arquivo baixado da internet (Mark of the Web), no Windows Shell	Exploração ativa; corrigida no Patch Tuesday de 13/10/2026
• EXPLORADA **Microsoft Defender**	CVE-2026-33825	Escalada de privilégio local	Divulgada antes da correção e explorada logo depois, inclusive por ransomware (catálogo da CISA, 22/04/2026). Corrigida na plataforma 4.18.26030.3011: conferir em Segurança do Windows → Configurações → Sobre. O Defender se atualiza sozinho se não estiver bloqueado

Material elaborado pela Hubsoft para provedores de internet. Pode ser compartilhado na íntegra, com a fonte.

Sistema	CVE	O que permite	Situação e correção
macOS	CVE-2026-86950 (CoreGraphics) e as correções de 09/11/2026	Execução de código ao processar um arquivo malicioso; a Apple relata uso em ataques direcionados contra iPhones	macOS Golden Gate 27.2.1, Tahoe 26.7.3 ou Sequoia 15.8.3 (de 09/11/2026). A 86950 foi corrigida em 28/09/2026, no Tahoe 26.7.1 e no Sequoia 15.8.1
Linux em desktop	As falhas de kernel da seção de servidores	Usuário comum vira root	Atualizar o kernel e reiniciar
● EXPLORADA **Windows**	CVE-2026-68820 (agosto); CVE-2026-81963 e CVE-2026-85880 (setembro)	Usuário local vira SYSTEM; usadas depois que o invasor já entrou na máquina	Exploradas como zero-day; cobertas por qualquer atualização cumulativa de setembro/2026 em diante

Dois programas comuns nas estações também merecem conferência. **Firefox:** 152.0.6 ou ESR 140.13 em diante (duas falhas com código de ataque público, corrigidas em julho/2026). **WinRAR:** a CVE-2025-8088, corrigida na 7.13, continua sendo usada em 2026 por grupos criminosos e de espionagem em arquivos enviados por e-mail, e em julho/2026 saiu a correção de outra falha de execução de código (CVE-2026-14191, corrigida na 7.23). O WinRAR e o 7-Zip não se atualizam sozinhos: é preciso instalar a versão mais recente manualmente em cada máquina.

Ação:

- Atualização automática ligada em Windows, navegadores e Office, com reinício obrigatório pelo menos uma vez por semana.
- Nenhuma estação com sistema fora de suporte (Windows 7, 8 e versões do Windows 10 e 11 sem atualização) nem com Office 2021, fora de suporte desde 13/10/2026.
- Funcionários sem perfil de administrador no uso diário.
- Antivírus ativo e gerenciador de senhas no lugar de senhas salvas em planilhas ou no navegador.
- Máquinas que acessam Winbox, OLT, hypervisor e o HubSoft merecem cuidado dobrado: são o caminho mais curto até a rede.

16. Celulares e aplicativos

O celular hoje guarda o aplicativo de 2FA, o WhatsApp da empresa, o e-mail e, no caso dos técnicos de campo, o acesso ao sistema. Um aparelho desatualizado ou perdido vale tanto quanto uma senha vazada.

Sistema	CVE	O que permite	Situação e correção
Android 14 a 17	CVE-2026-58868	Execução remota de código sem nenhuma ação do usuário	Crítica; sem registro de ataques até 04/11/2026. Corrigida no nível de patch 2026-11-01 ou superior (Configurações → Sobre o dispositivo → Versão do Android → Atualização de segurança do

Sistema	CVE	O que permite	Situação e correção
			Android; nos Samsung, Configurações → Sobre o telefone → Informações do software)
● EXPLORADA **iPhone e iPad**	CVE-2026-86950 e as correções de 09/11/2026	Execução de código ao processar um arquivo malicioso, usada em ataques altamente direcionados; as correções de novembro tratam Bluetooth, AirPlay, Mensagens e Brotli	iOS/iPadOS 27.2.1 ou 26.7.3 (de 09/11/2026); aparelhos antigos (iPhone XS e XR): 18.7.12
● EXPLORADA **WhatsApp (iPhone e Mac)**	CVE-2025-55177	Em 2025 foi usada em ataques sem clique, combinada com uma falha da Apple	Corrigida no WhatsApp para iOS 2.25.21.73 e para Mac 2.25.21.78; manter o aplicativo sempre na última versão da loja

Ação:

- Atualização automática do sistema e dos aplicativos ligada em todos os aparelhos usados para trabalho.
- Aparelho que não recebe mais patch de segurança do fabricante não deve ter 2FA, e-mail nem sistemas da empresa.
- Bloqueio de tela com senha ou biometria e localização/apagamento remoto ativados.
- Confirmação em duas etapas ligada no WhatsApp e no WhatsApp Business (Configurações → Conta → Confirmação em duas etapas), com e-mail de recuperação. Conta de WhatsApp de provedor roubada vira golpe contra os assinantes.
- Aplicativos só das lojas oficiais; nada de APK recebido por mensagem.
- Quando um colaborador sai ou perde o aparelho: desativar o usuário, encerrar as sessões e remover o aparelho do 2FA no mesmo dia.

17. Servidores Windows, colaboração e backup

Produto	CVE	Risco	Situação e correção
Windows Server	CVE-2026-116928 (Windows Search, nota 9,8), CVE-2026-119958 (LDAP, nota 9,8) e as demais do Patch Tuesday de 10/11/2026	Execução de código sem login. Na 116928, basta enviar um e-mail com anexo forjado a um servidor Exchange, sem ninguém abrir a mensagem; na 119958, por chamadas LDAP forjadas. Sem registro de ataques	Instalar a atualização cumulativa do Windows de novembro, primeiro nos servidores com Exchange e nos controladores de domínio. Windows Server 2012 e 2012 R2 estão fora de suporte; o 2016 sai do suporte em 12/01/2027
● EXPLORADA **Microsoft**	CVE-2026-45659,	Execução remota de código,	Instalar a atualização de

Produto	CVE	Risco	Situação e correção
SharePoint (local)	58644, 50522, 65660 e outras quatro	parte sem login; oito falhas do SharePoint entraram no catálogo de exploradas da CISA em 2026, uma delas (45659) com uso por ransomware	segurança mais recente (no mínimo a de agosto/2026, que cobre as oito). SharePoint 2016 e 2019 saíram do suporte em 14/07/2026: planejar a migração e não expor à internet
● EXPLORADA **Microsoft Exchange (local)**	CVE-2026-42897 (nota 8,1); fim de suporte	E-mail forjado executa código no navegador de quem abre a mensagem no webmail (OWA); explorada (catálogo da CISA, 15/05/2026)	Corrigida nas atualizações de junho e julho/2026. Exchange 2016 e 2019: o suporte estendido pago acabou em outubro/2026 e a atualização de 10/11/2026 já saiu só para o Exchange SE. Migrar para o Exchange SE ou o Exchange Online; não manter webmail de versão antiga exposto
Veeam Backup & Replication	CVE-2026-44963	Execução remota de código no servidor de backup por qualquer usuário comum do domínio, quando o servidor está ingressado no domínio (nota 9,4)	Afeta a 12.3.2.4465 e builds anteriores da v12; corrigida na 12.3.2.4854. Sem registro de ataques na divulgação
Veeam Backup & Replication 13	CVE-2026-108142 (nota 9,1)	Atacante sem login burla a autorização do serviço CDP Coordinator do servidor de backup	Afeta a 13.0 e a 13.1 (a 12 não): atualizar para 13.1.2.57 ou 13.0.3.63. Sem exploração declarada pela Veeam

Ação:

- Servidor de backup fora do domínio, com credenciais próprias e sem acesso a partir da rede dos usuários.
- Pelo menos uma cópia de backup offline ou imutável, com teste de restauração periódico. Em ataque de ransomware, o backup é o primeiro alvo.
- Active Directory: conta de administrador de domínio só para administrar o domínio, senhas de serviço longas e NTLM desativado onde for possível (a falha do Outlook deste mês rouba exatamente esse hash).
- SMB (445) e RDP (3389) nunca expostos à internet.
- Compartilhamentos de arquivos com permissão mínima, sem "Todos: controle total".

18. Site institucional, ERP de backoffice e ferramentas internas

O site do provedor, a wiki interna e o sistema de chamados costumam ficar esquecidos em uma hospedagem ou VM antiga. São alvos fáceis e, quando caem, servem para aplicar golpes nos assinantes (boleto falso, página de segunda via clonada) ou como ponte para a rede interna. O ERP de backoffice (SAP, TOTVS, Sankhya, NetSuite), que muitos provedores usam ao lado do HubSoft para contabilidade,

Material elaborado pela Hubsoft para provedores de internet. Pode ser compartilhado na íntegra, com a fonte.

fiscal e RH, entra aqui pelo mesmo motivo: guarda dados financeiros e de pessoal e costuma ficar anos sem atualização.

Produto	CVE	Risco	Situação e correção
• EXPLORADA **WordPress (núcleo)**	CVE-2026-119977 (nota 8,1)	Execução de código sem login durante a janela de atualização do próprio WordPress	Exploração ativa: no catálogo da CISA desde 03/11/2026, com mais de 240 mil tentativas bloqueadas desde a divulgação, segundo a Wordfence. Afeta da 4.7 à 7.1.3. Atualizar para a 7.1.4 ou para a correção do seu ramo (7.0.8, 6.9.11, 6.8.12 e equivalentes, todas de 28/10/2026) e depois conferir administradores e arquivos alterados, porque o site pode ser atacado durante a própria atualização
• EXPLORADA **WordPress (núcleo)**	CVE-2026-63030, CVE-2026-60137	Confusão de rotas na API REST e injeção de SQL	Exploradas em ataques; corrigidas em julho/2026 (7.0.2, 6.9.5 e 6.8.6) e incluídas nas versões da linha de cima
• EXPLORADA **Elementor Pro**	CVE-2026-32475 (até a 4.2.1)	Upload irrestrito de arquivos, quando existe formulário publicado com campo de envio de arquivo	Exploração desde 19/08/2026; corrigida na 4.2.2
• EXPLORADA **Everest Forms Pro**	CVE-2026-3300 (nota 9,8)	Execução remota de código; os ataques criam um administrador falso	Exploração ativa; atualizar para a 1.9.13 ou superior
• EXPLORADA **WP Maps Pro**	CVE-2026-8732 (nota 9,8)	Criação de conta de administrador sem login	Exploração ativa; corrigida na 6.1.1. Plugin comercial: a atualização pode não chegar sozinha
• EXPLORADA **Atlassian Data Center (Jira, Confluence, Bitbucket, Bamboo, Crowd)**	CVE-2026-21589 (nota 9,3)	Leitura de arquivos da aplicação sem login, desde que o atacante saiba o caminho exato; pode expor arquivos sensíveis conforme a configuração	Exploração ativa (catálogo da CISA, 15/10/2026). Corrigida em Jira Software 9.12.40, 10.3.26 e 11.3.12; Jira Service Management 5.12.40, 10.3.26 e 11.3.12; Confluence 9.2.26 e 10.2.19; Bitbucket 9.4.26, 10.2.8 e 10.5.1; Bamboo 10.2.24 e 12.1.12; Crowd 6.3.7, 7.0.3, 7.1.7 e 7.2.4
• EXPLORADA **Nextcloud com Collabora Online (CODE embutido)**	CVE-2026-110447 (nota 9,2)	Execução remota de código	Explorada (catálogo da CISA, 23/10/2026). Collabora Online 26.4.303 ou superior

Material elaborado pela Hubsoft para provedores de internet. Pode ser compartilhado na íntegra, com a fonte.

Produto	CVE	Risco	Situação e correção
● EXPLORADA **Zammad (helpdesk)**	CVE-2026-102489, CVE-2026-102490	Fixação de sessão e escalada local para root	Exploradas (catálogo da CISA, 02/10/2026). Zammad 7.2.2 ou superior
● EXPLORADA **SAP NetWeaver (Enterprise Portal 7.50)**	CVE-2025-42884 (nota 6,5)	Um atacante sem login redireciona uma consulta interna do portal (JNDI) e pode ler ou alterar dados do servidor; segundo a Onapsis, pode chegar à execução de código	Catálogo da CISA desde 20/11/2026. A correção existe desde novembro/2025: aplicar a Nota SAP 3660969 e não deixar o portal exposto à internet
SAP NetWeaver ABAP e S/4HANA	CVE-2026-120017, 76964, 89103 e 89126 (nota 10); CVE-2026-89107 (nota 9,9, no S/4HANA)	Quatro falhas de gravidade máxima exploráveis sem login no núcleo do NetWeaver, entre elas burla de autenticação por SAML e corrupção de memória no ICM; injeção de código no S/4HANA	Patch Day de 10/11/2026, sem exploração conhecida. Aplicar as Notas 3849308, 3778530, 3798345 e 3778556 (as quatro de nota 10) e a 3805589 (S/4HANA). Quem tem o SAP operado por parceiro deve confirmar com ele a aplicação
TOTVS (Protheus, RM, Fluig, Meu RH)	CVE-2024-55210 (Protheus 12.1.2310, nota 9,8); CVE-2025-9193 (Portal Meu RH até a 12.1.17)	Burla do segundo fator de autenticação no Protheus; falha na redefinição de senha do Meu RH	Poucas falhas da TOTVS ganham CVE pública: manter a release dentro do suporte e aplicar os pacotes de atualização. AppServer, SmartClient web, REST e portais só por VPN ou IP liberado
Sankhya	CVE-2022-42989 (única CVE pública)	Script malicioso (XSS) na Caixa de Entrada, em versões anteriores à 4.11b81	Sem falha crítica pública em 2026 nas fontes consultadas. Manter a versão atual e o acesso externo só por VPN ou IP liberado, com senhas individuais
Oracle NetSuite (nuvem)	Sem CVE: risco de configuração	A plataforma é atualizada pela Oracle. O risco está na configuração: tipos de registro personalizados com acesso "No Permission Required" já expuseram dados de clientes em lojas SuiteCommerce (pesquisa da AppOmni, 2024)	Exigir 2FA de todos os usuários, revisar papéis e permissões dos registros personalizados e revogar tokens de integração sem uso

Ação:

- WordPress: atualização automática do núcleo e dos plugins, remoção de plugins e temas sem uso (mesmo desativados), 2FA nos administradores e /wp-admin restrito por IP quando possível.
- Plugins pagos não atualizam sozinhos sem licença ativa: conferir um a um.

Material elaborado pela Hubsoft para provedores de internet. Pode ser compartilhado na íntegra, com a fonte.

- Se o site tem área do assinante, segunda via ou formulário de contratação, ele trata dado pessoal e precisa do mesmo cuidado de um sistema interno.
- Wiki, chamados, repositórios e painéis internos não precisam estar na internet: VPN ou restrição por IP.
- Conferir quem tem acesso ao registro do domínio e ao DNS, com 2FA. Quem controla o DNS controla o site e o e-mail do provedor.
- Backup do site guardado fora da hospedagem.

19. Câmeras e telefonia IP

Câmeras antigas com firmware defasado seguem sendo invadidas em massa: entre 17/06 e 22/07/2026, a campanha “CameraSwarm” comprometeu mais de 14.500 câmeras Dahua, a maior parte por senhas fracas e o restante por falhas de 2021. Interessa a provedores que vendem ou hospedam monitoramento.

Fabricante	CVE	O que permite	Situação e correção
• EXPLORADA **Dahua (câmeras, NVRs, videoporteiros)**	CVE-2021-33044, CVE-2021-33045 (nota 9,8)	Login sem senha	Exploração ativa em 2026; firmware com build de junho/2021 em diante; desativar P2P se não usar
Dahua	CVE-2026-29115, CVE-2026-29116	Negação de serviço, uma delas sem autenticação	Firmware com build de 26/03/2026 em diante
• EXPLORADA **Hikvision**	CVE-2017-7921, CVE-2021-36260	Burla de autenticação e execução remota de código	Exploração ativa em 2026; atualizar ou substituir modelos sem suporte
Hikvision	CVE-2026-57599; CVE-2026-57600 (nota 7,5)	Escalada de privilégio após login por SSH; vazamento de informação sem autenticação	Firmware indicado pela Hikvision (aviso de julho/2026)
Intelbras VIP 3260 Z IA	CVE-2026-2564	Falha no mecanismo de recuperação de senha (/OutsideCmd)	Afeta o firmware 2.840.00IB005.0.T; conferir com a Intelbras a versão corrigida
Intelbras iNVU 7016 FT	CVE-2026-12211	Leitura de arquivos por path traversal	A Intelbras lançou versão corrigida rapidamente
Intelbras TIP 635G (telefone IP)	CVE-2026-3101	Injeção de comandos por usuário autenticado, com prova de conceito pública	Sem resposta do fabricante segundo o registro da CVE; isolar em VLAN de voz

Plataformas de monitoramento em nuvem integradas ao HubSoft (Monuv, ZeusVision) são operadas pelo fornecedor: confirme com ele a política de atualização.

Ação: câmeras, NVRs e telefones IP nunca com porta redirecionada direto para a internet; acesso remoto só por VPN ou pela nuvem do fabricante; senha única por equipamento.

Material elaborado pela Hubsoft para provedores de internet. Pode ser compartilhado na íntegra, com a fonte.

20. IPTV, TV box e equipamentos de voz

Produto	CVE	Risco	Situação e correção
● EXPLORADA **TV box Android não certificada**	Botnets BadBox 2.0 e Kimwolf	Malware de fábrica, ou instalado pela porta de depuração (ADB, 5555): o aparelho vira proxy e participa de ataques DDoS a partir da rede do provedor	Mais de 10 milhões de aparelhos no BadBox 2.0 e mais de 2 milhões no Kimwolf. Não há correção: usar só aparelhos certificados (Play Protect)
Painéis de IPTV (Stalker Portal/Ministra, Xtream UI)	Senhas padrão e instalações desatualizadas	Tomada do painel e instalação de backdoor	Risco documentado desde 2025: painéis expostos com senha padrão e arquivo de backdoor instalado. Trocar as senhas padrão, atualizar e restringir o painel por IP
Grandstream GXP1600 (GXP1610 a GXP1630)	CVE-2026-2329 (nota 9,3)	Execução de código como root sem login pela interface web, o que permite interceptar chamadas	Firmware 1.0.7.81; há módulo de ataque público

Ação:

- Se o provedor entrega TV box ao assinante, entregar só modelo certificado e manter o firmware pelo ACS.
- Tráfego anormal de saída em um assinante (DDoS, proxy) costuma vir de TV box infectada: orientar a troca do aparelho.
- Telefones IP, ATAs e gateways de voz em VLAN de voz, sem interface web acessível da rede de usuários e com provisionamento por HTTPS.

Material elaborado pela Hubsoft para provedores de internet. Pode ser compartilhado na íntegra, com a fonte.

Parte 6 · Soluções próprias

21. Soluções próprias: Docker, IA e chatbots

Muitos provedores já mantêm soluções desenvolvidas em casa: site ou central em contêineres, automações em n8n, chatbot de WhatsApp, servidor de IA local. Essas ferramentas sobem rápido, muitas vezes seguindo um tutorial, e ficam no ar com a configuração padrão. Em 2026 elas viraram alvo constante, porque guardam no mesmo lugar chaves de API, tokens de WhatsApp e credenciais de outros sistemas.

Contêineres e orquestração

Produto	CVE	Risco	Situação e correção
• EXPLORADA **Docker (API remota)**	Configuração	A API do Docker exposta sem autenticação (porta 2375) permite criar um contêiner privilegiado e assumir o host	Campanhas ativas em 2026 (botnet CARBONATO, que rouba credenciais e chaves de IA e mantém acesso remoto ao host). Nunca expor a 2375; usar o socket local ou TLS com certificado
runc (Docker, containerd, Kubernetes)	CVE-2025-31133, CVE-2025-52565, CVE-2025-52881	Fuga do contêiner para o host com privilégio de root, a partir de imagem ou Dockerfile malicioso	runc 1.2.8, 1.3.3 ou 1.4.0-rc.3 em diante (vem com a atualização do Docker Engine ou do containerd)
NVIDIA Container Toolkit (servidores com GPU)	CVE-2025-23266 (nota 9,0), CVE-2026-24260 (nota 8,5)	Fuga do contêiner para o host	Toolkit 1.19.1 e GPU Operator 26.3.2 ou superiores
Kubernetes ingress-nginx	CVE-2026-4342, CVE-2026-3288, CVE-2026-1580, CVE-2026-24512	Injeção de configuração no nginx, com execução de código e acesso aos segredos do cluster	Corrigidas até a 1.13.9, 1.14.5 e 1.15.1. O projeto foi encerrado em março/2026 e não recebe mais correções: planejar a migração
Redis	CVE-2025-49844, CVE-2026-23479, CVE-2026-81934	Execução remota de código por usuário autenticado. Sem senha configurada, qualquer um que alcança a porta é esse usuário	Usar a última versão da sua linha: 6.2.24, 7.2.16, 7.4.11, 8.2.9, 8.4.6, 8.6.6, 8.8.2 ou 8.10.1 (cobrem até a falha de 28/08/2026). A imagem oficial sobe sem senha: definir senha e não publicar a porta 6379
Docker Engine	CVE-2026-34040 (nota 8,8)	Contorno dos plugins de autorização (AuthZ), permitindo criar contêiner privilegiado; só afeta quem usa plugin AuthZ	Docker Engine 29.3.1 ou superior

Material elaborado pela Hubsoft para provedores de internet. Pode ser compartilhado na íntegra, com a fonte.

Produto	CVE	Risco	Situação e correção
Portainer	CVE-2026-44848, CVE-2026-72533 (nota 8,8), CVE-2026-55761	Usuário de baixo privilégio contorna a autorização e obtém root no host; em instalação nova, qualquer um cria o primeiro administrador nos primeiros minutos	2.45.3 ou superior (2.39.9 na linha LTS anterior); painel só por VPN
Coolify	Onze falhas críticas divulgadas em janeiro/2026 (CVE-2025-66209 a 66213 e outras) e novos avisos até outubro	Injeção de comandos com root no servidor por usuário de baixo privilégio	Usar a versão atual (4.7.6); a release de segurança de 21/10/2026 cobre todas as linhas. Painel só por VPN

Automação, IA e chatbots

Produto	CVE	Risco	Situação e correção
• EXPLORADA **n8n**	CVE-2026-21858 (nota 10), CVE-2025-68613, CVE-2026-27577, CVE-2026-27493	Tomada do servidor sem login por formulários e webhooks públicos; execução de código por quem edita fluxos	Exploração ativa. Versões mínimas no boletim do n8n de 13/11/2026: 1.123.96 ou 2.47.6. Em 24/11/2026 o centro de cibersegurança do Canadá (aviso AV26-1200) listou novas correções do n8n: são afetadas as versões anteriores a 1.123.101, 2.48.8, 2.49.5, 2.50.0 e 3.4.0. Atualizar para uma delas ou superior; o suporte à linha 1.x termina em 31/12/2026
• EXPLORADA **Langflow**	CVE-2026-0768 (nota 9,8), CVE-2026-93680, CVE-2026-110186, CVE-2026-9198 e outras	Execução remota de código sem login; os ataques roubam chaves de IA e de nuvem	Mais de dez falhas exploradas em 2026, segundo a VulnCheck. Usar a 1.13.3 ou superior: a 1.13.0 corrige falhas críticas presentes da 1.0.0 à 1.12.8, e as seguintes trazem novas correções de segurança. Não expor à internet
• EXPLORADA **Flowise**	CVE-2026-69255 e mais de uma dezena de outras, várias críticas; CVE-2026-130796 (nota 8,8)	Execução de comandos no servidor, em alguns casos como root	Projeto descontinuado: congelado em 29/07/2026, arquivado em 13/08 e em fim de vida desde 31/08. A última versão (3.1.4) já tem falhas novas, de 17/11/2026, que não serão corrigidas, e versões antigas são exploradas (CVE-2025-59528). Tirar da internet e planejar a migração

Material elaborado pela Hubsoft para provedores de internet. Pode ser compartilhado na íntegra, com a fonte.

Produto	CVE	Risco	Situação e correção
Dify	CVE-2026-41947, CVE-2026-41948 (nota 9,4) e outras	Acesso a conversas, documentos e APIs internas, parte sem login	A 1.14.2 corrige só parte; a CVE-2026-41948 exige a 1.15.0. Usar a versão atual
Ollama	CVE-2026-7482 (nota 9,1)	Vazamento da memória do servidor sem login (prompts, chaves, dados)	Corrigida na 0.17.1, mas há falhas remotas mais novas (CVE-2026-108836 e CVE-2026-86289): usar a 0.34.2 ou superior. O Ollama não tem autenticação própria e cerca de 300 mil servidores estavam expostos na divulgação. Nunca publicar a porta 11434
Open WebUI	Mais de 50 avisos entre julho e setembro/2026	Falhas de controle de acesso entre usuários, modelos e arquivos	Manter na última versão e desligar o cadastro aberto
• EXPLORADA **LiteLLM**	CVE-2026-42208, CVE-2026-42271, CVE-2026-59822, CVE-2026-40217; CVE-2026-114612 (nota 9,9)	Leitura sem login do banco que guarda as chaves de todos os modelos; execução de comandos; burla de autenticação no MCP; usuário interno forja credencial de administrador	As quatro primeiras estão no catálogo de exploradas da CISA; a CVE-2026-40217 (execução de código pelo endpoint /guardrails/test_custom_code, corrigida na 1.83.10) entrou em 18/11/2026. Usar a 1.100.4 ou superior (nas linhas seguintes: 1.101.3, 1.102.2, 1.103.1 ou 1.104.0); a 1.84.0 é o piso para as quatro exploradas. Não usar a master key de exemplo dos tutoriais. As versões 1.82.7 e 1.82.8 foram publicadas adulteradas no PyPI: tratar como comprometidas
• EXPLORADA **vLLM, FastAPI e servidores MCP em Python**	CVE-2026-48710 ("BadHost", no Starlette); CVE-2026-22778 (vLLM, nota 9,8)	Burla de autenticação baseada em caminho; execução remota de código sem login pelo endpoint multimodal do vLLM	A BadHost tem exploração ativa (catálogo da CISA, 02/09/2026): Starlette 1.0.1 ou superior. vLLM 0.14.1 ou superior
Typebot	CVE-2026-62862 (crítica), CVE-2026-39969, CVE-2026-48768	Tomada de conta sem login pelo código de acesso enviado por e-mail; o webhook do WhatsApp aceita mensagens forjadas; geração de URL de upload sem login	3.19.1 ou superior
Chatwoot	CVE-2026-63765,	Envio de arquivos sem login	A 4.16.0 corrige a 63765; a 4990

Material elaborado pela Hubsoft para provedores de internet. Pode ser compartilhado na íntegra, com a fonte.

Produto	CVE	Risco	Situação e correção
	CVE-2026-4990	para qualquer conta; falha de autorização no cadastro	não tem correção documentada (desligar o cadastro aberto). Usar a versão atual (4.20.0): as versões seguintes à 4.16.0 trazem novas correções de segurança
• SEM CORREÇÃO **Evolution API**	CVE-2026-91997	Endpoint /metrics acessível sem autenticação, expondo dados do servidor	Afeta até a 2.3.7, que é a última versão estável, e não há correção publicada: bloquear /metrics no proxy
WPPConnect Server	CVE-2026-121557 (nota 8,2)	Qualquer pessoa pode enviar mensagens pela sessão de WhatsApp conectada (rota /api/:session/chatwoot sem autenticação)	Afeta até a 2.10.74; corrigida na 2.10.75 (04/11/2026). Atualizar e não expor a API

Aplicações próprias e pipeline

Produto	CVE	Risco	Situação e correção
Next.js e React Server Components	CVE-2026-126187, CVE-2026-96889	Execução de código no servidor sem login (App Router com Cache Components; otimização de imagens com SVG)	Next.js 16.4.5 ou 15.5.29 (rodada de segurança de 03/11/2026); pacotes react-server-dom 19.0.9, 19.1.10, 19.2.9 ou 19.3.1; biblioteca sharp 0.35.5 ou superior. Atualizar só o React não corrige o Next.js
• EXPLORADA **GitLab (auto-hospedado)**	CVE-2026-110264, CVE-2026-85706, CVE-2026-97229, CVE-2026-105437	Execução de código e leitura de arquivos do servidor sem login; quatro falhas críticas em dois meses	A CVE-2026-85706 tem exploração ativa (catálogo da CISA, 11/09/2026). Em 20/11/2026 saíram a 19.6.1, a 19.5.8 e a 19.4.10, que trocam o Ruby embutido e fecham o Ruby2Shell: usar uma delas (a linha 19.3 ficou sem essa correção). Segundo a imprensa especializada, o nginx embutido nesses pacotes ainda não trazia a correção do nginx2root
Pacotes npm e PyPI	Campanhas "Shai-Hulud" de 2026	Pacotes legítimos adulterados roubam tokens e chaves da máquina do desenvolvedor e do pipeline	Fixar versões (lockfile), não levar versão recém-publicada direto para produção e trocar as chaves se um pacote afetado foi instalado

Material elaborado pela Hubsoft para provedores de internet. Pode ser compartilhado na íntegra, com a fonte.

Ação:

- Nenhum painel dessas ferramentas deve ficar aberto para a internet. n8n, Langflow, Flowise, Dify, Open WebUI, Portainer e afins: só por VPN ou IP liberado. Para fora, apenas o webhook ou a página estritamente necessária, atrás de proxy com HTTPS.
- No Docker, conferir o que está publicado (`docker ps` mostra as portas). Porta publicada em 0.0.0.0 costuma passar por fora do firewall do host (ufw); publicar em 127.0.0.1 e expor pelo proxy.
- Trocar toda senha e chave padrão dos tutoriais (banco, Redis, master key, usuário admin) antes de colocar em produção.
- Chaves de API (provedores de IA, Meta/WhatsApp, gateway de pagamento) fora do código e do repositório, com limite de gasto configurado no fornecedor.
- Chatbot com IA ligado a sistemas internos: dar a ele só as permissões que um atendente de primeiro nível teria. O texto enviado pelo assinante pode conter instruções para a IA (injeção de prompt); o que protege é o limite de permissão, não o prompt.
- Integração com o HubSoft pela API oficial, com um usuário criado só para a integração, o mínimo de permissões e as credenciais guardadas fora do código.
- Atualização com rotina: essas ferramentas publicam correções de segurança a cada duas semanas ou menos. Definir um responsável e uma data fixa.
- Manter uma lista simples de cada solução interna: onde roda, quem cuida e que credenciais guarda.

Material elaborado pela Hubsoft para provedores de internet. Pode ser compartilhado na íntegra, com a fonte.

Parte 7 · Sem correção, checklist e fontes

22. Falhas divulgadas sem correção disponível

Os itens abaixo não tinham correção do fabricante até 24/11/2026, ou atingem versões que não serão mais corrigidas. Para eles, a proteção depende de mitigação e isolamento.

Item	Falha	Por que não há correção	O que fazer agora
OLT V-SOL série 1600 e Cloud EMS	Comandos sem login por SNMP e web; envio de arquivo sem autenticação no EMS	O artigo da Quarkslab não aponta firmware corrigido	Gerência isolada; trocar senhas e communities; cobrar o fabricante
Kernel Linux (SCTP)	Escalada para root, encadeada com o nginx2root	Presente desde o kernel 4.15 (2018); sem CVE confirmada e sem correção até 24/11/2026; os autores da pesquisa esperam o patch para as próximas semanas	Em servidores que não usam SCTP: criar /etc/modprobe.d/sctp.conf com a linha install sctp /bin/false
FreeRADIUS	CVE-2026-127030, 127029	Pacote do Debian ainda sem correção	Desabilitar EAP-FAST e EAP-SIM se não forem usados
Zyxel CPEs DSL legados	CVE-2024-40890, 40891, CVE-2025-0890	Fim de vida; a Zyxel declarou que não vai corrigir	Substituir; enquanto isso, bloquear Telnet e web pela WAN
Proxmox VE 7	PSA-2026-00043 (CVE-2023-54391): login como root sem senha pela API; exploração ativa	Versão fora de suporte	Migrar para o Proxmox VE 9. Até lá: porta 8006 só por VPN, 2FA em todas as contas e o patch paliativo da Proxmox
VMware vCenter 7.0	CVE-2026-123890: burla de autenticação sem login, com exploração ativa	Série sem correção pública; a Broadcom só atende quem tem contrato de suporte estendido	Migrar para o 8.0 U3m ou o 9.x. Até lá: vCenter isolado em rede de gerência, sem acesso a partir da rede dos usuários
Ruby 3.2 e anteriores	CVE-2026-132825 (Ruby2Shell)	Séries fora de suporte não recebem correção	Migrar para 3.3.14, 3.4.13 ou 4.0.10
PHP de séries fora de suporte	PHP2Shell (afeta do PHP 5.4 em diante)	Releases oficiais só para as séries 8.2 a 8.5; para 7.4, 8.0 e 8.1 há apenas patch de código-fonte	Migrar para uma série suportada; usar pacote com backport da distribuição, se houver
Tenda HG9, HG3, HG10, G103	CVE-2026-2907, 7096, 86167 e 5339:	Registros das CVEs sem resposta do fabricante nem	Trocar a senha de fábrica; bloquear a gerência pela WAN;

Material elaborado pela Hubsoft para provedores de internet. Pode ser compartilhado na íntegra, com a fonte.

Item	Falha	Por que não há correção	O que fazer agora
	estouro de buffer e injeção de comandos pela interface web, por usuário autenticado; exploits públicos	firmware corrigido	planejar a troca
Cambium ePMP Force 300-25 (4.7.0.1)	CVE-2023-6691: usuário local com credencial vira root (não explorável remotamente, segundo a CISA)	O fabricante não respondeu à CISA	Gerência isolada; trocar as contas de fábrica; consultar o suporte da Cambium
Intelbras TIP 635G	CVE-2026-3101	Sem resposta do fabricante segundo o registro da CVE	Isolar em VLAN de voz; restringir a interface web
GenieACS 1.2.13	CVE-2025-56015	Versão corrigida não identificada nas fontes	Fechar a NBI no firewall

Nos sistemas internos e nas soluções próprias:

Item	Falha	Por que não há correção	O que fazer agora
Evolution API (até a 2.3.7)	CVE-2026-91997: endpoint /metrics acessível sem autenticação	A 2.3.7 é a última versão estável e o defeito continua no código, inclusive nas pré-versões 2.4.0	Bloquear /metrics no proxy; não expor a API
Kubernetes ingress-nginx	Falhas novas de injeção de configuração	Projeto encerrado em março/2026; o Kubernetes não publica mais correções	Migrar para outro controlador de entrada
Exchange e SharePoint 2016 e 2019	Qualquer falha nova	Fora de suporte (Exchange desde 14/10/2025, SharePoint desde 14/07/2026)	Migrar; até lá, não expor à internet
Windows 10 sem ESU e Windows Server 2012	Qualquer falha nova	Fora de suporte	Atualizar o sistema ou trocar a máquina; não usar para acessar sistemas da empresa
Flowise	CVE-2026-130796 (sem login, nota 8,8) e CVE-2026-130615, de 17/11/2026	Projeto arquivado em 13/08/2026 e em fim de vida desde 31/08; a 3.1.4 é a última versão	Tirar da internet e migrar para outra ferramenta
Windows 11 24H2 (Home e Pro) e Office 2021	Qualquer falha nova	Fora de suporte desde 13/10/2026	Atualizar o Windows para a 25H2 ou superior; trocar o Office 2021 por versão com suporte

No datacenter e nas ferramentas de operação:

Material elaborado pela Hubsoft para provedores de internet. Pode ser compartilhado na íntegra, com a fonte.

Item	Falha	Por que não há correção	O que fazer agora
IPMI 2.0 (iLO, iDRAC, Supermicro)	CVE-2013-4786: o protocolo entrega o hash da senha	Falha de projeto do protocolo	Desativar IPMI sobre LAN; gerência em VLAN isolada
Placa de rede de nobreak Minuteman 1.60.3	Comandos como root sem login	CVE-2026-88560 (nota 9,8), divulgada em 31/08/2026 com prova de conceito pública; sem correção conhecida	Tirar a placa de qualquer rede exposta
NetBox (até a 4.7.6)	CVE-2026-86175: senhas de Git e S3 pela API	Divulgada em 05/09/2026; segue sem correção até a 4.7.6, de 24/11/2026 (as notas de versão não registram correção)	Restringir quem tem usuário; trocar as credenciais guardadas
Cacti	CVE-2026-71287 (nota 8,8)	Sem correção publicada; o projeto Cacti contesta a validade da CVE	Cacti fora da internet; acompanhar o projeto
Impressoras Brother e outras marcas	CVE-2024-51978: senha de fábrica calculável	Não é totalmente corrigível por firmware	Trocar a senha de administrador
TV box Android não certificada	Malware de fábrica (BadBox 2.0)	O fabricante não atualiza	Substituir por modelo certificado

Três sinais de que um equipamento entrou nessa categoria: o fabricante não publica firmware há mais de um ano, o modelo saiu da lista de suporte, ou a falha foi publicada por pesquisadores sem resposta do fabricante. Nesses casos, o equipamento deve sair de qualquer rede exposta.

23. Checklist para o responsável técnico

Roteiro em ordem de prioridade. Marque cada item conforme concluir.

Hoje

- ☐ Conferir se alguma gerência está aberta para a internet (Winbox, SSH, Telnet, web, SNMP, NBI do ACS, painel do hypervisor) e fechar.
- ☐ MikroTik: todos em 6.49.23, 7.24.6 ou 7.25.1, ou superior.
- ☐ Servidores Linux: nginx 1.30.8 ou 1.31.10 (reiniciando o serviço), PHP 8.2.36, 8.3.37, 8.4.28 ou 8.5.13, Brotli atualizado e kernel atualizado com reboot.
- ☐ Servidores que não usam SCTP: bloquear o carregamento do módulo sctp.
- ☐ GenieACS: porta da NBI liberada só para os IPs necessários.
- ☐ OLT V-SOL: gerência isolada, senha do admin e communities SNMP trocadas.
- ☐ Webmail e e-mail: Roundcube 1.6.21 ou 1.7.6; Zimbra 10.1.20.
- ☐ Estações: Chrome 157.0.8103.50 ou superior e atualização de novembro do Windows e do Office

Material elaborado pela Hubsoft para provedores de internet. Pode ser compartilhado na íntegra, com a fonte.

instaladas, com reinício.

- [ ] Site: WordPress e plugins atualizados, com conferência dos usuários administradores.
- [ ] Conferir se há painel de n8n, Langflow, Flowise, Dify, Open WebUI, Ollama, Redis ou a API do Docker (2375) aberto para a internet e fechar.
- [ ] ScreenConnect com cliente 26.6.5 ou superior e appliances de VPN (SonicWall, Ivanti, NetScaler, Check Point, GlobalProtect) na versão mínima indicada na seção de acesso remoto.
- [ ] Conferir se BMC (iLO, iDRAC, IPMI), nobreak, NAS ou painel de hospedagem está acessível pela internet e fechar.
- [ ] cPanel/WHM na última build da linha e Synology DSM atualizado.
- [ ] Alpine Linux (contêineres e VMs): pacote openssh atualizado e sshd reiniciado.
- [ ] Firewalls e gateways de e-mail (SonicWall, Barracuda, FortiMail, Cisco ASA/FTD, Check Point): conferir as falhas exploradas de outubro e novembro.

Nesta semana

- [ ] Ubiquiti: UniFi OS 5.1.31 e UniFi Access 4.3.24 ou superiores, com as demais aplicações atualizadas; airMAX M em 6.3.26 e demais rádios e bridges no firmware atual.
- [ ] Switches Zyxel GS1900 com o firmware Patch 3 (outubro/2026) ou posterior.
- [ ] VMware (vCenter 8.0 U3m, 9.0.2.0200 ou 9.1.1.0200, e ESXi) e Proxmox atualizados; Proxmox VE 7 e 8 com migração para o 9 agendada.
- [ ] Fortinet atualizado; FortiCloud SSO desativado se não for usado.
- [ ] FreePBX e Asterisk atualizados, com painel administrativo fora da internet.
- [ ] Java dos serviços próprios (Keycloak, Jenkins e similares) e Ruby atualizados.
- [ ] Celulares de trabalho atualizados (Android com patch 2026-11-01, iOS 27.2.1 ou 26.7.3) e confirmação em duas etapas no WhatsApp da empresa.
- [ ] n8n, Langflow, Dify, LiteLLM, Typebot, Chatwoot e WPPConnect nas versões corrigidas (o Flowise foi descontinuado: planejar a troca), com senhas e chaves padrão trocadas.
- [ ] Jira, Confluence, Bitbucket e GitLab auto-hospedados atualizados; ERP de backoffice (SAP, TOTVS, Sankhya) com as correções do fabricante e sem acesso direto pela internet.
- [ ] Veeam atualizado, servidor de backup fora do domínio e uma cópia offline ou imutável.
- [ ] Levantamento das ferramentas de acesso remoto instaladas nas máquinas, removendo as sem uso.
- [ ] OPNsense 26.7.8, pfSense Plus 26.07.1 ou CE 2.9.1, F5, SonicWall e WatchGuard atualizados.
- [ ] FRR 10.6.2, Unbound 1.26.2, PowerDNS Recursor 5.3.12 ou 5.4.8; accel-ppp e VyOS atualizados.
- [ ] Exim 4.99.3, Dovecot 2.4.5 e MariaDB na versão corrigida da série.
- [ ] SharePoint com a atualização de agosto/2026 ou posterior; Exchange 2016 e 2019 com plano de migração.
- [ ] Cisco SD-WAN, HPE Aruba e Citrix NetScaler nas versões corrigidas.
- [ ] Plesk, Portainer e Coolify atualizados; Evolution API com o /metrics bloqueado no proxy.

Neste mês

Material elaborado pela Hubsoft para provedores de internet. Pode ser compartilhado na íntegra, com a fonte.

- [ ] Juniper com os boletins de outubro/2026 aplicados e J-Web desativado; Cisco na release corrigida.
- [ ] Zabbix, Grafana, LibreNMS, Wazuh, BIND e FreeRADIUS na última versão da série.
- [ ] Firmware dos equipamentos de assinante atualizado pelo ACS; gerência pela WAN bloqueada.
- [ ] Câmeras e NVRs atualizados e sem porta redirecionada.
- [ ] Lista dos equipamentos fora de suporte, com plano de troca.
- [ ] Plano de saída para o que está fora de suporte: Windows 10 sem ESU, Windows Server 2012 e 2016, Exchange e SharePoint 2016 e 2019, ingress-nginx.
- [ ] Lista das soluções internas (onde roda, quem cuida, que credenciais guarda) e rotina quinzenal de atualização.
- [ ] Next.js, React e dependências npm e PyPI revisados; chaves de API fora do código e do repositório.
- [ ] Senha de fábrica trocada em BMCs, placas de nobreak e impressoras.
- [ ] NetBox, Cacti, Nagios e Vaultwarden atualizados e fora da internet.
- [ ] Microsoft 365 ou Google Workspace com 2FA para todas as contas; SPF, DKIM e DMARC no domínio.
- [ ] Telefones Grandstream GXP1600 no firmware 1.0.7.81 e telefonia em VLAN de voz.

Sempre

- [ ] Senhas únicas e 2FA em todos os painéis; usuários de ex-funcionários desativados.
- [ ] Backup testado e guardado fora do equipamento ou servidor de origem.
- [ ] Alguém responsável por acompanhar os boletins de segurança dos fabricantes usados na rede.

24. Fontes e limites deste levantamento

Este boletim é um ponto de partida, não uma lista completa: retrata o que estava público em 24/11/2026 e deve ser conferido contra o boletim oficial de cada fabricante antes de qualquer atualização.

Limites

- A ausência de CVE pública para um equipamento não significa que ele seja seguro. Vários fabricantes de OLT e CPE não publicam boletins.
- Para os fabricantes de menor porte (BDCom, C-Data, Hioso, HSGQ, Phyhome, Chima, GigaTelco, Think, Cianet, Digistar, Furukawa, Raisecom, Zhone, Parks, Datacom, Deliberant), para accel-ppp, Bequant, pfSense/OPNsense e para os ACS comerciais, a pesquisa não foi exaustiva.
- Versões corrigidas variam por modelo de hardware e por distribuição Linux. Pacotes de distribuição podem trazer a correção com o número de versão antigo.
- A situação de exploração muda rápido: uma falha sem exploração conhecida hoje pode passar a ser explorada em dias.
- Atualize sempre em janela de manutenção, com backup da configuração e plano de retorno.
- Para estações, celulares, ferramentas internas e soluções próprias, o boletim traz apenas o que tem exploração real ou gravidade crítica. Ele não substitui a atualização contínua de cada sistema.
- Para A10, BIRD, validadores RPKI, Wanguard, ntopng, switches de outras marcas (Huawei,

Material elaborado pela Hubsoft para provedores de internet. Pode ser compartilhado na íntegra, com a fonte.

Datacom, Extreme), Flussonic, Wowza, Yealink, Khomp, Oxidized, AWX, PRTG, Bitwarden, Passbolt, KeePass, Webmin, CyberPanel, phpMyAdmin e MySQL, a pesquisa não trouxe falha crítica ou explorada em 2026. Isso não quer dizer que estejam livres de falhas: valem as regras gerais e o boletim do fabricante.

- Atualização de 24/11/2026: entraram as correções e as falhas divulgadas de 19 a 24/11/2026, conferidas no catálogo da CISA de 23/11 e nos avisos dos fabricantes. As versões do n8n e do proxmox-kernel para os itens novos vêm de fonte secundária (aviso do centro de cibersegurança do Canadá e fórum da Proxmox). Revisão de 19/11/2026: cada linha foi reconferida contra o aviso do fabricante ou o registro da CVE. Em quatro casos a página do fabricante não abriu e a versão indicada vem de fonte secundária: HPE Aruba, Ivanti Connect Secure, SonicWall SonicOS e Juniper. Confirme no portal do fabricante antes de atualizar.
- Várias versões mínimas mudaram em outubro e novembro/2026 (MikroTik, PHP, cPanel, NetScaler, n8n, entre outras). Confira sempre se já existe versão mais nova que a indicada aqui.

Fontes principais

- MikroTik: CERT Polska
- nginx: Xint, nginx2root e Tenable
- PHP: php.net, avisos de 2026 e oss-security
- Juniper: resumo dos boletins de outubro/2026
- Cisco: advisory de hardening do IOS XE
- OLT V-SOL: Quarkslab
- Ubiquiti: Censys, boletim 067 e CSA Singapura, boletim 064
- Zyxel: SecurityWeek, GS1900 e avisos da Zyxel
- TP-Link: central de avisos de segurança
- GenieACS: NVD, CVE-2025-56015
- Kernel Linux: The Hacker News, Copy Fail e BleepingComputer, Fragnesia
- Proxmox: avisos de segurança do Proxmox VE
- VMware: BleepingComputer, vCenter
- Fortinet: Rapid7
- Roundcube e Zimbra: The Hacker News e SecurityWeek
- FreePBX: Security Affairs
- Zabbix, Grafana e BIND: Zabbix, Grafana e ISC
- Câmeras: The Hacker News, CameraSwarm
- Java4Shell e Ruby2Shell: Qualys e Aikido
- Catálogo de falhas exploradas: CISA KEV
- Estações, celulares, VPN, servidores Windows e backup: avisos dos fabricantes, catálogo CISA KEV e imprensa especializada
- Firefox e WinRAR: Mozilla, MFSA 2026-67 e Google Threat Intelligence
- WordPress: BleepingComputer
- Atlassian: The Hacker News

Material elaborado pela Hubsoft para provedores de internet. Pode ser compartilhado na íntegra, com a fonte.

- Docker e Redis: CSA Singapura, CARBONATO e The Hacker News, Redis
- Kubernetes ingress-nginx: oss-security
- n8n: boletim de segurança de 28/10/2026
- Langflow e Flowise: Cloud Security Alliance e NVD, CVE-2026-69255
- Ollama, LiteLLM e Dify: The Hacker News, Ollama, Help Net Security, LiteLLM e Security Affairs, Dify
- Typebot, Chatwoot, Evolution API e WPPConnect: INCIBE-CERT e VulnCheck
- Next.js e GitLab: Cloudflare Radar e notas de patch do GitLab
- LibreNMS e Wazuh: Tenable e Heise
- accel-ppp, VyOS e FRRouting: VyOS e rastreador do Debian
- F5 BIG-IP: CIS
- DNS recursivo: Safeguard, Unbound e PowerDNS
- Gerência de servidor (BMC): The Hacker News e runZero
- Synology: Security Affairs
- Nobreaks: Full Disclosure, Minuteman
- OPNsense e pfSense: Action1 e Netgate
- SonicWall e Omada: CyberScoop e aviso da Omada
- Impressoras: Dark Reading
- cPanel: Help Net Security e The Hacker News
- Exim e MariaDB: The Hacker News e Action1
- TV box e Grandstream: Krebs on Security e Rapid7
- NetBox: VulnCheck
- Revisão de 19/11/2026, fontes primárias: avisos da MikroTik, boletins da Ubiquiti, nginx, changelog do PHP, catálogo da CISA (espelho oficial) e rastreador de segurança do Debian
- VPN e borda: SonicWall SMA 1000, Citrix, boletim de 12/11/2026, Check Point, Rapid7, Ivanti, Palo Alto e pfSense
- Microsoft, Apple e backup: ciclo de vida da Microsoft, blog do Exchange, atualizações de segurança da Apple e Veeam
- Soluções próprias: n8n, boletim de 13/11/2026, Flowise, aviso de descontinuação, Next.js e Redis
- Datacenter e hospedagem: Synology, SecurityWeek, HPE Aruba e Proxmox

Dúvidas sobre este boletim: envie um e-mail para **security@hubsoft.com.br**.

Material elaborado pela Hubsoft para provedores de internet. Pode ser compartilhado na íntegra, com a fonte.