

Your IT Company

Principais Vulnerabilidades e Ameaças (novembro/26)

Sumário

1. Objetivo 2
2. Vulnerabilidades e Ameaças descobertas 2
2.1. Campanha utiliza falsas notificações judiciais para distribuir o malware XWorm 2
2.2. CISA alerta para exploração ativa de vulnerabilidade de execução de código no WordPress Core 4
2.3. Vulnerabilidade de cinco anos no kernel Linux permite elevação de privilégios para root 5
2.4. Falha no APT de Debian e Ubuntu permite ataques Man-in-the-Middle e execução como root 6
2.5. Grupo associado ao APT29 sequestra script de análise web para distribuir exploits contra iOS e Android 8
2.6. Vulnerabilidade zero-day no Cisco Secure Firewall é explorada para provocar reinicialização de dispositivos VPN 10

1. Objetivo

Este documento foi desenvolvido e fundamentado nas documentações oficiais do NIST (National Institute Of Standards and Technology), MITRE e CVE.org, que são mundialmente conhecidas na área de cibersegurança como modelos de padronização das melhores práticas de segurança, pesquisa de metodologias de ataques, defesa cibernética e catalogação de novas vulnerabilidades em sistemas operacionais e aplicações.

2. Vulnerabilidades e Ameaças descobertas

2.1. Campanha utiliza falsas notificações judiciais para distribuir o malware XWorm

Uma campanha de phishing identificada em outubro de 2026 tem como alvo organizações colombianas por meio de e-mails em espanhol que simulam notificações judiciais e documentos administrativos. Os anexos contêm scripts maliciosos em JavaScript ou VBScript, distribuídos individualmente ou em arquivos ZIP, para instalar o XWorm, um trojan de acesso remoto (RAT) que permite aos operadores controlarem sistemas Windows comprometidos. A pesquisa também identificou reutilização de infraestrutura e ferramentas observadas em campanhas anteriores.

Exploração

A infecção começa quando a vítima abre um anexo com aparência de documento oficial. O script executa comandos PowerShell ocultos e ofuscados, utilizando decodificação Base93 e camadas de criptografia. Em seguida, baixa componentes de serviços públicos de hospedagem, extrai uma biblioteca .NET denominada RSG_UnityApp e injeta o XWorm no processo legítimo RegAsm.exe. O malware contata servidores de comando e controle (C2), coleta informações do dispositivo e recebe comandos remotamente.

- Uso de arquivos .js e .vbs com nomes associados a notificações e processos judiciais.
- Execução encadeada de wscript.exe ou cscript.exe para iniciar PowerShell com parâmetros ocultos ou codificados.
- Descompactação e carregamento da DLL RSG_UnityApp e do payload XWorm.
- Injeção do malware no processo legítimo RegAsm.exe para mascarar sua atividade.
- Comunicação com servidores C2 utilizando tráfego criptografado com AES-128-ECB.

Impacto

- Controle remoto do computador infectado e execução de comandos arbitrários.
- Captura de tela, gerenciamento de arquivos, carregamento de plugins e coleta de informações sensíveis.

Classificação: Público

- Coleta de nome de usuário, características do sistema, hardware, status do antivírus e presença de webcam.
- Possível uso do equipamento para atividades como DDoS e apoio a outras etapas da intrusão.
- Comprometimento da confidencialidade e integridade dos dados, com risco de interrupção das atividades.

Mitigação e Prevenção

- **Recomendações imediatas:**
  - Isolar estações com execução suspeita de scripts ou comunicação com os indicadores listados, preservando evidências.
  - Bloquear domínios, IPs e URLs identificados em DNS, proxy e firewall, após validação no ambiente.
  - Pesquisar nos logs a cadeia wscript.exe/cscript.exe powershell.exe RegAsm.exe, especialmente com comandos ocultos ou codificados.
  - Verificar downloads recentes de arquivos .js, .vbs, .zip e DLLs provenientes de serviços de hospedagem não usuais.
  - Executar varredura completa nos endpoints suspeitos e avaliar redefinição de credenciais.

- **Recomendações para Administradores de Sistema:**
  - Implementar detecção comportamental para scripts, PowerShell ofuscado, injeção de processos e conexões originadas por RegAsm.exe.
  - Restringir Windows Script Host quando desnecessário e aplicar controle de aplicações.
  - Configurar EDR para registrar criação de processos, carregamento de DLLs e conexões de rede.
  - Aplicar filtragem de e-mail e sandboxing de anexos; bloquear scripts recebidos de fontes externas quando possível.
  - Manter sistemas operacionais e soluções de segurança atualizados.

- **Recomendações para usuários finais:**
  - Não abrir anexos inesperados que simulem intimações, notificações judiciais ou documentos administrativos.
  - Confirmar comunicações judiciais diretamente nos canais oficiais.
  - Não executar arquivos .js, .vbs ou scripts recebidos por e-mail, mesmo compactados.
  - Comunicar mensagens suspeitas ou abertura acidental de anexos à equipe de TI.

Para saber informações mais detalhadas sobre esta vulnerabilidade acesse: https://cybersecuritynews.com/xworm-malware-3/

2.2. CISA alerta para exploração ativa de vulnerabilidade de execução de código no WordPress Core

A CISA adicionou a CVE-2026-119977 ao catálogo Known Exploited Vulnerabilities (KEV) em 3 de novembro de 2026, após evidências de exploração ativa. A falha, com CVSS 8.1, afeta versões do WordPress entre as ramificações 4.7 e 7.1.3 e pode permitir execução de código PHP no servidor sem autenticação durante uma janela específica do processo de atualização do núcleo. A versão WordPress 7.1.4, lançada em 28 de outubro de 2026, corrige o problema.

Exploração

A vulnerabilidade decorre de uma condição de corrida time-of-check to time-of-use (TOCTOU, CWE-367). Durante uma atualização completa, arquivos são extraídos em diretórios temporários previsíveis dentro de wp-content/upgrade. Se esses diretórios estiverem acessíveis publicamente e permitirem execução de PHP, um atacante pode acessar o setup-config.php temporário antes que a atualização finalize e remova os arquivos. A exploração depende da coincidência com essa janela.

Impacto

- Execução remota de código PHP no servidor web sem credenciais válidas.
- Possível comprometimento do site, da aplicação e dos dados armazenados.
- Criação de contas administrativas, instalação de código malicioso ou alteração de conteúdo, conforme o nível de controle obtido.
- Uso do servidor comprometido como ponto de apoio para outras atividades maliciosas.
- Indisponibilidade, danos reputacionais e necessidade de investigação forense.

Mitigação e Prevenção

- **Recomendações imediatas:**
  - Atualizar imediatamente para WordPress 7.1.4 ou versão corrigida/backport da ramificação utilizada.
  - Confirmar manualmente a versão instalada e se a atualização automática foi concluída.
  - Revisar logs durante atualizações recentes, procurando requisições a wp-content/upgrade e setup-config.php.
  - Verificar arquivos PHP desconhecidos, novas contas administrativas e alterações inesperadas em plugins, temas e arquivos centrais.
  - Preservar logs e iniciar análise forense se houver indícios de exploração.

- **Recomendações para Administradores de Sistema:**
  - Manter WordPress Core, plugins, temas e componentes do servidor atualizados.
  - Impedir acesso HTTP público aos diretórios temporários de atualização e desabilitar execução de PHP em diretórios de upload/staging quando aplicável.

Classificação: Público

- Aplicar regras de WAF para identificar acessos indevidos a caminhos temporários e arquivos de instalação.
- Revisar permissões de arquivos e diretórios e monitorar a integridade dos arquivos do WordPress.
- Manter backups offline ou imutáveis e testar a restauração regularmente.

- **Recomendações para usuários finais:**
  - Visitantes comuns não possuem ação técnica específica; administradores de sites devem solicitar confirmação da atualização à equipe responsável.
  - Reportar redirecionamentos, páginas alteradas ou comportamentos suspeitos.

IoCs e artefatos

- Caminho temporário: wp-content/upgrade/.
- Arquivo envolvido: setup-config.php.

Para saber informações mais detalhadas sobre esta ameaça acesse: https://gbhackers.com/cisa-warns-of-wordpress-core-code-execution-vulnerability/

2.3. Vulnerabilidade de cinco anos no kernel Linux permite elevação de privilégios para root

A CVE-2026-31695 é uma vulnerabilidade use-after-free (CWE-416) no driver virt_wifi do kernel Linux. O problema permaneceu no código por quase cinco anos e pode permitir que um usuário local sem privilégios obtenha controle root. Pesquisadores publicaram uma exploração funcional contra uma instalação padrão do Fedora 44 Server x86_64, aumentando o risco para ambientes que executam código local não confiável.

Exploração

A falha está no gerenciamento de dispositivos de rede virtuais. Durante a remoção de um dispositivo virt_wifi, a desmontagem pode ocorrer simultaneamente à liberação do dispositivo inferior associado, deixando dev.parent apontando para memória já liberada. Uma operação posterior do ethtool alcança o ponteiro inválido. A pesquisa demonstra como estabilizar a condição de corrida e utilizar uma estrutura struct device forjada para contornar proteções do kernel e alcançar privilégios elevados.

Impacto

- Elevação de privilégios de uma conta local de baixo privilégio para root.
- Comprometimento da confidencialidade, integridade e disponibilidade do sistema.
- Contorno de controles de isolamento em servidores multiusuário, ambientes de CI, hospedagem compartilhada e hosts de containers.
- Facilitação de movimentação lateral ou instalação de ferramentas persistentes após acesso inicial.

- Risco ampliado pela existência de exploit público funcional.

Mitigação e Prevenção

- **Recomendações imediatas:**
  - Identificar a versão do kernel em execução e verificar a presença do módulo virt_wifi.
  - Priorizar hosts que executam código local não confiável, ambientes multiusuários, runners de CI e hosts de containers.
  - Aplicar kernel corrigido ou backport fornecido pela distribuição.
  - Quando o driver não for necessário, avaliar seu bloqueio temporário conforme procedimentos de mudança e compatibilidade.
  - Monitorar criação/remoção repetida de dispositivos virtuais e atividade incomum do ethtool.

- **Recomendações para Administradores de Sistema:**
  - Atualizar para kernels corrigidos 5.15.203, 6.1.168, 6.6.134, 6.12.81, 6.18.22 e 6.19.12, ou backports oficiais equivalentes.
  - No Amazon Linux 2023, aplicar ALAS2023-2026-1681 e ALAS2023-2026-1746; a publicação indica Amazon Linux 2 como não afetado.
  - Verificar o kernel ativo com uname -r e a presença do módulo com lsmod | grep virt_wifi.
  - Se não necessário, avaliar blacklist para virt_wifi e remoção controlada do módulo.
  - Reiniciar quando necessário e confirmar que o kernel corrigido está em execução.
  - Reduzir execução de código não confiável em hosts compartilhados e reforçar isolamento de usuários, containers e workloads.

- **Recomendações para usuários finais:**
  - Evitar executar scripts, binários ou ferramentas não confiáveis em sistemas Linux compartilhados.
  - Manter a estação atualizada por meio dos repositórios oficiais.
  - Comunicar comportamentos anormais ou solicitações inesperadas de privilégios à equipe de TI.

IoCs e artefatos

- Referências técnicas: netdev_run_todo(), ethnl_ops_begin(), pm_runtime_get_sync(dev->dev.parent) e SET_NETDEV_DEV (dev, &priv->lowerdev->dev).

Para saber informações mais detalhadas sobre esta ameaça acesse: https://gbhackers.com/5-year-old-linux-kernel-vulnerability/

2.4. Falha no APT de Debian e Ubuntu permite ataques Man-in-the-Middle e execução como root

Uma vulnerabilidade no APT (Advanced Package Tool), gerenciador de pacotes de Debian e Ubuntu, permite que um atacante capaz de modificar downloads substitua um pacote verificado

por um pacote malicioso. Identificada como CVE-2026-109518, recebeu prioridade alta no Ubuntu, com CVSS 4.0 de 7.7. O risco é especialmente relevante em Debian 12 ou posterior e Ubuntu 22.04 ou posterior, nos quais a repetição automática de downloads com falha está habilitada por padrão.

Exploração

O ataque exige que o invasor consiga interferir no tráfego entre o APT e o servidor de pacotes, por exemplo, por meio de proxy ou mirror malicioso. O atacante utiliza redirecionamentos HTTP e erros temporários para forçar o APT a repetir o download. A lógica vulnerável permite que o pacote substituto seja utilizado na instalação, fazendo com que o código controlado pelo atacante seja executado como root. Em versões antigas, Acquire::Retries também pode habilitar a condição quando configurado manualmente.

Impacto

- Execução de código arbitrário com privilégios root.
- Comprometimento do sistema operacional e dos dados e serviços acessíveis ao usuário root.
- Instalação de backdoors, alteração de configurações e implantação de ferramentas maliciosas.
- Comprometimento da cadeia de fornecimento de software e risco para ambientes que utilizam mirrors/proxies afetados.
- Risco para servidores Linux, estações administrativas e distribuições derivadas de Debian/Ubuntu.

Mitigação e Prevenção

- **Recomendações imediatas:**
  - Atualizar imediatamente o APT para a versão corrigida disponibilizada pela distribuição.
  - Realizar a atualização por rede e repositório confiáveis, validando a origem dos pacotes.
  - Identificar Debian 12+ e Ubuntu 22.04+, além de versões antigas com Acquire::Retries habilitado manualmente.
  - Revisar configurações de repositórios, proxies e mirrors em busca de alterações não autorizadas.
  - Investigar instalações recentes de pacotes e processos privilegiados incomuns diante de suspeita de interferência no tráfego.

- **Recomendações para Administradores de Sistema:**
  - Aplicar pacotes corrigidos conforme a versão: Ubuntu 26.10 (3.3.3ubuntu0.1), 26.04 LTS (3.2.1ubuntu0.1), 24.04 LTS (2.8.4ubuntu0.1) e 22.04 LTS (2.4.15ubuntu0.1), ou versões posteriores corrigidas.

Classificação: Público

- Em Debian, utilizar as versões corrigidas publicadas para cada linha; para Debian 11, a publicação informa APT 2.2.5.
- Verificar todas as versões instaladas, inclusive homologação, containers e derivados de Debian/Ubuntu.
- Auditar Acquire::Retries e scripts de automação que ativem repetição de downloads em versões antigas.
- Utilizar repositórios oficiais e proteger mirrors/proxies; a publicação não confirma as fontes HTTPS também são afetadas, portanto não presumir que HTTPS isoladamente elimina o risco.
- Monitorar alterações inesperadas em pacotes, scripts de pós-instalação, serviços e arquivos de sistema.

- **Recomendações para usuários finais:**
  - Não instalar pacotes de repositórios desconhecidos ou mirrors não autorizados.
  - Manter o sistema atualizado pelos canais oficiais e solicitar suporte se a atualização apresentar erros repetidos.
  - Evitar comandos de instalação copiados de fontes não verificadas.

IoCs e artefatos

- Configuração relevante: Acquire::Retries.
- Vetores técnicos: redirecionamentos HTTP, respostas temporárias de erro e interferência no tráfego entre cliente APT e servidor de pacotes.

Para saber informações mais detalhadas sobre esta ameaça acesse: https://thehackernews.com/2026/11/debian-and-ubuntu-apt-flaw-lets-mitm.html

2.5. Grupo associado ao APT29 sequestra script de análise web para distribuir exploits contra iOS e Android

A campanha Poisoned Source, atribuída presumivelmente ao APT29, utiliza sites legítimos comprometidos, páginas falsas e o comprometimento da cadeia de fornecimento do serviço ucraniano Plerdy SEO Tracker para atingir usuários de iOS e Android. Identificada em outubro de 2026, a atividade entrega cadeias de exploração específicas para cada plataforma, com potencial de roubar cookies, senhas de Wi-Fi e dados de dispositivos móveis.

Exploração

O JavaScript malicioso é inserido em sites comprometidos ou distribuído por domínios semelhantes a páginas legítimas. Também foi identificado código injetado em a.plerdy[.]com/public/js/click/main.js entre 27 de agosto e 3 de setembro de 2026. O script coleta atributos do navegador e do dispositivo e encaminha o visitante para uma cadeia compatível com seu sistema operacional. Em iOS, utiliza kits como DarkSword; em Android, explora

Classificação: Público

vulnerabilidades do Chrome para obter execução remota, escapar do sandbox e elevar privilégios, entregando AndroSnitch.

- iOS 16.7: CVE-2025-43529 e CVE-2024-27834 para roubo de cookies.
- iOS 18.5: cadeia DarkSword com CVE-2025-43529, CVE-2026-20700, CVE-2025-14174, CVE-2025-43510 e CVE-2025-43520 para coleta ampliada de dados.
- Android com Chrome 139 a 145, exceto a versão 143: CVE-2026-3910 e CVE-2025-27038, seguida da entrega do AndroSnitch.
- Coleta de atributos do navegador e dispositivo para selecionar a cadeia de exploração.
- Exfiltração para infraestrutura remota; a cadeia Android encerra a exploração quando identifica Samsung Galaxy S25 Ultra (SM-S938B).

Impacto

- Roubo de cookies de sessão e possível acesso indevido a contas autenticadas.
- Exposição de senhas Wi-Fi e dados armazenados no Chrome em dispositivos Android.
- Em iOS, possível coleta de SMS/iMessage, dados de aplicativos de mensagens, chaves iCloud, contatos, histórico de chamadas, histórico e cookies do Safari, fotos e arquivos pessoais.
- Comprometimento da privacidade e confidencialidade de informações pessoais e corporativas.
- Risco para organizações cujos colaboradores acessam sites comprometidos por dispositivos móveis corporativos ou pessoais.

Mitigação e Prevenção

- **Recomendações imediatas:**
  - Atualizar iOS, Android, Chrome e navegadores móveis para as versões mais recentes dos fabricantes.
  - Identificar dispositivos que acessaram sites suspeitos ou carregaram o script Plerdy no período informado.
  - Bloquear, após validação, ad.starx-net[.]com e domínios suspeitos relacionados à campanha em DNS, proxy e MDM.
  - Investigar tráfego de saída, scripts JavaScript de terceiros e redirecionamentos inesperados.
  - Em dispositivos suspeitos, acionar resposta a incidentes, preservar evidências e avaliar revogação de sessões, tokens e credenciais.

- **Recomendações para Administradores de Sistema:**
  - Manter inventário de dispositivos móveis e impor versões mínimas por MDM/EMM e acesso condicional.
  - Revisar scripts de analytics, tags de publicidade e bibliotecas JavaScript de terceiros nos sites corporativos.
  - Aplicar CSP, SRI quando aplicável e controle rigoroso de alterações em scripts externos.

- Monitorar DNS e conexões ao endpoint de exfiltração, além de domínios recém-registrados ou semelhantes a marcas conhecidas.
- Restringir acesso a dados corporativos em dispositivos sem atualizações e exigir MFA resistente a phishing quando disponível.
- Orientar desenvolvimento e marketing a validar alterações e possíveis comprometimentos em serviços de analytics/publicidade.

- **Recomendações para usuários finais:**
  - Manter sistema operacional e navegador atualizados e habilitar atualizações automáticas.
  - Evitar links suspeitos e páginas desconhecidas, inclusive em redes sociais, anúncios ou mensagens.
  - Considerar que sites legítimos comprometidos podem distribuir código sem solicitar downloads.
  - Reportar comportamento anormal do navegador ou sinais de acesso indevido à equipe responsável.

Para saber informações mais detalhadas sobre esta ameaça acesse: https://thehackernews.com/2026/11/apt29-linked-hackers-hijack-web.html

2.6. Vulnerabilidade zero-day no Cisco Secure Firewall é explorada para provocar reinicialização de dispositivos VPN

A Cisco divulgou atualizações para a CVE-2026-76418, vulnerabilidade de alta severidade com CVSS 8.6 que afeta Cisco Secure Firewall ASA e FTD. A falha foi explorada ativamente em outubro de 2026 e pode permitir que um atacante remoto não autenticado provoque a reinicialização inesperada do dispositivo, causando negação de serviço. A exposição depende de configuração específica do serviço Remote Access SSL VPN.

Exploração

A vulnerabilidade decorre de erros de lógica no serviço Remote Access SSL VPN quando a autenticação secundária está configurada em um tunnel group. Um atacante envia uma requisição especialmente construída durante a conexão com o serviço VPN e aciona o caminho vulnerável, provocando reload do appliance sem concluir autenticação válida. A exposição exige software ASA/FTD vulnerável, serviço SSL VPN acessível e autenticação secundária configurada no grupo correspondente.

Impacto

- Reinicialização inesperada do firewall e indisponibilidade temporária do serviço VPN.
- Interrupção de sessões de acesso remoto e conexões que dependem do dispositivo.
- Impacto na conectividade de usuários remotos, filiais e aplicações corporativas.
- Interrupção de operações críticas e aumento da carga sobre infraestrutura e suporte.

- A publicação confirma negação de serviço, mas não relata roubo de dados nem execução remota de código associados a esta CVE.

Mitigação e Prevenção

- **Recomendações imediatas:**
  - Identificar dispositivos ASA e FTD expostos com Remote Access SSL VPN habilitado.
  - Verificar webvpn nas interfaces e secondary-authentication-servidor-group nos tunnel groups.
  - Revisar todos os grupos, incluindo DefaultWEBVPNGroup, especialmente com tunnel-group-list enable.
  - Aplicar imediatamente a versão corrigida correspondente à linha instalada.
  - Revisar histórico de reload, logs de VPN e requisições HTTP anormais direcionadas ao serviço SSL VPN.

- **Recomendações para Administradores de Sistema:**
  - Atualizar ASA para 9.16.4.104, 9.18.4.96, 9.20.4.50, 9.22.3.200, 9.23.1.48, 9.24.1.27 ou 9.24.10.1, conforme a linha aplicável.
  - Atualizar FTD para 7.0.11, 7.2.13, 7.4.9, 7.6.7, 7.7.14, 10.0.3 ou 10.1.1, conforme a plataforma e a linha utilizada.
  - Utilizar Cisco Software Checker e o comunicado oficial para confirmar a versão adequada.
  - Se não for possível atualizar imediatamente, avaliar orientações temporárias da Cisco para tunnel groups; desabilitar autenticação secundária pode reduzir a segurança e exige análise de risco.
  - Não considerar a remoção da lista de grupos como mitigação suficiente sem verificar o grupo padrão.
  - Após a atualização, validar a VPN, revisar registros de reinicialização e monitorar tentativas de exploração.

- **Recomendações para usuários finais:**
  - Reportar interrupções inesperadas de VPN à equipe de TI, informando horário e duração.
  - Não tentar contornar falhas de conectividade com ferramentas não autorizadas.
  - Seguir orientações corporativas para restabelecimento do acesso remoto.

Para saber informações mais detalhadas sobre esta ameaça acesse: https://cybersecuritynews.com/cisco-secure-firewall-0-day-vulnerability-exploited/

Esta publicação tem como objetivo orientar a equipe interna e os nossos clientes sobre ameaças emergentes no ambiente cibernético, possibilitando assim ações proativas de prevenção para tornar a infraestrutura de nossas empresas cada vez mais segura.

A publicação do documento de Inteligência de Ameaças será realizada semanalmente.

Produzido por: Equipe de Cyber Threat Intelligence da Service IT Security

Classificação: Público