

Your IT Company

Principais Vulnerabilidades e Ameaças (novembro/26)

Sumário

1. Objetivo 2
2. Vulnerabilidades e Ameaças descobertas 2
2.1. Apache HTTP Server: execução remota de código via HTTP/2 2
2.2. Java4Shell: falha crítica no decodificador Base64 do OpenJDK 3
2.3. NoisyTCP: condição de corrida no kernel Linux provoca negação de serviço 4
2.4. ForgePtr: driver NVIDIA permite root e fuga de contêineres 5
2.5. Operation ShadowCloud: backdoors usam SharePoint e GitHub para espionagem 6
2.6. PHP2Shell e TSGA comprometem gateways Check Point 7
2.7. Falha de proteção no ANGLE afeta o Google Chrome para Android 8

1. Objetivo

Este documento reúne e analisa sete divulgações de segurança cibernética de novembro de 2026, com foco em descrição técnica, condições de exploração, impacto operacional, mitigação e indicadores de monitoramento. São diferenciados ataques observados, demonstrações em laboratório e possibilidades técnicas, conforme as fontes.

2. Vulnerabilidades e Ameaças descobertas

2.1. Apache HTTP Server: execução remota de código via HTTP/2

A CVE-2026-119618 afeta o Apache HTTP Server 2.4.55 a 2.4.70 com mod_http2 habilitado e versões independentes mod_h2 2.0.8 a 2.0.42. O Apache classificou a falha como crítica, a CSA de Singapura atribuiu CVSS 8,1 e alertou para exploração ativa em 17 de novembro.

Exploração

Uma falha de sincronização entre threads (CWE-362) na função assign_headers() do módulo mod_http2 do Apache HTTP Server permite corrupção de memória heap durante o processamento concorrente de requisições HTTP/2. Um atacante remoto não autenticado pode explorar a condição de corrida para provocar negação de serviço (DoS) ou, em condições favoráveis, executar código arbitrário com os privilégios do processo web. A vulnerabilidade afeta versões do Apache HTTP Server de 2.4.55 a 2.4.70 e exige que o HTTP/2 esteja habilitado.

Impacto

- Execução de comandos no contexto do servidor web, com potencial comprometimento de aplicações e dados.
- Interrupção do serviço e possibilidade de movimentação posterior conforme privilégios do processo.

Mitigação e Prevenção

- **Recomendações imediatas:**
  - Atualizar Apache para 2.4.71 ou pacote do fornecedor com correção comprovada.
  - Priorizar instâncias expostas e preservar logs para investigar atividade anterior ao patch.
- **Recomendações para Administradores de Sistema:**
  - Inventariar mod_http2 e configurações h2/h2c por virtual host.
  - Se não for possível corrigir imediatamente, desabilitar temporariamente HTTP/2 (Protocols http/1.1), recarregar e verificar listeners.

Para saber informações mais detalhadas sobre esta vulnerabilidade ou ameaça acesse: https://cybersecuritynews.com/apache-http-server-rce-exploitation/

Classificação: Pública

2.2. Java4Shell: falha crítica no decodificador Base64 do OpenJDK

A CVE-2026-114938, apelidada de Java4Shell, afeta o caminho otimizado de decodificação Base64 do HotSpot em determinadas versões do Java. A pesquisa atribui uma pontuação CVSS 4.0 de 9,2, a exposição depende de CPU x86-64 com AVX-512 VBMI, runtime vulnerável e processamento de dados controlados por atacante.

Exploração

A vulnerabilidade ocorre no decodificador Base64 acelerado por hardware da JVM HotSpot (OpenJDK), no qual entradas Base64 malformadas podem provocar uma escrita fora dos limites do buffer (*out-of-bounds write*), resultando em corrupção de memória heap. Em sistemas x86-64 com suporte às instruções AVX-512 VBMI e utilizando versões vulneráveis do Java, um atacante remoto pode explorar aplicações que processem dados Base64 controlados externamente, provocando negação de serviço (DoS) e, mediante condições específicas de exploração, execução remota de código (RCE) sem autenticação. A exploração depende da configuração de cada aplicação, não existindo um exploit universal para todos os serviços Java.

A vulnerabilidade está associada principalmente a versões não corrigidas do OpenJDK 17.0.6 ou posteriores, incluindo as linhas Java 21, 25 e 27, quando executadas em processadores x86-64 compatíveis com AVX-512 VBMI. Sistemas ARM64 não são afetados por esse vetor específico.

Impacto

- Execução de código com privilégios do processo Java, vazamento de segredos presentes na memória e queda da JVM.
- Aplicações com runtime Java embutido podem permanecer expostas mesmo após atualização de bibliotecas.

Mitigação e Prevenção

- **Recomendações imediatas:**
  - Aplicar as atualizações de segurança de Java publicadas em 17 de novembro de 2026.
  - Priorizar aplicações acessíveis pela internet e investigar falhas inesperadas de JVM.
- **Recomendações para Administradores de Sistema:**
  - Inventariar o Java efetivamente utilizado por cada processo, contêiner e appliance; reiniciar ou reconstruir imagens após atualização.
  - Como medida temporária avaliada em teste, utilizar -XX:-UseBASE64Intrinsics ou, em x86-64, -XX:UseAVX=2; restringir entrada não autenticada e validar tamanho dos dados.

Classificação: Pública

- **Recomendações para usuários finais:**
  - Reportar indisponibilidade ou comportamento inesperado de serviços afetados.

  Para saber informações mais detalhadas sobre esta vulnerabilidade ou ameaça acesse: https://cybersecuritynews.com/java4shell/

2.3. NoisyTCP: condição de corrida no kernel Linux provoca negação de serviço

A CVE-2026-99288, denominada como NoisyTCP, é uma falha antiga no processamento TCP do kernel Linux, introduzida em 2015 e corrigida em novembro de 2026. Serviços que escutam conexões TCP podem ser afetados em hosts com múltiplas filas de recepção ou Receive Packet Steering.

Exploração

Uma condição de corrida no subsistema TCP do kernel Linux, durante consultas simultâneas à tabela de conexões estabelecidas (established hash table), permite que uma thread acesse um objeto de socket parcialmente inicializado ou reutilizado indevidamente. Um atacante remoto não autenticado pode explorar essa falha por meio do envio coordenado de fragmentos IPv4 e pacotes TCP distribuídos entre diferentes CPUs, provocando uma desreferência de ponteiro nulo (NULL Pointer Dereference) e, consequentemente, um kernel panic, resultando em negação de serviço (DoS).

A exploração pode afetar servidores com múltiplas filas de recepção de rede (RX) ou mecanismos RPS habilitados, podendo comprometer a disponibilidade de todo o sistema operacional, inclusive em ambientes virtualizados ou conteinerizados. Não há evidências de que a falha permita execução arbitrária de código.

Impacto

- Queda remota do host e interrupção de todos os serviços, inclusive quando o gatilho ocorre em aplicação conteinerizada.
- Não há demonstração pública de execução remota de código confiável associada à falha.

Mitigação e Prevenção

- **Recomendações imediatas:**
  - Atualizar o kernel conforme correção disponibilizada pela distribuição e reiniciar o host.
  - Priorizar servidores Linux com serviços TCP expostos e investigar reinicializações inesperadas.
- **Recomendações para Administradores de Sistema:**
  - Verificar kernels e configurações de filas de recepção e RPS/RFS.

Classificação: Pública

- Avaliar, apenas como contingência com análise de risco, limitar a uma fila de recepção e desabilitar RPS/RFS; desativar SYN cookies reduz proteção contra SYN flood e não deve ser medida padrão.

Para saber informações mais detalhadas sobre esta vulnerabilidade ou ameaça acesse: https://cybersecuritynews.com/noisytcp-linux-kernel-vulnerability/

2.4. ForgePtr: driver NVIDIA permite root e fuga de contêineres

CVE-2026-47501, chamada ForgePtr, afeta versões do módulo aberto de driver GPU NVIDIA para Linux. A Stealthium demonstrou elevação de privilégios em hosts com driver vulnerável e acesso local ao dispositivo GPU, incluindo ambientes de contêineres compartilhados.

Exploração

Uma falha de validação no gerenciamento de buffers de eventos do driver de vídeo NVIDIA para Linux permite que identificadores inválidos sejam tratados como ponteiros de memória válidos, ocasionando uma escrita fora dos limites (Out-of-Bounds Write) na memória do kernel. Um atacante local com privilégios reduzidos pode explorar essa condição para corromper estruturas internas do kernel. Em uma demonstração técnica, a falha foi combinada com uma vulnerabilidade de vazamento de informações para contornar o KASLR, localizar endereços de memória e obter execução de código com privilégios de root no host, possibilitando também a fuga de contêineres (Container Escape).

A vulnerabilidade afeta o NVIDIA GPU Display Driver e possui pontuação CVSS 3.1 de 7,8 (Alta). Apesar do impacto demonstrado, sua exploração exige acesso local ao dispositivo GPU e privilégios iniciais reduzidos, não sendo uma vulnerabilidade explorável diretamente pela rede.

Impacto

- Escalada de usuário local ou contêiner para root do host, com exposição de outros workloads e dados.
- Possibilidade de adulterar proteções do kernel em tempo de execução, mesmo com Secure Boot habilitado.

Mitigação e Prevenção

- **Recomendações imediatas:**
  - Atualizar drivers afetados para 615.71.09 ou posterior conforme fornecedor.
  - Priorizar hosts multi-tenant que disponibilizam GPUs a cargas não confiáveis.
- **Recomendações para Administradores de Sistema:**
  - Conferir a versão real do driver carregado no host, não apenas a imagem do contêiner.

Classificação: Pública

- Correlacionar erros do driver com mudanças inesperadas em configurações do kernel e reforçar isolamento de acesso aos dispositivos GPU

Para saber informações mais detalhadas sobre esta vulnerabilidade ou ameaça acesse: https://gbhackers.com/nvidia-gpu-driver-flaw/

2.5. Operation ShadowCloud: backdoors usam SharePoint e GitHub para espionagem

Pesquisadores identificaram uma operação de espionagem contra setores governamentais na Ásia e África, utilizando os backdoors GraphDoor e GitDoor. Os implantes exploram serviços legítimos de nuvem para comando e controle; a identidade do operador não foi estabelecida conclusivamente.

Exploração

Após acesso inicial não esclarecido, uma cadeia com MeshCentral Agent, carregamento lateral de DLL e payload cifrado instala componentes modulares. GraphDoor usa Microsoft Graph e SharePoint; GitDoor utiliza repositórios GitHub para receber instruções e armazenar resultados.

Impacto

- Coleta de credenciais, registros de teclas, capturas de tela e outros dados sensíveis.
- Persistência e comando remoto disfarçados em tráfego legítimo de APIs corporativas.

Mitigação e Prevenção

- **Recomendações imediatas:**
  - Investigar instalações não autorizadas de MeshCentral Agent e autenticações de aplicativos desconhecidos.
  - Revisar conexões com tenants SharePoint externos e repositórios GitHub atípicos.
- **Recomendações para Administradores de Sistema:**
  - Monitorar concessões de aplicativos no Entra ID, acessos Graph API e transferências para SharePoint fora da organização.
  - Aplicar allowlisting, telemetria EDR e regras para carregamento lateral de DLL e acesso anormal a LSASS.
- **Recomendações para usuários finais:**
  - Reportar solicitações inesperadas de autenticação ou instalação de ferramentas de suporte remoto.

Para saber informações mais detalhadas sobre esta vulnerabilidade ou ameaça acesse: https://boletimsec.com/backdoors-usam-sharepoint-e-github-para-espionar-redes-governamentais/

Classificação: Pública

2.6. PHP2Shell e TSGA comprometem gateways Check Point

Uma campanha observada pela Check Point explora CVE-2026-109618 e CVE-2026-109619 em portais Mobile Access expostos, encadeadas pela CVE-2026-123039 no Gaia OS. Após obter acesso, o ator instala o backdoor TSGA e, em alguns casos, executa ações destrutivas.

Exploração

Atacantes exploram vulnerabilidades PHP2Shell (CVE-2026-109618 e CVE-2026-109619) nos portais Mobile Access de dispositivos Check Point Security Gateway, por meio de requisições especialmente elaboradas, obtendo execução remota de código no contexto do serviço do portal. Em seguida, exploram uma falha de autorização insuficiente no componente DynamicCLI (CVE-2026-123039) para elevar privilégios e obter acesso root ao dispositivo.

Após o comprometimento, implantam web shells PHP e o backdoor TSGA, que utiliza o componente TSProxy para ocultar comunicações maliciosas por meio de processos e serviços legítimos. Em determinadas intrusões, também foram identificados reconhecimento da rede interna, movimentação lateral via SSH para hosts VMware ESXi e implantação do malware destrutivo (wiper) destroy_v6, destinado à exclusão de arquivos e dados.

Impacto

- Comprometimento de dispositivos Check Point Security Gateway, com obtenção de privilégios de root e controle administrativo não autorizado;
- Acesso indevido, extração e exposição de configurações de segurança, credenciais e informações sensíveis armazenadas nos gateways;
- Adulteração ou exclusão de logs de firewall, comprometendo a rastreabilidade de eventos e dificultando a identificação de atividades maliciosas;
- Desativação, manipulação ou comprometimento de mecanismos de segurança e monitoramento da infraestrutura de rede;
- Interrupção de serviços e indisponibilidade de gateways, afetando a conectividade e a proteção dos ambientes corporativos;
- Utilização dos dispositivos comprometidos como ponto de entrada para movimentação lateral e propagação de atividades maliciosas na rede interna;
- Comprometimento de servidores VMware ESXi alcançados durante a movimentação lateral;
- Possibilidade de exclusão, corrupção ou destruição de dados em ambientes virtualizados por meio da implantação de ferramentas do tipo wiper;
- Interrupção de máquinas virtuais, sistemas corporativos e serviços críticos, podendo resultar em indisponibilidade operacional prolongada;
  Comprometimento da confidencialidade, integridade e disponibilidade dos ativos e serviços da organização.

Classificação: Pública

Mitigação e Prevenção

- **Recomendações imediatas:**
  - Aplicar correções para PHP2Shell e Gaia OS conforme avisos Check Point; tratar dispositivos expostos como prioritários.
  - Investigar web shells, acessos administrativos atípicos e evidências de persistência antes de limpeza.
- **Recomendações para Administradores de Sistema:**
  - Inventariar gateways Mobile Access e versões Gaia afetadas; restringir acesso de gerenciamento.
  - Revisar logs de DynamicCLI, alterações de firewall, backups e snapshots; monitorar acessos SSH inesperados a ESXi.

Para saber informações mais detalhadas sobre esta vulnerabilidade ou ameaça acesse: https://boletimsec.com/cibercriminosos-exploram-php2shell-para-infectar-gateways-check-point/

2.7. Falha de proteção no ANGLE afeta o Google Chrome para Android

Criticidade: Crítica | CVSS 9.6 | CVE-2026-130910 | Divulgada em 17/11/2026

O Google Chrome para Android, anterior à versão 158.0.8127.36, apresenta uma falha no mecanismo de proteção do ANGLE. Segundo a NVD, um atacante remoto pode explorar uma página HTML cuidadosamente construída para executar código arbitrário fora do sandbox. A severidade informada pelo Chrome é alta, enquanto a coleta atribui uma pontuação de CVSS 9.6 e criticidade crítica.

Exploração

Uma falha no mecanismo de proteção do componente ANGLE (Almost Native Graphics Layer Engine), utilizado pelo Google Chrome para Android, permite que uma página HTML especialmente elaborada explore deficiências no isolamento do navegador. Ao induzir a vítima a acessar uma página maliciosa, um atacante remoto, sem necessidade de autenticação, pode potencialmente executar código arbitrário fora do ambiente de sandbox, comprometendo a confidencialidade, a integridade e a disponibilidade do dispositivo.

A vulnerabilidade afeta o Google Chrome para Android em versões anteriores à 158.0.8127.36. Até 19/11/2026, não há registro de PoC pública, exploração ativa confirmada ou inclusão na CISA KEV. Também não foram divulgados indicadores de comprometimento (IOCs), como endereços IP, domínios ou hashes associados à exploração.

Impacto

- Execução de código arbitrário fora do ambiente isolado (sandbox) do navegador;
- Comprometimento da integridade, confidencialidade e disponibilidade de dispositivos Android vulneráveis;
- Acesso não autorizado a informações e dados armazenados no dispositivo;
- Manipulação, alteração ou exclusão de arquivos e dados locais;

Classificação: Pública

- Possibilidade de instalação e execução de aplicações ou componentes maliciosos;
- Comprometimento de sessões, dados de navegação e informações sensíveis acessíveis ao processo comprometido;
- Utilização do dispositivo como ponto de apoio para atividades maliciosas adicionais;
- Potencial exploração de vulnerabilidades complementares para ampliar os privilégios e o nível de comprometimento do dispositivo.

Mitigação e Prevenção

Ações imediatas:

- Atualizar o Google Chrome nos dispositivos Android gerenciados para a versão 158.0.8127.36 ou posterior.
- Identificar dispositivos Android que utilizem versões anteriores do Google Chrome e priorizar a atualização.
- Monitorar atividades suspeitas em dispositivos compartilhados ou utilizados em processos operacionais do aeroporto.

Recomendações para Administradores de Sistema:

- Validar em inventário e nos mecanismos de gestão de dispositivos a versão do Google Chrome instalada nos equipamentos Android.
- Confirmar a aplicação da atualização por meio de uma política centralizada e verificar a redução de sistemas desatualizados.
- Restringir o acesso a sites não essenciais até a conclusão da atualização nos dispositivos-juízo de maior criticidade operacional.

Recomendações para Usuários Finais:

- Atualizar o Google Chrome para a versão 158.0.8127.36 ou posterior por meio dos mecanismos oficiais de atualização.
- Evitar a abertura de páginas HTML recebidas por canais não confiáveis enquanto a atualização não estiver concluída.

Para saber informações mais detalhadas sobre este tema acesse: https://chromereleases.googleblog.com/2026/11/stable-channel-update-for-desktop_01699533288.html.

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: Pública