Your IT Company

Principais Vulnerabilidades e Ameaças (setembro/26)

Sumário

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. Atores de ameaça abusando da vulnerabilidade de carregamento lateral de DLL do Chrome - IOCs ativos

A técnica de **DLL Side-Loading** consiste em utilizar um executável legítimo para carregar uma DLL maliciosa localizada em um diretório controlado pelo atacante. A técnica permite que o malware seja executado dentro de um processo aparentemente legítimo e pode dificultar sua detecção.

A técnica já foi documentada em ataques envolvendo componentes legítimos do **Google Chrome**, inclusive por grupos como APT3 e APT41, que utilizaram executáveis legítimos associados ao Chrome ou outros softwares para realizar o carregamento de DLLs maliciosas.

Em uma campanha recente analisada pela D3Lab, um arquivo JavaScript distribuído por meio de uma isca de documento foi utilizado para entregar um executável legítimo que realizou o carregamento lateral de uma DLL maliciosa.

Exploração

A cadeia observada utiliza um arquivo executável legítimo acompanhado de uma DLL maliciosa. Quando o executável é iniciado, o mecanismo de busca de DLLs do Windows pode localizar primeiro a biblioteca maliciosa no diretório controlado pelo atacante, resultando na execução do código malicioso.

Mitigação e Prevenção

- **Recomendações para Administradores de Sistema:**
  - Monitorar executáveis legítimos carregando DLLs a partir de diretórios incomuns.
  - Utilizar EDR para detectar carregamento anômalo de bibliotecas.
  - Restringir execução de arquivos provenientes de diretórios temporários e downloads.
  - Manter Chrome, Windows e demais aplicações atualizadas.
  - Implementar Application Control/AppLocker quando aplicável.
  - Investigar executáveis assinados que carreguem DLLs não assinadas ou desconhecidas.
- **Recomendações para Usuários Finais:**
  - Evitar abrir anexos ou executar arquivos recebidos de fontes desconhecidas.
  - Não instalar versões modificadas ou distribuídas fora dos canais oficiais.
  - Manter navegador e sistema operacional atualizados.

IOCs

- **Arquivos:**
  - Fattura-2819889242.pfd.js
  - client_124578.exe
  - d3d11.dll
- **Hashes:**
  - **JS SHA-256:**
    b11ef9f11c9bb6228582f38a61f4c04dc7160939d8c5b7ee4e467ffde6317f02
  - **EXE SHA-256:**
    e77747f06d1d3ee5b8466340a10416874439dd69a7e9cd8653647be7782899b6
  - **DLL SHA-256:**
    94f333cba95e76e6b8c0f8831bffc446b5f3c90db2c598c6079a98f1a0ef9701

Para saber informações mais detalhadas sobre esta vulnerabilidade acesse: https://rewterz.com/threat-advisory/threat-actors-abusing-chrome-dll-side-loading-vulnerability-for-malware-execution-active-iocs.

2.2. Campanha de instaladores falsos compromete usuários por meio de sites fraudulentos de download

A Microsoft identificou uma campanha ativa que utiliza sites falsos de download de softwares para se passar por fabricantes legítimos e distribuir instaladores maliciosos. A campanha atingiu organizações de diversos setores e apresenta forte direcionamento a usuários chineses ou operações localizadas na China.

Os sites utilizam marcas conhecidas, como Razer, Microsoft Edge, Kaspersky, Sejda, Baidu, SteelSeries e Calibre, para induzir o usuário a baixar softwares aparentemente legítimos. A atividade foi associada com confiança moderada à campanha conhecida como **Silver Fox/Yinhu**, embora a Microsoft não tenha atribuído formalmente a atividade a um ator de Estado-nação.

Exploração

A vítima acessa um domínio que imita o site legítimo de um fornecedor e baixa um instalador malicioso. Após a execução, o malware pode estabelecer persistência, tentar enfraquecer mecanismos de segurança e iniciar comunicação com infraestrutura controlada pelos atacantes.

Mitigação e Prevenção

- **Recomendações para Administradores de Sistema:**
  - Permitir instalação de softwares somente a partir de fontes oficiais.
  - Habilitar SmartScreen, proteção de rede e proteção contra adulteração.
  - Utilizar EDR/antivírus com proteção baseada em nuvem.
  - Monitorar downloads e execução de instaladores provenientes de domínios recém-criados ou suspeitos.
  - Implementar Application Control para restringir softwares não autorizados.

- Investigar sistemas que tenham acessado os domínios listados abaixo.

- **Recomendações para Usuários Finais:**
  - Baixar programas somente dos sites oficiais dos fabricantes.
  - Desconfiar de resultados patrocinados ou páginas que utilizem domínios semelhantes aos oficiais.
  - Não desabilitar antivírus ou SmartScreen para instalar um programa.
  - Verificar cuidadosamente o domínio antes de realizar downloads.

IOCs

- **Domínios de phishing/impersonação:**
  - pc-razerzone[.]com[.]cn
  - app-microsoft-edge[.]com[.]cn
  - kaspersky-lab[.]hl[.]cn
  - sejda[.]hl[.]cn
  - translate-youdao[.]hl[.]cn
  - zh-diskgenius[.]com[.]cn
  - baidu-pan[.]com[.]cn
  - ocam-pc[.]com[.]cn
  - cn-drawio[.]com[.]cn
  - steelseries-cn[.]com[.]cn
  - gw-sogou[.]com[.]cn
  - calibre-ebook[.]com[.]cn
  - mindmoster[.]com[.]cn
- **Infraestrutura de distribuição/C2:**
  - gehie246[.]com
  - yimxg25tiy[.]com
  - cc8ttkv35b[.]com
  - n7b8t85zsg[.]com
  - iualef[.]net
  - oijfwe[.]net
  - 202.95.14[.]237:5090
  - 103.183.3[.]162:5090
- **URL de distribuição:**
  - hxxps://www.gehie246[.]com/712down

Para saber informações mais detalhadas sobre esta vulnerabilidade acesse: https://www.microsoft.com/en-us/security/blog/2026/09/01/counterfeit-installers-system-compromise-tracking-deceptive-software-download-campaign/.

2.3. Campanha TerminalFix utiliza engenharia social e ClickFix para implantação de túnel reverso

A Microsoft identificou uma campanha denominada **TerminalFix**, uma variante da técnica de engenharia social **ClickFix**. Sites comprometidos exibem uma falsa verificação Cloudflare CAPTCHA para induzir usuários a copiar e executar comandos PowerShell no Windows Terminal.

Após a execução, a campanha realiza uma cadeia de múltiplos estágios envolvendo DLL Side-Loading, esteganografia, persistência, reconhecimento do Active Directory e implantação de um túnel reverso baseado em WebSocket.

Exploração

O usuário é induzido a executar um comando PowerShell aparentemente relacionado à verificação CAPTCHA. O comando baixa um arquivo ZIP contendo **LockScreenContentServer.exe** e uma DLL maliciosa chamada **dui70.dll**.

O executável legítimo realiza o carregamento lateral da DLL, que posteriormente recupera payloads ocultos em imagens PNG. O malware estabelece persistência por meio de chaves Registry Run e tarefas agendadas e realiza reconhecimento do domínio.

Por fim, é implantado um cliente Python que estabelece um túnel WebSocket reverso para a infraestrutura do atacante, permitindo o encaminhamento de tráfego TCP através do equipamento comprometido.

Mitigação e Prevenção

- **Recomendações para Administradores de Sistema:**
  - Restringir PowerShell e Windows Terminal para usuários que não necessitem dessas ferramentas.
  - Implementar AppLocker ou Windows Application Control.
  - Habilitar PowerShell Script Block Logging.
  - Monitorar execução de **LockScreenContentServer.exe** fora de diretórios legítimos.
  - Monitorar carregamento de DLLs a partir de diretórios incomuns.
  - Detectar criação de tarefas agendadas e chaves **Run** suspeitas.
  - Monitorar conexões WebSocket/TLS anômalas.
  - Utilizar EDR, Network Protection e proteção contra scripts ofuscados.
  - Investigar imediatamente hosts que apresentem os IOCs.
- **Recomendações para Usuários Finais:**
  - Nunca copiar comandos fornecidos por páginas da Internet para PowerShell ou Windows Terminal.
  - Desconfiar de páginas que solicitem comandos para "provar que você é humano".

- CAPTCHA legítimo não exige que o usuário execute comandos PowerShell.
- Reportar imediatamente páginas ou mensagens suspeitas à equipe de segurança.

IOCs

- **Domínios C2/conteúdo:**
  - gitnow[.]dev
  - bestsocialmedianewspapper[.]com
  - offlineupdater[.]com
- **Arquivos:**
  - LockScreenContentServer.exe
  - dui70.dll
  - client.py
  - verify_pkg.zip
- **SHA-256:**
  - **ZIP**: 18c2090e8a0ae0568af9b87e59eaf8270f23d2909600ed9db91a9444fd8b278f
  - **client.py**: b8d107800403b9197e5b7609ceacd8e4cac1b0f9a1d156e6dacd6c3f7794b36a
  - **dui70.dll**: ba77feed86bcda49308746421bdc684a432dd5d68c363975b2a3c6831bda3f07
- **Comunicação:**
  - gitnow[.]dev:443

Para saber informações mais detalhadas sobre esta vulnerabilidade acesse: https://www.microsoft.com/en-us/security/blog/2026/08/28/terminalfix-campaign-deploys-reverse-tunnel-through-multistage-intrusion/.

2.4. CVE-2026-53362: Vulnerabilidade no Linux Kernel permite elevação de privilégios

A CVE-2026-53362 é uma vulnerabilidade do Linux Kernel relacionada ao subsistema de **rede IPv6**, adicionada pela CISA ao catálogo KEV após confirmação de exploração em ataques reais. A falha pode permitir que um atacante local obtenha privilégios elevados em sistemas vulneráveis.

Exploração

Um atacante que já possua acesso local ao sistema pode explorar a falha presente no componente IPv6 para elevar seus privilégios. Uma exploração bem-sucedida pode permitir a obtenção de permissões significativamente maiores, potencialmente incluindo privilégios de root.

Mitigação e Prevenção

- **Recomendações para administradores de sistema:**
  - Aplicar imediatamente os patches disponibilizados pelo fabricante da distribuição.
  - Identificar servidores que utilizem versões vulneráveis do kernel.
  - Priorizar ativos expostos e sistemas que armazenem informações críticas.
  - Realizar análise forense caso existem indícios de exploração anterior.
  - Monitorar eventos de elevação de privilégios e atividades anômalas no kernel.
- **Recomendações para Usuários Finais:**
  - Manter o sistema operacional atualizado.
  - Evitar execução de aplicações não confiáveis.
  - Não utilizar contas administrativas para atividades rotineiras.

Para saber informações mais detalhadas sobre esta vulnerabilidade acesse: https://cybersecuritynews.com/linux-kernel-privilege-escalation-vulnerability-exploited/.

2.5. CVE-2025-20241: Vulnerabilidade no Cisco Nexus 3000/9000 pode causar negação de serviço

A CVE-2025-20241 é uma vulnerabilidade de alta severidade no recurso **IS-IS** do Cisco NX-OS, afetando determinados switches Cisco Nexus 3000 e 9000 em modo standalone NX-OS.

A falha resulta de validação insuficiente de pacotes IS-IS recebidos e pode permitir que um atacante não autenticado, localizado na mesma proximidade de camada 2, provoque a reinicialização do processo IS-IS e, potencialmente, o reload do equipamento, causando negação de serviço (DoS).

Exploração

O atacante envia um pacote **IS-IS** especialmente criado ao equipamento vulnerável. O processamento inadequado do pacote pode provocar a reinicialização do processo **IS-IS** e, em determinadas condições, o reinício do próprio dispositivo.

Mitigação e Prevenção

- **Recomendações para Administradores de Sistema:**
  - Aplicar as atualizações de software recomendadas pela Cisco.
  - Avaliar a utilização do protocolo **IS-IS** no ambiente.
  - Implementar autenticação para **IS-IS** quando disponível e aplicável.
  - Restringir o acesso à infraestrutura de rede e aos segmentos onde os switches estão conectados.
  - Monitorar reinicializações inesperadas do processo **IS-IS**.
  - Não depender de workaround, pois a Cisco informa que não existe uma solução alternativa disponível para essa vulnerabilidade.

Para saber informações mais detalhadas sobre esta vulnerabilidade acesse: https://cybersecuritynews.com/cisco-nexus-9000-series-switches-vulnerability/.

2.6. CVE-2026-19632: Falha crítica no Plugin TranslatePress para WordPress pode permitir tomada de contas administrativas

A CVE-2026-19632 é uma vulnerabilidade crítica de **Account Takeover** no plugin TranslatePress para WordPress. A falha recebeu pontuação **CVSS 9.8** e afeta versões até **3.3.1**, sendo corrigida na versão **3.3.2**. O plugin possui mais de 400 mil instalações ativas.

Exploração

A vulnerabilidade permite que um atacante não autenticado obtenha a URL de redefinição de senha de um administrador. A falha está relacionada à ação AJAX **trp_get_translations_regular** e à forma como determinadas strings são armazenadas na tabela de tradução.

Quando as condições necessárias estão presentes, o atacante consegue recuperar o link de redefinição contendo a chave de recuperação e parâmetros de login, possibilitando assumir a conta administrativa e, consequentemente, comprometer completamente o site.

Mitigação e Prevenção

- **Recomendações para Administradores de Sistema:**
  - Atualizar imediatamente o TranslatePress para a versão **3.3.2 ou posterior**.
  - Verificar contas administrativas e alterações recentes de credenciais.
  - Invalidar sessões e redefinir senhas administrativas após uma possível exposição.
  - Utilizar MFA nas contas administrativas.
  - Monitorar requisições anômalas ao endpoint AJAX relacionado ao plugin.
  - Manter WordPress, plugins e temas atualizados.

Para saber informações mais detalhadas sobre esta vulnerabilidade acesse: https://cybersecuritynews.com/translatepress-wordpress-plugin-vulnerability/.

2.7. CVE-2026-32475: Vulnerabilidade crítica no Plugin Elementor Pro para WordPress permite upload de arquivos maliciosos

A CVE-2026-32475 é uma vulnerabilidade crítica de upload irrestrito de arquivos perigosos no Elementor Pro. O problema pode permitir que um atacante não autenticado envie arquivos maliciosos para o servidor, podendo resultar em execução de código e comprometimento do site.

A vulnerabilidade afeta o Elementor Pro até a versão **4.2.1** e foi corrigida na **4.2.2**. O CVE recebeu classificação crítica, com CVSS 9.0.

Exploração

A falha está relacionada ao mecanismo de upload do widget Forms. Em determinadas condições, arquivos que deveriam ser bloqueados podem escapar das validações e ser armazenados no servidor.

Um atacante pode utilizar esse comportamento para enviar um arquivo PHP ou outro conteúdo executável e, posteriormente, tentar acessá-lo remotamente para executar comandos no servidor.

Mitigação e Prevenção

- **Recomendações para Administradores de Sistema:**
  - Atualizar o Elementor Pro para a versão **4.2.2 ou posterior**.
  - Restringir uploads a extensões estritamente necessárias.
  - Impedir execução de scripts em diretórios destinados ao armazenamento de uploads.
  - Utilizar WAF/Firewall para proteção de aplicações web.
  - Monitorar criação de arquivos PHP inesperados no diretório de uploads.
  - Revisar logs de acesso em busca de requisições POST suspeitas.

Para saber informações mais detalhadas sobre esta vulnerabilidade acesse: https://cybersecuritynews.com/wordpress-plugin-vulnerability-exposes-3/.

2.8. Apache Tomcat: Múltiplas vulnerabilidades podem permitir bypass de segurança e negação de serviço

A Apache Software Foundation corrigiu diversas vulnerabilidades no Apache Tomcat divulgadas em agosto de 2026. Entre os problemas estão falhas que podem permitir bypass de controles de acesso e autenticação, além de condições de negação de serviço. Entre os principais problemas estão:

- **CVE-2026-65182** — bypass de restrições de segurança devido ao processamento incorreto de caminhos.
- **CVE-2026-68569** — falha de autenticação que pode permitir autenticação indevida em determinadas configurações.
- **CVE-2026-65927** — problema no RewriteValve.
- **CVE-2026-68525** — possível bypass de restrições relacionadas ao método HTTP.
- **CVE-2026-68763** — vulnerabilidade no HTTP/2 que pode levar à exaustão de recursos e DoS.
- **CVE-2026-66299** — crescimento ilimitado de memória no exemplo WebSocket Chat, podendo provocar indisponibilidade.

Exploração

Dependendo da vulnerabilidade, um atacante remoto pode utilizar requisições HTTP especialmente elaboradas para contornar mecanismos de autorização, explorar falhas de autenticação ou provocar consumo excessivo de recursos.

A CVE-2026-65182, por exemplo, pode permitir o bypass de uma restrição de segurança quando regras referentes a caminhos mais longos são processadas antes de regras mais restritivas aplicadas a subcaminhos. Já a CVE-2026-68569 pode resultar em autenticação indevida em determinadas configurações.

Versões Afetadas

As vulnerabilidades atingem diferentes versões do Apache Tomcat. Para as principais falhas de autenticação e controle de acesso, as correções estão disponíveis, entre outras, nas versões:

- **Tomcat 11.0.25**
- **Tomcat 10.1.58**
- **Tomcat 9.0.121**

Versões antigas, incluindo determinados releases 8.5 e 7.x, também podem estar afetadas e devem ser tratadas conforme as orientações oficiais do projeto.

Mitigação e Prevenção

- **Recomendações para Administradores de Sistema:**
  - Atualizar o Apache Tomcat para uma versão corrigida.
  - Priorizar servidores Tomcat expostos diretamente à Internet.
  - Revisar regras de autenticação e autorização após a atualização.
  - Remover aplicações de exemplo que não sejam necessárias.
  - Monitorar logs HTTP e eventos de autenticação anômalos.
  - Utilizar WAF e controles de acesso adicionais quando aplicável.
  - Evitar a utilização de versões antigas e fora de suporte.

Para saber informações mais detalhadas sobre esta vulnerabilidade acesse: https://cybersecuritynews.com/apache-tomcat-vulnerabilities-crash-servers/.

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 quinzenalmente.

Produzido por: Equipe de Threat Intelligence da Service IT Security