Your IT Company

Principais Vulnerabilidades e Ameaças (Maio/25)

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. Vulnerabilidade no Kernel Linux SMB Client pode levar a vazamentos de memória e Use-After-Free

Uma nova vulnerabilidade no kernel Linux, identificada como CVE-2025-37835, afeta o cliente SMB. A falha, relacionada ao gerenciamento incorreto de contagem de referência em namespaces de rede, pode causar vazamentos de memória e situações de "use-after-free". A exploração bem-sucedida desta vulnerabilidade pode levar à instabilidade do sistema e potencial execução de código malicioso.

Exploração

A vulnerabilidade reside no cliente SMB do kernel Linux, especificamente no tratamento de referências a namespaces de rede (netns). A falha ocorre devido a um desequilíbrio no uso de get_net() e put_net(), resultando em vazamentos de contagem de referência e na possibilidade de uso de memória após ela ter sido liberada (use-after-free). Isso pode ocorrer durante o processo de montagem de compartilhamentos CIFS (Common Internet File System), especialmente em situações de reconexão ou falhas na conexão.

Mitigação e Prevenção

- **Atualize o Kernel:** A solução para essa vulnerabilidade é a aplicação dos patches corretivos disponibilizados pelos desenvolvedores do kernel Linux. Verifique regularmente se há atualizações de segurança para a sua distribuição Linux e instale-as assim que estiverem disponíveis.
- **Monitoramento:** Monitore os logs do sistema em busca de erros relacionados ao cliente SMB ou operações de rede que possam indicar um comportamento anômalo.
- **Teste em Ambiente Controlado:** Antes de aplicar a atualização em ambientes de produção, teste-a em um ambiente de teste para garantir a compatibilidade e estabilidade do sistema.

Para saber informações mais detalhadas sobre esta vulnerabilidade acesse: https://www.tenable.com/cve/CVE-2025-37835

2.2. Vulnerabilidade no Plugin PeepSo Core para WordPress permite download não autorizado de arquivos

Uma falha crítica no plugin PeepSo Core para WordPress, afeta todas as versões até a 6.4.6.0. A vulnerabilidade, causada por uma falha na validação de uma chave controlada pelo usuário através do endpoint da API REST file_download, permite que atacantes não autenticados baixem arquivos de outros usuários, expondo potencialmente informações sensíveis.

Exploração

A vulnerabilidade reside na função de upload de arquivos do plugin PeepSo Core para WordPress. A ausência de validação adequada em uma chave específica, controlada pelo usuário, permite que atacantes utilizem o endpoint file_download da API REST para solicitar o download de arquivos sem a devida autorização. Isso significa que um invasor pode obter acesso a arquivos privados e informações sensíveis carregadas por outros usuários na plataforma.

Mitigação e Prevenção

- **Atualização:** A principal ação a ser tomada é atualizar o plugin PeepSo Core para a versão mais recente, que corrige essa vulnerabilidade.
- **Monitoramento:** Monitore o tráfego da sua aplicação WordPress em busca de acessos suspeitos ou anormais ao endpoint file_download.
- **Auditoria de Segurança:** Realize auditorias regulares de segurança em seu site WordPress e em todos os plugins instalados para identificar e corrigir outras possíveis vulnerabilidades.

Para saber informações mais detalhadas sobre esta vulnerabilidade acesse: https://www.tenable.com/cve/CVE-2024-8988, https://www.wordfence.com/threat-intel/vulnerabilities/id/d3184996-655c-41d5-a3c5-6b36fbff58dc?source=cve, https://www.peepso.com/changelog/.

2.3. Vulnerabilidade de Injeção de Objeto PHP no Plugin Uncanny Automator para WordPress

Uma vulnerabilidade crítica de injeção de objeto PHP foi descoberta no plugin Uncanny Automator para WordPress, afetando todas as versões até a 6.4.0.1. Esta falha permite que atacantes autenticados, com acesso de nível Subscriber ou superior, injetem objetos PHP maliciosos, possibilitando a exclusão de arquivos arbitrários. A exploração desta vulnerabilidade pode levar a comprometimentos significativos de sites WordPress.

Exploração

A vulnerabilidade reside na função automator_api_decode_message() do plugin, que realiza a desserialização de dados não confiáveis. Isso permite que invasores injetem código PHP por meio da manipulação de objetos. A presença de uma cadeia POP (Property-Oriented Programming) adicional agrava o problema, permitindo que os atacantes excluam arquivos no servidor.

Mitigação e Prevenção

- **Atualize o Plugin:** A ação mais importante é atualizar o plugin Uncanny Automator para a versão 6.4.0.2 ou superior, que corrige a vulnerabilidade.

- **Verifique as Permissões:** Revise e restrinja as permissões de acesso dos usuários no WordPress, especialmente aqueles com nível Subscriber, para minimizar o risco de exploração.
- exploração.
- **Monitore Ativamente:** Monitore os logs do servidor e as atividades do WordPress em busca de sinais de atividades suspeitas, como tentativas de acesso não autorizadas ou alterações anormais em arquivos.

Para saber informações mais detalhadas sobre esta vulnerabilidade acesse: https://www.tenable.com/cve/CVE-2025-3623, https://www.wordfence.com/threat-intel/vulnerabilities/id/00bcfd8f-9785-449a-a0ea-16e2583d684a?source=cve

2.4 Nova vulnerabilidade de execução remota de código no Microsoft Outlook

Uma falha crítica de execução remota de código (RCE) no Microsoft Outlook, identificada como CVE-2025-32705, foi corrigida pela Microsoft em maio de 2025. A vulnerabilidade, com um score CVSSv3 de 7.8, permite a execução de código malicioso através de um arquivo especialmente criado. É crucial que usuários e empresas apliquem as atualizações de segurança imediatamente para se protegerem.

Exploração

A vulnerabilidade CVE-2025-32705 reside em um erro de leitura fora dos limites (out-of-bounds read) no Outlook. Um atacante pode explorar essa falha enviando um arquivo malicioso via e-mail ou outros meios. Quando o usuário abre este arquivo em uma versão vulnerável do Outlook, o erro é acionado, permitindo a execução de código arbitrário no sistema. O Painel de Visualização do Outlook não é um vetor de ataque, o que significa que a simples visualização de um e-mail não acionará a vulnerabilidade.

Mitigação e Prevenção

- **Aplique as Atualizações de Segurança Imediatamente**: Instale os patches oficiais da Microsoft para todas as instalações afetadas do Outlook.
- **Cuidado com Anexos de E-mail**: Evite abrir arquivos suspeitos ou inesperados, mesmo de contatos conhecidos.
- **Mantenha a Segurança do Endpoint**: Utilize soluções de antivírus e detecção de endpoint atualizadas para identificar e bloquear tentativas de exploração.

  Monitore os Avisos de Segurança: Mantenha-se informado sobre as ameaças emergentes e atualizações da Microsoft e comunidades de segurança cibernética.

Para saber informações mais detalhadas sobre esta vulnerabilidade acesse: https://cybersecuritynews.com/outlook-remote-code-execution-vulnerability/

2.5 Microsoft alerta sobre vulnerabilidade no Active Directory Certificate Services (AD CS) que pode causar interrupção de serviço

A Microsoft emitiu um alerta de segurança sobre uma vulnerabilidade no Active Directory Certificate Services (AD CS), identificada como CVE-2025-29968. Essa falha pode permitir que atacantes autenticados causem interrupções nos serviços de gerenciamento de certificados, afetando operações críticas em ambientes Windows. A Microsoft recomenda a aplicação imediata de atualizações para mitigar os riscos.

Exploração

A vulnerabilidade, classificada como "Importante" com pontuação CVSS v3.1 de 6.5, reside na validação inadequada de entradas no AD CS (CWE-20). Ela permite ataques de negação de serviço (DoS) contra servidores AD CS. A exploração da falha pode levar à interrupção de serviços essenciais, como o serviço de inscrição web da Autoridade de Certificação, tornando o sistema temporariamente inoperante.

Mitigação e Prevenção

Para se proteger contra essa vulnerabilidade, a Cisco recomenda as seguintes ações:

- Aplicar as atualizações de segurança da Microsoft imediatamente aos servidores AD CS, priorizando aqueles que lidam com um grande volume de solicitações de certificado.
- Auditar os logs de autenticação em busca de uso incomum de credenciais, especialmente em contas com direitos de inscrição de certificado, mas com poucos privilégios administrativos.
- Segmentar os servidores AD CS atrás de firewalls para restringir o acesso a usuários e sistemas autorizados, reduzindo a superfície de ataque.
- Desativar interfaces de inscrição web do AD CS não utilizadas e impor controles de acesso à rede rigorosos, se a aplicação imediata da correção não for possível.
- Implementar ferramentas de monitoramento para sinalizar falhas repetidas em solicitações de certificado ou reinicializações inesperadas de serviços, indicando possíveis tentativas de exploração.

  Implementar limitação de taxa de emissão de certificado e detecção de anomalias nos padrões de inscrição como medida de defesa em profundidade.

Para saber informações mais detalhadas sobre esta vulnerabilidade acesse: https://gbhackers.com/microsoft-alerts-on-ad-cs-flaw/

2.6 Falha no Microsoft Defender permite elevação de privilégios, alertam especialistas

Uma nova falha de segurança no Microsoft Defender for Endpoint pode permitir que invasores com acesso local elevem seus privilégios ao nível do sistema (SYSTEM). A vulnerabilidade, identificada como CVE-2025-26684, foi corrigida nas atualizações de segurança de maio de 2025 da Microsoft. A falha, com pontuação CVSS de 6.7, exige atenção imediata para evitar comprometimentos.

Exploração

A vulnerabilidade CVE-2025-26684 reside em uma falha de "controle externo de nome de arquivo ou caminho" no Microsoft Defender for Endpoint. Ela permite que um invasor autorizado manipule operações de arquivos para acessar recursos restritos do sistema. A exploração bem-sucedida concede aos invasores privilégios SYSTEM, possibilitando a instalação de programas, modificação/exclusão de dados e criação de contas administrativas completas. A falha afeta as versões do Microsoft Defender for Endpoint para Linux anteriores a 101.25XXX.

Mitigação e Prevenção:

- **Administradores de Sistema**: Aplicar imediatamente a atualização de segurança mais recente do Microsoft Defender for Endpoint. * Verificar a instalação da atualização usando o MDE Client Analyzer em dispositivos possivelmente afetados. * Monitorar tentativas suspeitas de elevação de privilégios e atividades incomuns no nível do sistema
- **Usuários Finais**: Garantir que os administradores de TI de sua organização apliquem as atualizações de segurança a tempo e reportar quaisquer atividades suspeitas ou anormais no sistema aos administradores de TI.

Para saber informações mais detalhadas sobre esta vulnerabilidade acesse: https://cybersecuritynews.com/microsoft-defender-vulnerability-allows-attackers/.

2.7 Fortinet alerta sobre vulnerabilidade crítica no FortiVoice com Exploração Ativa

A Fortinet divulgou uma vulnerabilidade crítica de estouro de buffer (CVE-2025-32756) em vários de seus produtos, com exploração ativa em sistemas FortiVoice. A falha permite que atacantes remotos executem código arbitrário através de requisições HTTP maliciosas, concedendo potencialmente controle total sobre os dispositivos afetados. É crucial que usuários e administradores de sistemas tomem medidas imediatas para mitigar os riscos.

Exploração

A vulnerabilidade, classificada com uma pontuação CVSS de 9.6, reside em um estouro de buffer baseado em pilha, afetando produtos como FortiVoice, FortiMail, FortiNDR, FortiRecorder e FortiCamera. Ela permite que atacantes não autenticados executem comandos ou códigos arbitrários por meio de requisições HTTP especialmente criadas. Ataques observados incluem reconhecimento

de rede, exclusão de logs para ocultar atividades maliciosas e a habilitação de depuração FCGI para capturar credenciais.

Mitigação e Prevenção

- **Atualização Imediata:** A Fortinet recomenda fortemente que os usuários atualizem para as versões mais recentes corrigidas dos produtos afetados o mais rápido possível.
- **Desabilite as interfaces administrativas HTTP/HTTPS:** Como solução temporária, desabilitar as interfaces administrativas HTTP/HTTPS pode mitigar o risco para organizações que não podem atualizar imediatamente.
- **Monitoramento:** Monitore os logs do sistema em busca de atividades suspeitas, incluindo as entradas mencionadas nos IOCs.

Para saber informações mais detalhadas sobre esta vulnerabilidade acesse: https://cybersecuritynews.com/fortivoice-0-day-vulnerability/

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: Comitê Editorial de Segurança da Service Sec