Your IT Company

Principais Vulnerabilidades e Ameaças (Novembro/25)

Sumário

1. Objetivo 2
2. Vulnerabilidades e Ameaças descobertas 2
2.1. CISA alerta sobre exploração ativa de vulnerabilidade Zero-Day no Kernel do Windows 2
2.2. Vulnerabilidade crítica no Windows Remote Desktop Services (RDS) permite elevação de privilégios 2
2.3. Alerta crítico: Vulnerabilidade em Firewalls Palo Alto permite ataques remotos de negação de serviço (DoS) 3
2.4. Ataque ClickFix: Nova campanha engana usuários com falsa atualização do Windows 4
2.5. Vulnerabilidade crítica de injeção SQL no SQL Server da Microsoft expõe dados a ataques remotos . 5

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. CISA alerta sobre exploração ativa de vulnerabilidade Zero-Day no Kernel do Windows

A CISA emitiu um alerta urgente sobre a exploração ativa de uma nova vulnerabilidade zero-day, identificada como CVE-2025-62215, no Kernel do Windows. Esta falha de segurança, que se aproveita de uma condição de corrida, permite que atacantes elevem seus privilégios no sistema, concedendo-lhes controle total sobre o dispositivo. A vulnerabilidade é particularmente perigosa devido à ausência de correções prévias, tornando sistemas não corrigidos alvos fáceis.

Exploração

A vulnerabilidade CVE-2025-62215 reside no Kernel do Windows, caracterizando-se por uma condição de corrida. Essa condição ocorre quando múltiplos processos acessam recursos compartilhados de maneira que causa comportamentos inesperados. No contexto da exploração, um atacante local, alguém com acesso limitado ao sistema, pode explorar essa falha para obter privilégios de nível SYSTEM, o mais alto nível de acesso no Windows. Isso concede ao atacante controle total sobre o dispositivo afetado, permitindo a instalação de programas, visualização e modificação de dados sensíveis, ou criação de novas contas com direitos completos de usuário.

Mitigação e Prevenção

- **Aplique as atualizações da Microsoft:** Instale os patches e as mitigações da Microsoft assim que estiverem disponíveis.
- **Siga as diretrizes da CISA:** Se estiver utilizando serviços baseados em nuvem, siga as orientações da CISA (BOD 22-01).
- **Descontinue o uso temporariamente:** Se não for possível aplicar os patches, considere interromper o uso dos serviços ou sistemas afetados até que uma correção seja lançada.
- **Mantenha-se atualizado:** Monitore ativamente seus sistemas em busca de atividades suspeitas ou sinais de comprometimento relacionados a essa vulnerabilidade.

Para saber informações mais detalhadas sobre esta vulnerabilidade acesse: https://gbhackers.com/cisa-warns-of-active-exploitation-of-windows-kernel-0-day/.

2.2. Vulnerabilidade crítica no Windows Remote Desktop Services (RDS) permite elevação de privilégios

A Microsoft revelou uma falha significativa no Windows Remote Desktop Services (RDS), identificada como CVE-2025-60703, que pode permitir que atacantes autorizados elevem seus privilégios. Esta vulnerabilidade, classificada como "Importante", é resultado de uma falha na

Classificação: Público

segurança da memória e afeta diversas versões do Windows, incluindo Windows 10, 11 e edições Server. A exploração bem-sucedida pode levar ao acesso de nível SYSTEM.

Exploração

A vulnerabilidade CVE-2025-60703 reside no Windows RDS, um protocolo amplamente utilizado para acesso remoto a sistemas Windows. A falha, classificada como CWE-822 (Untrusted Pointer Dereference), ocorre quando o software não valida um ponteiro antes de acessá-lo, levando a uma possível corrupção de memória. Um atacante local, com credenciais já comprometidas, pode explorar essa falha para obter privilégios elevados, potencialmente alcançando acesso de nível SYSTEM. Embora a exploração seja considerada "improvável" no momento, devido à necessidade de autenticação local, o risco é significativo em ambientes multiusuário, como redes corporativas.

Mitigação e Prevenção

- **Aplique os patches da Microsoft imediatamente:** As atualizações de segurança estão sendo distribuídas via Windows Update.
- **Priorize a atualização em ambientes críticos:** Especialmente em infraestruturas que dependem do RDS para VDI (Virtual Desktop Infrastructure) ou administração remota.
- **Implemente o princípio do menor privilégio:** Garanta que os usuários tenham apenas os acessos necessários para suas tarefas.
- **Monitore atividades suspeitas:** Fique atento a tentativas incomuns de elevação de privilégios.
- **Segmente a rede:** Limite a movimentação lateral de possíveis invasores, segmentando a rede.
- **Teste os patches em um ambiente de teste:** Antes de implantar as atualizações em produção, teste-as para evitar interrupções.

Para saber informações mais detalhadas sobre esta vulnerabilidade acesse: https://cybersecuritynews.com/windows-remote-desktop-services-flaw/.

2.3. Alerta crítico: Vulnerabilidade em Firewalls Palo Alto permite ataques remotos de negação de serviço (DoS)

Uma vulnerabilidade crítica de Negação de Serviço (DoS) foi descoberta nos firewalls PAN-OS da Palo Alto Networks, identificada como CVE-2025-4619. Essa falha permite que invasores não autenticados reiniciem remotamente os firewalls enviando pacotes especialmente criados. A vulnerabilidade afeta várias versões do PAN-OS e exige atenção imediata devido ao seu potencial de interrupção nas operações de rede.

Exploração

A vulnerabilidade, classificada como CWE-754 (Verificação inadequada para condições incomuns ou excepcionais), reside no dataplane do software PAN-OS. Ataques bem-sucedidos resultam na reinicialização inesperada do firewall, com tentativas repetidas podendo forçá-lo ao modo de manutenção, interrompendo severamente as operações de rede. A exploração não requer autenticação ou interação do usuário, tornando-a particularmente perigosa. A vulnerabilidade afeta

Classificação: Público

firewalls PA-Series, VM-Series e implantações Prisma Access que executam versões PAN-OS vulneráveis, incluindo as versões 10.2 (até 10.2.13), 11.1 (até 11.1.6) e 11.2 (até 11.2.4).

Mitigação e Prevenção

- A Palo Alto Networks recomenda que os usuários atualizem para as versões corrigidas do PAN-OS.
- As versões 11.2 devem ser atualizadas para 11.2.5 ou posterior; as versões 11.1 devem ser atualizadas para 11.1.7; e os usuários da versão 10.2 devem aplicar a correção para 10.2.14.
- É crucial priorizar a aplicação dos patches, dada a facilidade de exploração e o impacto potencial nas operações.

Para saber informações mais detalhadas sobre esta vulnerabilidade acesse: https://cybersecuritynews.com/palo-alto-pan-os-firewall-vulnerability/

2.4. Ataque ClickFix: Nova campanha engana usuários com falsa atualização do Windows

Uma nova campanha ClickFix, denominada "Fake OS Update", está enganando usuários com uma falsa atualização do Windows que opera diretamente no navegador. Esta tática explora a confiança dos usuários na tela azul da morte (BSOD) da Microsoft, com o objetivo de instalar malware através de engenharia social.

Exploração

A campanha "Fake OS Update" se propagam principalmente através do domínio groupewadesecurity[.]com, acionado ao visitar o site por meio de malvertising ou links maliciosos. A página simula uma tela de erro ou atualização do Windows em tela cheia, exibindo códigos de erro e barras de progresso, tanto em computadores quanto em smartphones. As vítimas são então instruídas a realizar três "correções manuais" usando atalhos de teclado, que, na verdade, concedem acesso remoto aos atacantes ou instalam infostealers e ransomware.

Mitigação e Prevenção

- **Usuários**:
  - Desconfie de alertas e atualizações inesperadas, especialmente aquelas que solicitam ações urgentes ou instalação de software de fontes desconhecidas.
  - Não execute comandos ou baixe arquivos de sites suspeitos.
  - Mantenha o navegador e o sistema operacional atualizados.
  - Considere o uso de extensões de navegador como uBlock Origin para bloquear domínios maliciosos.
- **Administradores de sistema:**
  - Implemente programas de conscientização sobre segurança cibernética, simulando cenários como este.

Classificação: Público

- Monitore o tráfego da rede em busca de atividades suspeitas relacionadas aos domínios e IOCs identificados.
- Bloqueie o acesso a domínios maliciosos em nível de rede.

Para saber informações mais detalhadas sobre esta vulnerabilidade acesse: https://cybersecuritynews.com/clickfix-attack-fake-os-update/.

2.5. Vulnerabilidade crítica de injeção SQL no SQL Server da Microsoft expõe dados a ataques remotos

A Microsoft divulgou uma vulnerabilidade crítica de injeção SQL no SQL Server (CVE-2025-59499) que permite a invasores autenticados elevarem seus privilégios através da rede. A falha, classificada como "Importante" e com pontuação CVSS 3.1 de até 8.8, permite acesso não autorizado a dados confidenciais, exigindo ação imediata dos administradores de banco de dados.

Exploração

A vulnerabilidade reside na falha de neutralização de elementos especiais em comandos SQL, possibilitando a execução de código SQL arbitrário com privilégios elevados. Isso permite que atacantes manipulem, extraiam ou excluam dados sensíveis. A exploração é feita remotamente, através da rede, exigindo apenas credenciais válidas do SQL Server. A vulnerabilidade não requer interação do usuário e é de baixa complexidade, tornando-a um alvo fácil para invasores.

Mitigação e Prevenção

- Priorizar a aplicação de patches da Microsoft em todas as instâncias afetadas do SQL Server.
- Revisar e fortalecer os controles de acesso, implementando o princípio do menor privilégio.
- Monitorar os logs do SQL Server em busca de padrões de consulta suspeitos e tentativas de elevação de privilégios.
- Coordenar a aplicação de patches com os administradores de banco de dados, seguindo um cronograma de manutenção regular.

Para saber informações mais detalhadas sobre esta vulnerabilidade acesse: https://gbhackers.com/critical-blink-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 quinzenalmente.

Produzido por: Equipe de Threat Intelligence da Service IT Security

Classificação: Público