Your IT Company

Principais Vulnerabilidades e Ameaças (dezembro/25)

Sumário

1. Objetivo 2
2. Vulnerabilidades e Ameaças descobertas 2
2.1. Vulnerabilidades críticas no Cisco Unified Contact Center Express (CCX) 2
2.2. Vulnerabilidade no Windows Cloud Files Mini Filter Driver explorada ativamente 2
2.3. Fortinet FortiWeb: Vulnerabilidade de injeção de comandos explorada em ataques reais 3
2.4. Fortinet FortiGate sob ataque ativo por bypass de autenticação SAML SSO 4
2.5. Vulnerabilidade crítica no Apache Commons Text permite execução remota de código 4
2.6. Ataques de password spraying miram gateways VPN Cisco e Palo Alto Networks 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. Vulnerabilidades críticas no Cisco Unified Contact Center Express (CCX)

O Cisco Unified Contact Center Express (CCX) é uma solução amplamente utilizada para gerenciamento de centrais de atendimento, integrando telefonia IP, automação de fluxos de chamadas e administração centralizada. Recentemente, foram identificadas vulnerabilidades críticas que afetam componentes internos do CCX responsáveis pela comunicação remota e pelo gerenciamento administrativo da plataforma.

Essas falhas permitem que atacantes não autenticados comprometam o sistema, resultando em execução remota de código, bypass de autenticação e possível controle total do ambiente. Devido à natureza do CCX frequentemente integrado a infraestruturas críticas de comunicação corporativa a exploração dessas vulnerabilidades representa um risco elevado de interrupção de serviços, vazamento de informações sensíveis e movimentação lateral na rede.

Exploração

A exploração ocorre por meio do envio de requisições especialmente manipuladas a serviços internos expostos pelo CCX, incluindo interfaces baseadas em Java RMI e componentes administrativos. Um atacante pode explorar essas falhas para enviar arquivos maliciosos, executar scripts arbitrários e obter privilégios elevados no sistema operacional subjacente.

Em cenários mais graves, a exploração bem-sucedida permite ao invasor assumir controle administrativo completo, modificar configurações do contact center, interceptar fluxos de chamadas, acessar dados sensíveis de clientes e utilizar o sistema como ponto de pivô para ataques a outros ativos da rede corporativa.

Mitigação e Prevenção

- Aplicar imediatamente as atualizações de segurança disponibilizadas pela Cisco.
- Restringir o acesso aos serviços administrativos do CCX apenas a redes confiáveis.
- Monitorar logs de autenticação e execução de comandos suspeitos.
- Implementar segmentação de rede para isolar o ambiente de contact center.

Para saber informações mais detalhadas sobre esta vulnerabilidade acesse: https://cybersecuritynews.com/cisco-unified-contact-center-vulnerabilities .

2.2. Vulnerabilidade no Windows Cloud Files Mini Filter Driver explorada ativamente

O Windows Cloud Files Mini Filter Driver (cldflt.sys) é um componente crítico do sistema operacional Windows, responsável por gerenciar a integração entre arquivos locais e serviços de

Classificação: Público

armazenamento em nuvem, como o Microsoft OneDrive. A CISA alertou sobre a exploração ativa de uma vulnerabilidade nesse driver, classificada como uma falha de elevação de privilégios locais.

Por se tratar de um driver em modo kernel, qualquer falha explorável nesse componente amplia significativamente o impacto de ataques, permitindo que um usuário mal-intencionado eleve privilégios até o nível SYSTEM, comprometendo completamente a integridade, confidencialidade e disponibilidade do sistema afetado.

Exploração

A vulnerabilidade é explorada por meio de uma condição de use-after-free, onde o sistema acessa regiões de memória já liberadas de forma inadequada. Um atacante com acesso local inicial seja por credenciais comprometidas, malware ou outro vetor, pode manipular o comportamento do driver para executar código arbitrário no kernel.

Essa técnica é frequentemente utilizada como etapa pós-exploração, permitindo que agentes maliciosos desativem mecanismos de segurança, instalem rootkits, mantenham persistência avançada ou executem outras ações maliciosas com privilégios máximos no sistema.

Mitigação e Prevenção

- Aplicar imediatamente os patches de segurança da Microsoft.
- Monitorar eventos de escalonamento de privilégios locais.
- Utilizar soluções EDR para detectar exploração de drivers do kernel.
- Restringir privilégios de usuários locais sempre que possível.

Para saber informações mais detalhadas sobre esta vulnerabilidade acesse: https://cybersecuritynews.com/cisa-warns-of-windows-cloud-files-mini-filter-vulnerability-exploited.

2.3. Fortinet FortiWeb: Vulnerabilidade de injeção de comandos explorada em ataques reais

O Fortinet FortiWeb é um Web Application Firewall (WAF) projetado para proteger aplicações web contra ataques como SQL Injection, XSS e exploração de vulnerabilidades conhecidas. No entanto, foi identificada uma vulnerabilidade crítica de injeção de comandos no sistema operacional do FortiWeb, que foi posteriormente incluída pela CISA em seu catálogo de vulnerabilidades exploradas ativamente. Essa falha compromete diretamente a confiabilidade do dispositivo, pois permite que um atacante execute comandos arbitrários no sistema subjacente, colocando em risco não apenas o próprio WAF, mas também toda a infraestrutura que ele protege.

Exploração

A exploração ocorre quando um atacante autenticado envia entradas maliciosas a funcionalidades vulneráveis da interface de gerenciamento do FortiWeb. Essas entradas não são devidamente sanitizadas, permitindo a injeção e execução de comandos no sistema operacional do appliance.

Uma vez explorada, a vulnerabilidade pode ser utilizada para alterar configurações críticas, desativar proteções do WAF, criar contas administrativas ocultas, instalar backdoors persistentes ou usar o dispositivo como ponto de entrada para ataques mais amplos dentro da rede corporativa.

Classificação: Público

Mitigação e Prevenção

- Atualizar imediatamente o FortiWeb OS para versões corrigidas.
- Restringir o acesso administrativo às redes internas confiáveis.
- Monitorar logs do sistema para comandos não autorizados.
- Revisar contas administrativas e aplicar o princípio do menor privilégio.

Para saber informações mais detalhadas sobre esta vulnerabilidade acesse: https://cybersecuritynews.com/cisa-fortinet-fortiweb-vulnerability-2/.

2.4. Fortinet FortiGate sob ataque ativo por bypass de autenticação SAML SSO

Os dispositivos Fortinet FortiGate, amplamente utilizados como firewalls de perímetro e gateways de segurança, estão sendo alvo de ataques ativos explorando falhas críticas no mecanismo de autenticação SAML Single Sign-On (SSO). Essas vulnerabilidades afetam ambientes que utilizam FortiCloud SSO, permitindo o contorno completo dos mecanismos de autenticação.

Dado o papel central do FortiGate na proteção do tráfego de rede, a exploração dessas falhas representa um risco severo, podendo resultar em acesso administrativo não autorizado, exposição de configurações sensíveis e comprometimento total da postura de segurança da organização.

Exploração

Os atacantes exploram falhas na validação de mensagens SAML, enviando tokens manipulados que são aceitos como legítimos pelo FortiGate. Esse bypass permite que o invasor se autentique como administrador sem a necessidade de credenciais válidas.

Após obter acesso, foram observadas atividades como exportação completa das configurações do firewall, possibilitando o roubo de credenciais armazenadas, regras de segurança, certificados e informações de topologia de rede. Essas informações podem ser usadas para ataques subsequentes, movimentação lateral ou comprometimento de outros dispositivos.

Mitigação e Prevenção

- Atualizar imediatamente o FortiOS para versões corrigidas.
- Desabilitar temporariamente o FortiCloud SSO, se possível.
- Restringir o acesso à interface administrativa (GUI/SSH).
- Redefinir credenciais administrativas após qualquer suspeita de comprometimento.

Para saber informações mais detalhadas sobre esta vulnerabilidade acesse: https://thehackernews.com/2025/12/fortinet-fortigate-under-active-attack.html.

2.5. Vulnerabilidade crítica no Apache Commons Text permite execução remota de código

O Apache Commons Text é uma biblioteca Java amplamente utilizada para manipulação e interpolação de strings em aplicações corporativas. Uma vulnerabilidade crítica foi identificada em seu mecanismo de interpolação, permitindo que expressões maliciosas sejam processadas quando dados não confiáveis são utilizados.

Devido à ampla adoção da biblioteca, essa falha possui um alto potencial de impacto, afetando aplicações web, APIs e serviços corporativos que utilizam o componente de forma indireta.

Classificação: Público

Exploração

A exploração ocorre quando entradas controladas pelo usuário são processadas pelo mecanismo de interpolação sem validação adequada. Expressões maliciosas podem acionar chamadas a serviços remotos ou executar comandos no sistema subjacente, resultando em execução remota de código.

Em aplicações expostas à internet, essa falha pode ser explorada remotamente e sem autenticação, permitindo o comprometimento completo do servidor e o acesso não autorizado a dados sensíveis.

Mitigação e Prevenção

- Atualizar imediatamente o Apache Commons Text para versões corrigidas.
- Evitar o uso de interpolação dinâmica com entradas não confiáveis.
- Implementar validação rigorosa de dados.
- Monitorar logs de aplicação para padrões anômalos.

Para saber informações mais detalhadas sobre esta vulnerabilidade acesse: https://gbhackers.com/critical-apache-commons-text-flaw-lets-hackers-execute-remote-code/ .

2.6. Ataques de password spraying miram gateways VPN Cisco e Palo Alto Networks

Pesquisadores identificaram uma campanha em larga escala de ataques de password spraying direcionada a gateways VPN corporativos, incluindo Cisco SSL VPN e Palo Alto Networks GlobalProtect. A técnica consiste em testar senhas comuns ou reutilizadas contra múltiplas contas de usuários, explorando falhas em políticas de autenticação e ausência de MFA.

A campanha foi caracterizada por milhões de tentativas de login automatizadas, originadas de milhares de endereços IP distintos, indicando um esforço coordenado para obtenção de acesso inicial a redes corporativas expostas à internet.

Exploração

A exploração observada se caracteriza como uma atividade de reconhecimento e credenciais, e não envolve exploração de vulnerabilidades de softwares específicos. As requisições de login seguem o fluxo de autenticação legítimo dos serviços SSL VPN incluindo o tratamento de tokens CSRF o que indica que os atacantes estão tentando nomes de usuário e senhas comuns para acessar interfaces administrativas e de login VPN.

As tentativas de login com credenciais repetidas e uso de um user agent atípico (Firefox) para atividade automatizada sugerem que a campanha foi executada por meio de scripts personalizados, focados em identificar serviços de VPN com proteções fracas de senha ou ausência de mecanismos de defesa robustos

Autoridades da Palo Alto Networks confirmaram que essa atividade foi classificada como tentativas automatizadas de credenciais, sem indicação de falha ou exploração de vulnerabilidade no PAN-OS ou nos portais GlobalProtect.

Mitigação e Prevenção

- Habilitar autenticação multifator (MFA) em todos os acessos VPN.

Classificação: Público

- Implementar políticas de senha fortes e impedir reutilização de credenciais.
- Monitorar e alertar sobre picos anômalos de falhas de login.
- Aplicar rate limiting e bloqueio temporário de IPs suspeitos.
- Restringir o acesso VPN a redes ou endereços confiáveis sempre que possível.

Para saber informações mais detalhadas sobre esta vulnerabilidade acesse: https://www.bleepingcomputer.com/news/security/new-password-spraying-attacks-target-cisco-pan-vpn-gateways/ .

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