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. CVE-2026-69485 - Falha de RCE no Windows Remote Desktop Client

A Microsoft corrigiu a CVE-2026-69485, uma vulnerabilidade de execução remota de código no Windows Remote Desktop Client, causada pelo uso de um recurso não inicializado (CWE-908). A falha possui CVSS 3.1 de 8.8 (Alta).

A vulnerabilidade afeta diversas versões do Windows 10, Windows 11 e Windows Server, incluindo Windows Server 2016, 2019, 2022 e 2025, quando não atualizadas para as versões corrigidas.

Exploração

Um atacante autenticado com baixos privilégios pode enviar uma requisição de rede especialmente criada para atingir o componente vulnerável do Remote Desktop Client e provocar uma condição que possibilite execução arbitrária de código no sistema afetado. A exploração não exige interação do usuário.

A exploração bem-sucedida pode resultar em comprometimento da confidencialidade, integridade e disponibilidade do sistema, podendo servir como etapa para persistência, movimentação lateral ou comprometimento de servidores.

Mitigação e Prevenção

- **Recomendações imediatas:**
  - Aplicar imediatamente as atualizações de segurança de setembro de 2026.
  - Priorizar servidores e estações que utilizam recursos de Remote Desktop.
  - Validar se sistemas expostos ou críticos estão executando versões corrigidas.
- **Recomendações para Administradores de Sistema:**
  - Implementar as atualizações Microsoft correspondentes à CVE-2026-69485.
  - Restringir o acesso ao RDP e aos serviços relacionados somente a redes e usuários autorizados.
  - Monitorar eventos de autenticação e conexões RDP anômalas.
  - Correlacionar atividades suspeitas do Remote Desktop Client com criação de processos ou conexões de saída incomuns.
- **Recomendações para Usuários Finais:**
  - Manter o Windows atualizado e reiniciar o equipamento quando solicitado.
  - Não utilizar contas administrativas para atividades rotineiras.

- Reportar comportamentos incomuns após conexões remotas.

Para saber informações mais detalhadas sobre esta vulnerabilidade acesse: https://cybersecuritynews.com/windows-remote-desktop-client-rce-vulnerability/.

2.2. CVE-2026-26084 - FortiSandbox: Acesso indevido a informações sensíveis

A CVE-2026-26084 é uma vulnerabilidade de controle de acesso inadequado (CWE-284) no Fortinet FortiSandbox. A falha permite que um atacante acesse informações sensíveis por meio de requisições HTTP especialmente elaboradas. O problema possui CVSS 3.1 de 8.9 (Alta) e não exige autenticação ou interação do usuário.

São afetados FortiSandbox 4.4.0–4.4.8 e 5.0.0–5.0.5, além de determinadas versões do FortiSandbox Cloud e PaaS.

Exploração

A exploração ocorre remotamente por meio do envio de requisições HTTP manipuladas aos componentes vulneráveis. A ausência adequada de verificações de autorização pode permitir que um atacante não autenticado obtenha acesso a informações que deveriam estar restritas. Não há evidências públicas, até o momento, de exploração da CVE-2026-26084 em ambiente real.

O acesso indevido pode expor informações armazenadas ou processadas pelo sandbox, potencialmente fornecendo aos atacantes dados úteis para reconhecimento, preparação de ataques e comprometimento de outros ativos.

Mitigação e Prevenção

- **Recomendações imediatas:**
  - Atualizar o FortiSandbox para uma versão corrigida.
  - Remover a exposição direta das interfaces administrativas à Internet.
  - Revisar logs HTTP em busca de requisições anômalas.
- **Recomendações para Administradores de Sistema:**
  - FortiSandbox 4.4: atualizar para **4.4.9 ou superior**.
  - FortiSandbox 5.0: atualizar para **5.0.6 ou superior**.
  - FortiSandbox Cloud: atualizar para **5.0.6 ou superior**.
  - Restringir as interfaces de gerenciamento a redes administrativas confiáveis.
  - Monitorar acessos não usuais aos endpoints HTTP/API.
  - Investigar qualquer exposição de informações sensíveis caso o equipamento tenha permanecido acessível externamente.

Para saber informações mais detalhadas sobre esta vulnerabilidade acesse: https://cybersecuritynews.com/fortisandbox-vulnerability-access-sensitive-data/.

2.3. CVE-2026-59346 e CVE-2026-59347 - Vulnerabilidades críticas no VMware Workstation e Fusion

A Broadcom corrigiu duas vulnerabilidades no VMware Workstation e VMware Fusion. A mais grave, CVE-2026-59346, possui CVSS 3.1 de 9.3 (Crítica**)** e corresponde a um integer overflow relacionado ao adaptador de rede VMXNET3.

Também foi corrigida a CVE-2026-59347, uma vulnerabilidade de stack-based buffer overflow no componente HGFS, com CVSS 3.1 de 8.1.

Exploração

A CVE-2026-59346 pode ser explorada por um atacante que já possua privilégios administrativos locais dentro de uma máquina virtual utilizando VMXNET3, possibilitando a execução de código no **host**. A CVE-2026-59347 também exige privilégios administrativos locais na VM e pode permitir execução de código com os privilégios do processo VMX no host.

Embora as vulnerabilidades dependam de privilégios prévios dentro da VM, um comprometimento anterior por phishing, malware ou configuração inadequada pode fornecer esse nível de acesso.

O principal risco é a quebra do isolamento entre guest e host, permitindo que um invasor que tenha comprometido uma máquina virtual avance para o sistema hospedeiro e, potencialmente, para outras VMs.

Mitigação e Prevenção

- **Recomendações imediatas:**
  - Atualizar VMware Workstation e Fusion imediatamente.
  - Priorizar hosts utilizados para ambientes de desenvolvimento, testes ou processamento de informações sensíveis.
  - Avaliar VMs onde existam contas com privilégios administrativos.
- **Recomendações para Administradores de Sistema:**
  - Atualizar para VMware Workstation 26H1u1 ou superior.
  - Atualizar para VMware Fusion 26H1u1 ou superior.
  - Não há workaround disponibilizado pela Broadcom para essas falhas.
  - Aplicar princípio do menor privilégio nas VMs.
  - Restringir o uso desnecessário de contas administrativas.
  - Monitorar processos executados dentro das VMs e atividades anormais no host.
- **Recomendações para Usuários Finais:**
  - Evitar executar softwares desconhecidos com privilégios administrativos dentro de VMs.

Para saber informações mais detalhadas sobre esta vulnerabilidade acesse: https://thehackernews.com/2026/09/critical-vmware-workstation-and-fusion.html.

2.4. CVE-2026-69449 - Vulnerabilidade de RCE no Windows BitLocker

A CVE-2026-69449 é uma vulnerabilidade de heap-based buffer overflow (CWE-122) no Windows BitLocker, classificada pela Microsoft como Important e com CVSS 3.1 de 6.7. A exploração pode resultar em execução de código no sistema afetado.

Exploração

A vulnerabilidade possui vetor local, baixa complexidade e exige privilégios elevados. Dessa forma, não representa uma vulnerabilidade de RCE diretamente explorável pela Internet, mas pode ser utilizada por um invasor que já tenha obtido privilégios suficientes no sistema.

Um atacante que já possua privilégios elevados pode explorar a falha para executar código, ampliando o comprometimento do endpoint e potencialmente facilitando persistência ou ações pós-exploração.

Mitigação e Prevenção

- **Recomendações imediatas:**
  - Aplicar as atualizações de segurança de setembro de 2026.
  - Priorizar dispositivos corporativos que utilizam BitLocker.
  - Confirmar a instalação dos patches nos endpoints críticos.
- **Recomendações para administradores de sistema:**
  - Distribuir as atualizações Microsoft correspondentes à CVE-2026-69449.
  - Verificar a conformidade dos endpoints por meio de ferramentas de gerenciamento de patches.
  - Manter o BitLocker habilitado e utilizar proteção adequada das chaves de recuperação.
  - Restringir privilégios administrativos locais.
  - Monitorar elevação de privilégios e execução de processos incomuns.
- **Recomendações para Usuários Finais:**
  - Não fornecer credenciais administrativas para aplicações desconhecidas.
  - Manter o Windows atualizado.
  - Comunicar perda ou comprometimento de dispositivos corporativos imediatamente.

Para saber informações mais detalhadas sobre esta vulnerabilidade acesse: https://gbhackers.com/windows-bitlocker-flaw-2/.

2.5. CVE-2026-83548 e CVE-2026-83549 - Zero-Days do SonicWall SMA 1000 podem formar uma cadeia de ataque

A SonicWall corrigiu duas vulnerabilidades **zero-day** no Secure Mobile Access (SMA) 1000 que já foram exploradas em ataques.

- **CVE-2026-83548 — CVSS 10.0:** SSRF pré-autenticação no Appliance Work Place.

- **CVE-2026-83549 — CVSS 7.8:** command injection pós-autenticação no Appliance Management Console (AMC).

Os problemas afetam os modelos SMA 6210, 7210 e 8200v em determinadas versões 12.4.3 e 12.5.0.

Exploração

A CVE-2026-83548 pode permitir que um atacante remoto não autenticado alcance funcionalidades internas do appliance. A segunda vulnerabilidade pode então ser utilizada por um atacante autenticado como administrador para executar comandos arbitrários.

A combinação das duas vulnerabilidades pode formar uma cadeia de ataque capaz de levar ao comprometimento do appliance.

O comprometimento de um equipamento SMA é especialmente crítico por sua posição de perímetro. Um atacante pode obter acesso privilegiado ao dispositivo e potencialmente utilizá-lo como ponto de entrada para recursos internos.

Mitigação e Prevenção

- **Recomendações imediatas:**
  - Atualizar imediatamente os appliances afetados.
  - Investigar o dispositivo em busca de comprometimento antes de considerar a atualização suficiente.
  - Caso sejam identificados IOCs, realizar reimagem do appliance físico ou redeploy do appliance virtual.
  - Alterar senhas de usuários e administradores.
  - Resetar os tokens TOTP/MFA.
- **Recomendações para Administradores de Sistema:**
  - Atualizar para: 12.4.3-03526 ou superior; ou 12.5.0-02952 ou superior.
  - Restringir a exposição administrativa do SMA.
  - Monitorar autenticações originadas diretamente do appliance.
  - Investigar conexões do SMA para controladores de domínio e demais ativos internos.
  - Revisar credenciais armazenadas, sessões ativas e configurações de MFA após suspeita de comprometimento.
- **Recomendações para Usuários Finais:**
  - Caso utilizem o SMA para acesso remoto, reportar imediatamente comportamentos anômalos, solicitações inesperadas de autenticação ou problemas relacionados ao MFA.
  - Não reutilizar credenciais utilizadas em outros serviços.

Para saber informações mais detalhadas sobre esta vulnerabilidade acesse: Attackers Exploit Two SonicWall SMA 1000 Zero-Days That May Form an Attack Chain.

2.6. CVE-2026-9586 - Sangoma Switchvox: SQL Injection não autenticada para RCE

A CVE-2026-9586 é uma vulnerabilidade crítica de SQL Injection não autenticada no Sangoma Switchvox que pode levar à execução remota de código. A falha recebeu CVSS 4.0 de 9.3 e afeta o componente responsável por notificações para telefones. A vulnerabilidade foi corrigida no Switchvox 8.4.0.2, lançado em 14 de julho de 2026. A Horizon3 posteriormente observou tentativas válidas de exploração em honeypots expostos à Internet.

Exploração

O endpoint HTTP **/pa**, acessível sem autenticação, processa informações fornecidas pelo cliente e as insere diretamente em uma consulta PostgreSQL sem sanitização adequada.

Um atacante remoto pode manipular esse parâmetro para injetar comandos SQL e, em determinadas condições, alcançar execução de comandos no sistema operacional com privilégios elevados.

A exploração pode resultar em comprometimento completo do servidor Switchvox, permitindo execução de comandos, instalação de ferramentas maliciosas, coleta de informações e utilização do sistema como ponto de apoio para ataques posteriores.

Mitigação e Prevenção

- **Recomendações imediatas:**
  - Atualizar o Switchvox para 8.4.0.2 ou superior.
  - Priorizar instalações expostas diretamente à Internet.
  - Verificar os logs em busca de tentativas de exploração.
  - Caso seja identificado comprometimento, realizar investigação forense antes de simplesmente atualizar o sistema.
- **Recomendações para Administradores de Sistema:**
  - Remover a exposição desnecessária da interface web à Internet.
  - Restringir o acesso por firewall/VPN e permitir somente origens confiáveis.
  - Monitorar conexões de saída do servidor Switchvox.
  - Revisar processos e arquivos recentemente criados.
  - Correlacionar logs da aplicação com eventos de rede e criação de processos.
  - Restringir o acesso ao Switchvox por firewall, ACL ou VPN, evitando exposição desnecessária à Internet.
  - Permitir acesso administrativo somente a redes de gerenciamento ou endereços IP previamente autorizados.
  - Monitorar requisições direcionadas ao endpoint **/pa**, especialmente aquelas contendo parâmetros anormais ou caracteres associados a tentativas de SQL Injection.

- Monitorar o arquivo **/var/log/switchvox/db-quirks.log** em busca de consultas SQL anômalas.
- Monitorar processos executados pelo serviço do Switchvox e investigar processos filhos inesperados.
- Monitorar criação ou alteração de arquivos em diretórios temporários, especialmente **/tmp**.
- Monitorar conexões de saída originadas pelo servidor para endereços externos desconhecidos.
- Correlacionar eventos do Switchvox com firewall, IDS/IPS, EDR e SIEM.
- Aplicar o princípio do menor privilégio às contas administrativas.

Para saber informações mais detalhadas sobre esta vulnerabilidade acesse: CVE-2026-9586: Sangoma Switchvox RCE | Horizon3.

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