Your IT Company

Principais Vulnerabilidades e Ameaças (junho/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. Microsoft Defender – Zero-Day CVE-2026-41091 e CVE-2026-45498

A Microsoft corrigiu duas vulnerabilidades de dia zero identificadas no Microsoft Defender que estavam sendo exploradas ativamente por agentes maliciosos. A CVE-2026-41091 é uma falha de elevação de privilégios que permite que um invasor obtenha permissões de nível SYSTEM após comprometer um dispositivo. Já a CVE-2026-45498 afeta componentes internos do mecanismo de proteção do Defender, possibilitando interrupções no serviço de segurança e reduzindo a capacidade de detecção de ameaças.

Exploração

A exploração da CVE-2026-41091 exige acesso prévio ao equipamento, porém permite que um atacante amplie significativamente seus privilégios dentro do sistema operacional. Após a exploração bem-sucedida, atividades como instalação de malware, criação de contas administrativas e movimentação lateral tornam-se mais simples. Já a CVE-2026-45498 pode ser utilizada para interferir no funcionamento do Microsoft Defender, permitindo que códigos maliciosos sejam executados com menor probabilidade de detecção. A inclusão das falhas no catálogo Known Exploited Vulnerabilities (KEV) da CISA indica que ataques reais já foram observados.

Mitigação e Prevenção

- **Ações imediatas recomendadas:**
  - Aplicar os patches de segurança disponibilizados pela Microsoft.
  - Atualizar manualmente as assinaturas e os mecanismos do Microsoft Defender.
  - Verificar se existem sistemas sem atualização em ambientes corporativos.
- **Recomendações para Administradores de Sistema:**
  - Restringir privilégios administrativos locais.
  - Monitorar eventos relacionados à elevação de privilégios e alterações em serviços de segurança.
  - Revisar ferramentas EDR/XDR para identificar atividades suspeitas associadas às vulnerabilidades.
- **Recomendações para Usuários Finais:**
  - Evitar executar arquivos provenientes de fontes desconhecidas.
  - Manter o sistema operacional atualizado.
  - Reportar imediatamente comportamentos incomuns do equipamento.

Para saber informações mais detalhadas sobre esta vulnerabilidade acesse: https://threataft.com/articles/microsoft-defender-zero-days-cve-2026-41091-cve-2026-45498./

2.2. Sétimo Zero-Day do Cisco SD-WAN Permite Execução de Código como Root

A Cisco divulgou uma nova vulnerabilidade zero-day no Cisco Catalyst SD-WAN Manager, identificada como CVE-2026-20245. A falha afeta a interface de linha de comando (CLI) da plataforma e permite que um atacante autenticado com privilégios netadmin execute comandos arbitrários com privilégios de root por meio do envio de um arquivo especialmente manipulado.

Segundo a Cisco, a vulnerabilidade já foi observada em ataques reais e limitados, incluindo incidentes nos quais alterações de configuração foram propagadas para dispositivos de borda gerenciados pela solução.

Exploração

A exploração ocorre quando um usuário autenticado com privilégios administrativos envia um arquivo especialmente manipulado para o Cisco Catalyst SD-WAN Manager. Devido à falha na validação dos dados processados pelo CLI, comandos arbitrários podem ser executados diretamente no sistema operacional subjacente com privilégios de root. Uma vez comprometido, o ambiente pode permitir:

- Execução remota de comandos privilegiados;
- Alteração de configurações críticas da infraestrutura SD-WAN
- Modificação de políticas de roteamento e segurança
- Movimentação lateral para outros dispositivos da rede
- Implantação de mecanismos de persistência para manutenção do acesso

A Cisco confirmou a existência de exploração ativa da vulnerabilidade em ambiente real, tornando o risco significativamente mais elevado para organizações que utilizam a solução afetada.

Mitigação e Prevenção

- **Ações imediatas:**
  - Revisar imediatamente todas as contas com privilégios netadmin.
  - Alterar credenciais administrativas que possam ter sido expostas.
  - Restringir o acesso administrativo apenas a usuários autorizados.
  - Implementar autenticação multifator (MFA) sempre que possível.
  - Monitorar atividades administrativas incomuns no ambiente SD-WAN.
- **Recomendações para Administradores de Sistema:**
  - Coletar os arquivos admin-tech de todos os componentes de controle antes da aplicação de futuras atualizações.
  - Revisar os indicadores de comprometimento e orientações de logs fornecidos pela Cisco.
  - Monitorar uploads de arquivos suspeitos e execuções de comandos privilegiados.

- Investigar alterações inesperadas em dispositivos de borda.
- Garantir que vulnerabilidades relacionadas, como CVE-2026-20182 e CVE-2026-20127, estejam totalmente corrigidas em todo o ambiente.
- Caso seja identificado comprometimento, entrar em contato com o suporte da Cisco (TAC) para orientações específicas de resposta ao incidente.

- **Recomendações para Usuários Finais:**
  - Reportar imediatamente comportamentos incomuns nos serviços de rede.
  - Não compartilhar credenciais administrativas.
  - Utilizar senhas fortes e exclusivas para acessos privilegiados.
  - Seguir as políticas de segurança definidas pela organização para acessos remotos e administrativos.

Para saber informações mais detalhadas sobre esta vulnerabilidade acesse: https://threat-modeling.com/vulnerability-intelligence-report-june-1-2026/?utm_source.

2.3. Citrix NetScaler – CVE-2026-3055

A CVE-2026-3055 é uma vulnerabilidade crítica que afeta dispositivos Citrix NetScaler ADC e NetScaler Gateway configurados para atuar como provedores de identidade SAML. A falha está relacionada ao processamento inadequado de determinadas requisições, permitindo a exposição indevida de informações armazenadas na memória do dispositivo.

Exploração

A Pesquisadores observaram tentativas de exploração ativa da vulnerabilidade em dispositivos expostos à internet. Um invasor remoto pode explorar a falha para acessar dados sensíveis presentes na memória do equipamento, incluindo informações relacionadas a sessões autenticadas. Dependendo do cenário, isso pode facilitar o sequestro de sessões, acesso não autorizado a aplicações corporativas e movimentação lateral dentro da rede.

Mitigação e Prevenção

- **Ações imediatas:**
  - Atualizar os dispositivos NetScaler para as versões corrigidas.
  - Identificar equipamentos expostos diretamente à internet.
  - Revisar sessões ativas e renovar credenciais administrativas após a correção.
- **Recomendações para Administradores de Sistema:**
  - Monitorar logs de autenticação e acessos suspeitos.
  - Revisar integrações SAML e políticas de acesso.
  - Executar análises forenses caso existam indícios de exploração.
- **Recomendações para Usuários Finais:**
  - Alterar senhas caso a organização informe possível comprometimento.

- Utilizar autenticação multifator em serviços corporativos.
- Reportar acessos não reconhecidos.

Para saber informações mais detalhadas sobre esta vulnerabilidade acesse: https://www.techradar.com/pro/security/critical-citrix-netscaler-flaw-gets-official-patch-warning-from-cisa.

2.4. Drupal Core – SQL Injection Crítica (CVE-2026-9082)

A CVE-2026-9082 é uma vulnerabilidade crítica de SQL Injection identificada no núcleo do Drupal. A falha afeta principalmente ambientes que utilizam PostgreSQL como banco de dados e permite que consultas SQL sejam manipuladas por usuários não autenticados, comprometendo a integridade e a confidencialidade das informações armazenadas.

Exploração

A exploração ocorre por meio do envio de requisições especialmente elaboradas que exploram falhas no tratamento de parâmetros utilizados em consultas ao banco de dados. Um invasor pode executar comandos SQL arbitrários, acessar informações sensíveis, modificar registros, criar contas privilegiadas ou até preparar o ambiente para ataques mais avançados. Em determinados cenários, a falha pode servir como porta de entrada para comprometimento completo da aplicação.

Mitigação e Prevenção

- **Recomendações imediatas:**
  - Atualizar imediatamente o Drupal para as versões corrigidas.
  - Identificar instâncias vulneráveis expostas à internet.
  - Revisar contas administrativas recentemente criadas.
- **Recomendações para administradores de sistema:**
  - Implementar regras de proteção em WAF.
  - Monitorar logs de aplicação e banco de dados.
  - Revisar permissões de acesso ao banco PostgreSQL.
  - Executar varreduras de vulnerabilidades após a aplicação das correções.
- **Recomendações para administradores de sistema:**
  - Utilizar senhas fortes para contas administrativas.
  - Habilitar autenticação multifator quando disponível.
  - Reportar comportamentos anormais observados na aplicação.

Para saber informações mais detalhadas sobre esta vulnerabilidade acesse: https://www.akamai.com/blog/security-research/cve-2026-9082-mitigating-critical-sql-injection-drupal.

2.5 Trend Micro Apex One: Vulnerabilidade crítica em exploração ativa permite comprometer endpoints

A falha CVE-2026-34926 no Trend Micro Apex One (implementações on-premise) é uma vulnerabilidade de traversal de diretório que já está sendo explorada ativamente, segundo a CISA. A exploração permite que um atacante local pré-autenticado manipule caminhos de arquivos e modifique uma tabela-chave do banco de dados, possibilitando injeção de código que pode ser distribuída a todos os agentes conectados representando risco de comprometimento em larga escala da infraestrutura de endpoint.

Exploração

A vulnerabilidade é do tipo Directory Traversal (CWE-23) e afeta implantações locais do Trend Micro Apex One. A falha permite que um usuário autenticado manipule caminhos de arquivos para acessar diretórios que normalmente deveriam estar restritos.

A exploração possibilita modificar uma tabela crítica no banco de dados do servidor Apex One. A partir dessa alteração, um atacante pode inserir código ou payloads maliciosos que serão distribuídos aos agentes de endpoint gerenciados pela plataforma.

Os principais alvos são o servidor central de gerenciamento e todos os agentes conectados ao ambiente. Como o Apex One possui amplo alcance sobre os endpoints corporativos, a exploração pode se propagar rapidamente pela infraestrutura.

O impacto potencial inclui modificação não autorizada de componentes do servidor, injeção de payloads maliciosos em agentes, comprometimento ou evasão de soluções EDR, movimentação lateral na rede e comprometimento em larga escala dos dispositivos gerenciados.

A vulnerabilidade foi adicionada ao catálogo KEV da **Cybersecurity and Infrastructure Security Agency**, que confirmou exploração ativa em ambiente real. Embora ainda não haja associação pública com campanhas de ransomware, o risco permanece elevado para organizações que não aplicaram as correções recomendadas.

Mitigação e Prevenção

- **Recomendações imediatas:**
  - Aplicar os patches/atualizações fornecidos pela Trend Micro sem demora.
  - Seguir as orientações oficiais de mitigação da Trend Micro.
  - Se não for possível aplicar o patch imediatamente, considerar desativar ou isolar temporariamente o servidor Apex One até a correção.
  - Restringir e controlar o acesso local ao servidor Apex One (reduzir contas com acesso físico/SSH/console).
  - Implementar controles de acesso por privilégio mínimo para contas e serviços do servidor.
  - Isolar o servidor de gerenciamento em uma VLAN/segmento separado e limitar conectividade às redes e portas estritamente necessárias.
  - Habilitar e revisar logs detalhados no servidor Apex One e no banco de dados; configurar alertas para alterações incomuns em tabelas críticas.

- Ativar File Integrity Monitoring (FIM) e verificar assinaturas/checksums de arquivos binários do servidor e agentes.
- Auditar e validar a integridade do banco de dados do Apex One e dos repositórios de atualização de agentes.
- Rotacionar credenciais/segredos associados ao servidor e aos agentes, se houver suspeita de comprometimento.
- Fortalecer monitoramento SIEM: buscar padrões como atualizações de agentes fora de janela, alterações em tabelas do BD, processos desconhecidos no servidor de gerenciamento e comunicação de agentes para servidores não reconhecidos.

- **Recomendações por público:**
  - Administradores de sistemas / equipes de segurança: aplicar patch, isolar/segmentar servidores, revisar logs e integridade do BD, seguir BOD 22-01 para remediação rápida.
  - Monitorar logs de aplicação e banco de dados.
  - Usuários finais / estações de trabalho: garantir que agentes e endpoints apliquem atualizações e reportar qualquer comportamento estranho (rebootes, alertas do EDR, instalação de software não autorizado).
  - Equipes de resposta/IR: preparar playbook para investigação de alterações no banco de dados, coleta de evidências do servidor Apex One e contenção de agentes potencialmente comprometidos.

Para saber informações mais detalhadas sobre esta vulnerabilidade acesse: CISA Warns of Trend Micro Apex One Vulnerability Exploited in Attacks.

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