




Your IT Company

Principais Vulnerabilidades e Ameaças (março/26)

Sumário

1. Objetivo	2
2. Vulnerabilidades e Ameaças descobertas	2
2.1. Nova variante do VoidStealer contorna ABE do Chrome usando depuração — sem injeção nem privilégios elevados.....	2
2.2. Vulnerabilidades no Jenkins expõem servidores CI/CD — RCE via extração de .tar e WebSocket.....	4
2.3. CISA alerta: 0-day no Cisco Secure Firewall Management Center explorado em campanhas de ransomware	6
2.4. CISA alerta: vulnerabilidade crítica no Microsoft SharePoint já em exploração ativa	7
2.5. CISA alerta: Vulnerabilidade crítica em Zimbra (Classic UI) sendo explorada em ataques	9

	Inteligência de Ameaças Cibernéticas Comite Editorial	Código
		SGSI-081
		Página
		2 de 10

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. Nova variante do VoidStealer contorna ABE do Chrome usando depuração sem injeção em privilégios elevados

Uma nova variante do infostealer VoidStealer (v2.0, 13/03/2026) tornou-se o primeiro malware conhecido a contornar a Application-Bound Encryption (ABE) do Google Chrome sem injetar código nem exigir privilégios SYSTEM, extraindo credenciais criptografadas diretamente da memória via técnicas de depurador.

A técnica reduz significativamente a superfície de detecção tradicional, tornando o roubo de senhas e cookies mais furtivo e elevando o risco imediato para contas e sessões autenticadas.

Exploração

O Application-Bound Encryption (ABE) é um mecanismo introduzido pelo Google em julho de 2024 para proteger credenciais e cookies no Google Chrome. Ele vincula a chave de criptografia (v20_master_key) a um serviço executado em nível SYSTEM (Google Chrome Elevation Service), dificultando o acesso direto por malware.


A variante VoidStealer v2.0 contorna essa proteção usando uma abordagem baseada em depuração, inspirada no projeto ElevationKatz. Em vez de tentar extrair a chave diretamente ou elevar privilégios, o malware captura o momento em que a v20_master_key aparece em texto claro na memória do processo do navegador, sem modificar sua memória.

O fluxo técnico envolve a criação de um processo de navegador em modo suspenso (CreateProcessW com SW_HIDE e CREATE_SUSPENDED), seguido da anexação como depurador (DebugActiveProcess). O malware monitora eventos com WaitForDebugEvent e, ao identificar o carregamento de chrome.dll ou msedge.dll, analisa a seção .rdata em busca de referências como OSCrypt.AppBoundProvider.Decrypt.ResultCode para localizar o ponto onde a chave é manipulada.

A partir disso, define *breakpoints* de hardware diretamente nos registradores (DR0/DR7) via SetThreadContext, evitando alterações na memória do processo. Quando o breakpoint é acionado, o ponteiro para a chave aparece em registradores como R15 (Chrome) ou R14 (Edge), sendo então extraído com chamadas ReadProcessMemory.

Os principais alvos são Google Chrome e Microsoft Edge. O impacto inclui roubo de senhas salvas e cookies de sessão, permitindo sequestro de contas, acesso não autorizado e potencial movimentação lateral em ambientes corporativos.


Como agravante, o VoidStealer é distribuído no modelo Malware-as-a-Service (MaaS) em fóruns da dark web desde dezembro de 2025, com evolução rápida. Isso aumenta a probabilidade de outras famílias de malware adotarem técnicas semelhantes para contornar proteções modernas de navegadores.

	Inteligência de Ameaças Cibernéticas Comite Editorial	Código
		SGSI-081
		Página
		3 de 10

Mitigação e Prevenção

- **Para administradores de segurança / equipes de TI:**
 - Bloquear ou monitorar binários maliciosos conhecidos, aplicar bloqueio por hash em EDR/AV:
f783fde5cf7930e4b3054393efadd3675b505cbef8e9d7ae58aa35b435adeea4.
 - **Criar detecções/alertas no EDR para comportamentos suspeitos relacionados a depuração:** chamadas DebugActiveProcess direcionadas a processos de navegador (chrome.exe, msedge.exe), SetThreadContext escrevendo em registradores de breakpoint (DR0/DR7), ReadProcessMemory lendo espaço de memória de processos de navegador por processos não autorizados.
 - Detectar e alertar sobre navegadores iniciados com SW_HIDE, CREATE_SUSPENDED ou em modo headless por processos não autorizados (padrões de criação de processo anômalos).
 - Reforçar policies de aplicação de privilégio mínimo, restringir contas que possam criar processos ou usar APIs de depuração; auditar e limitar contas administrativas.
 - Implementar e ajustar regras de proteção baseada em comportamento (behavioral) no EDR para detectar anomalias de depuração e leitura de memória inter-processo.
 - Manter navegadores e SO atualizados; revisar configurações de hardening e integridade do serviço Google Chrome Elevation Service.
 - Revisar e restringir o uso de ferramentas de depuração legítimas em endpoints corporativos e controlar quem pode depurar processos de navegador.
- **Para usuários finais e equipes de identidade:**
 - Habilitar autenticação multifator (MFA) em todas as contas que suportam, reduz o impacto do roubo de credenciais.
 - Evitar salvar senhas no navegador; preferir gerenciadores de senha dedicados e com proteção adicional (p. ex. vaults locais/segurança por hardware).
 - Rotacionar senhas e revogar sessões ativas se houver suspeita de comprometimento; forçar logout de dispositivos/sessões quando possível.
 - Educar usuários sobre sinalizações de comportamentos suspeitos e exigir reporte imediato de notificações de acesso ou e-mails de recuperação de conta.

Para saber informações mais detalhadas sobre esta vulnerabilidade acesse: <https://cybersecuritynews.com/new-voidstealer-variant-bypasses-chrome-abe/>.

	Inteligência de Ameaças Cibernéticas Comite Editorial	Código
		SGSI-081
		Página
		4 de 10

2.2. Vulnerabilidades no Jenkins expõem servidores CI/CD — RCE via extração de .tar e WebSocket

Um alerta crítico publicado em 18 de março de 2026 descreve várias vulnerabilidades de alta severidade no núcleo do Jenkins e no plugin LoadNinja que podem permitir execução remota de código (RCE) e exposição de chaves de API.

As falhas mais críticas incluem exploração via extração de arquivos .tar/.tar.gz com links simbólicos e um problema de DNS rebinding que permite sequestro de sessões WebSocket CLI, com impacto imediato em pipelines CI/CD se não forem mitigadas.

Exploração

O Jenkins apresenta múltiplas vulnerabilidades críticas que afetam diretamente o controlador e seus componentes.

A CVE-2026-33001 está relacionada ao tratamento incorreto de links simbólicos durante a extração de arquivos .tar e .tar.gz no controlador. Um atacante com permissão de configuração de item pode enviar um artefato malicioso que, ao ser extraído, grava arquivos em caminhos arbitrários do sistema. Isso permite, por exemplo, inserir scripts em `$JENKINS_HOME/init.groovy.d/` ou implantar plugins maliciosos em `$JENKINS_HOME/plugins/`, resultando em execução remota de código e comprometimento total do controlador. Funcionalidades como “Archive the artifacts” e etapas de pipeline que manipulam artefatos dependem diretamente desse processo vulnerável.


A CVE-2026-33002 envolve uma falha de DNS rebinding na validação de origem do WebSocket CLI. O Jenkins calcula origens confiáveis com base em cabeçalhos HTTP, mas um atacante pode enganar a vítima para acessar um site malicioso que resolve para o IP do controlador. Isso permite estabelecer uma conexão WebSocket não autorizada com o endpoint CLI. Em cenários onde o acesso anônimo está habilitado e o serviço roda sem TLS, é possível executar comandos CLI com privilégios do usuário anônimo, o que pode evoluir para execução de scripts Groovy e RCE.

Já o plugin LoadNinja, afetado pelas CVE-2026-33003 e CVE-2026-33004, apresenta falhas no armazenamento e exposição de credenciais. As chaves de API são salvas em texto claro nos arquivos de configuração dos jobs e não são mascaradas na interface, permitindo que usuários com permissões de leitura ampliadas ou acesso ao sistema de arquivos obtenham essas informações sensíveis.

O impacto combinado dessas falhas inclui execução remota de código, comprometimento total do controlador Jenkins, exposição de credenciais e manipulação de pipelines, o que pode afetar diretamente a cadeia de desenvolvimento e entrega de software.


Mitigação e Prevenção

- **Recomendação imediata:**
 - Atualize o Jenkins para 2.555 (weekly) ou 2.541.3 (LTS) o mais rápido possível.
 - Atualize o LoadNinja Plugin para a versão v2.2.
- **Controles de configuração e mitigadores temporários:**
 - Remova completamente permissões para o usuário anônimo no controlador Jenkins.
 - Exija autenticação estrita para acesso ao controlador (disable anonymous access).
 - Habilite TLS/HTTPS para o Jenkins (não operar em HTTP puro).

	Inteligência de Ameaças Cibernéticas Comite Editorial	Código
		SGSI-081
		Página
		5 de 10

- Desabilite ou restrinja endpoints CLI/WebSocket se não forem necessários; considere bloquear o CLI remoto.
- Restringir quem pode executar ações de configuração de itens e quem pode carregar artefatos; aplique princípio do menor privilégio.
- Se possível, desative temporariamente ações/post-build que extraiam arquivos (ex.: “Archive the artifacts”) para jobs sensíveis ou aplique validação de conteúdo antes da extração.
- **Deteção, resposta e remediação pós-comprometimento:**
 - Verifique `$JENKINS_HOME/init.groovy.d/` por scripts não autorizados e `$JENKINS_HOME/plugins/` por plugins recém-adicionados ou assinaturas ausentes.
 - Procure alterações recentes em arquivos de configuração de jobs (config.xml) contendo credenciais não criptografadas; remova e rode procedimentos de rotação de chaves/APIs comprometidas.
 - Faça auditoria de permissões e logs de acesso, e revise tokens/credenciais usados por jobs e integrações.
 - Considere isolar o controlador Jenkins (só acesso a partir de rede de gestão) e usar agentes em máquinas separadas com permissões limitadas.
 - Implemente monitoramento e alertas para mudanças em diretórios sensíveis do Jenkins e para a instalação/atualização de plugins.
- **Recomendações específicas por público:**
 - **Administradores de sistema:** aplicar patches imediatamente, revisar políticas de acesso (anônimos e item configuration), forçar TLS, auditar e rotacionar credenciais, e ativar deteção de alterações em `$JENKINS_HOME`.
 - **Equipes de DevOps / CI owners:** revisar jobs que usam extração de artefatos, evitar que pipelines executem extrações de artefatos não validados, e remover credenciais em texto claro dos arquivos de configuração.
 - **Usuários finais/Desenvolvedores:** evite visitar páginas não confiáveis enquanto autenticado no Jenkins, reporte comportamentos estranhos nos pipelines e não conceda permissões além do necessário para usuários e tokens.

Para saber informações mais detalhadas sobre esta vulnerabilidade acesse: <https://cybersecuritynews.com/jenkins-vulnerabilities-expose-ci-cd-servers/>.

	Inteligência de Ameaças Cibernéticas Comite Editorial	Código
		SGSI-081
		Página
		6 de 10

2.3. CISA alerta: 0-day no Cisco Secure Firewall Management Center explorado em campanhas de ransomware

Um zero-day crítico identificado como CVE-2026-20131 afeta o Cisco Secure Firewall Management Center (FMC) e o Cisco Security Cloud Control (SCC) Firewall Management, sendo já explorado ativamente em campanhas de ransomware. A falha permite execução remota de código com privilégios root via interface web de gerenciamento, e a CISA adicionou o caso ao seu Known Exploited Vulnerabilities Catalog, estabelecendo prazo de correção até 22 de março de 2026.

Exploração

A vulnerabilidade é do tipo deserialização de dados não confiáveis (CWE-502) na interface web de gerenciamento das soluções Cisco Firepower Management Center e Cisco Secure Cloud Control. Esse tipo de falha ocorre quando o sistema processa objetos serializados sem validação adequada.

O mecanismo de exploração envolve o envio, por um atacante remoto não autenticado, de um objeto Java serializado especialmente manipulado para a interface web. Ao desserializar esse objeto, o sistema vulnerável pode executar código arbitrário controlado pelo atacante.

O impacto é crítico, podendo resultar em execução de código com privilégios root, comprometimento total do sistema de gerenciamento de firewall, alteração de políticas de segurança, movimentação lateral em redes internas, exfiltração de dados e até implantação de ransomware, incluindo cenários de dupla extorsão.


Os principais alvos são organizações que utilizam Cisco FMC ou SCC, especialmente quando a interface de gerenciamento está exposta à Internet ou acessível a muitos administradores.

A relevância é imediata, pois já há exploração confirmada em campanhas de ransomware e inclusão no catálogo da Cybersecurity and Infrastructure Security Agency, tornando a aplicação de correções uma prioridade para evitar impactos operacionais e vazamento de dados.

Mitigação e Prevenção

- **Ações imediatas:**

- Aplicar imediatamente os patches e mitigação fornecidos pela Cisco conforme o advisory oficial.
- **Se não for possível patchar de imediato, restringir o acesso à interface web de gerenciamento:** bloquear acesso externo, aplicar listas de controle de acesso (ACL) e permitir apenas IPs administrativos confiáveis.
- Mover o acesso de gerenciamento para redes segregadas (VLAN de gerenciamento) e exigir acesso via VPN ou jump host com autenticação forte.
- Desativar temporariamente a interface web pública se não for estritamente necessária.
- Implementar autenticação multifator (MFA) para contas administrativas e revisar políticas de senha/rotação de credenciais.
- Habilitar e centralizar logs de auditoria (acesso, comandos e eventos Java), enviar para SIEM e configurar alertas para atividade anômala.

	Inteligência de Ameaças Cibernéticas Comite Editorial	Código
		SGSI-081
		Página
		7 de 10

- **Procurar e isolar sinais de comprometimento:** varredura de arquivos alterados, instâncias Java desconhecidas, processos com escalonamento de privilégio.
- Segmentar a rede e limitar privilégios para reduzir impacto de lateral movement; manter backups offline e testados para recuperação.
- Atualizar detecções em IDS/IPS/EDR com assinaturas ou regras indicadas pelo fornecedor e por fontes de threat intel.
- **Recomendações por público:**
 - **Administradores de sistema / redes:** aplicar patch/mitigação da Cisco imediatamente, revisar exposição da interface de gerenciamento, restringir acesso por IP/VPN, reforçar monitoramento e planos de resposta a incidentes.
 - **Equipes de segurança / SOC:** criar/ajustar regras de detecção para comportamento Java anômalo, monitorar logs de auditoria e tráfego para egressos suspeitos, preparar playbook de contenção e investigação.
 - **Usuários finais / Equipos de negócio:** garantir backups críticos off-line, reportar indisponibilidade/alertas incomuns, seguir instruções da TI para suspensão de serviços se solicitado.

Para saber informações mais detalhadas sobre esta vulnerabilidade acesse: <https://cybersecuritynews.com/cisco-firewall-0-day-exploited/>.

2.4. CISA alerta: vulnerabilidade crítica no Microsoft SharePoint já em exploração ativa


CISA adicionou a falha crítica do Microsoft SharePoint (CVE-2026-20963) ao catálogo Known Exploited Vulnerabilities, confirmando exploração ativa em ambientes reais. A vulnerabilidade permite execução remota de código via desserialização de dados não confiáveis, representando risco imediato a documentos e comunicações corporativas sensíveis.

Exploração

A vulnerabilidade está relacionada ao processo de desserialização no Microsoft SharePoint, onde dados recebidos podem ser convertidos em objetos executáveis na memória sem validação adequada. Isso permite que conteúdos maliciosos sejam interpretados como instruções válidas pela aplicação.

O vetor de ataque envolve um invasor remoto, sem necessidade de credenciais, que envia um pacote de dados especialmente forjado ao servidor SharePoint. Durante a desserialização, o sistema pode executar código embutido nesse conteúdo, resultando em execução remota de código.

No ambiente Linux, foi identificado o PeerTime, um backdoor que utiliza o protocolo BitTorrent para comunicação e execução de comandos remotos. Esse método permite que o tráfego malicioso se misture ao tráfego P2P legítimo, dificultando a detecção em redes que já utilizam esse tipo de protocolo. O binário também contém strings de depuração em chinês simplificado, fornecendo um possível indicativo linguístico sobre os operadores.

	Inteligência de Ameaças Cibernéticas Comite Editorial	Código
		SGSI-081
		Página
		8 de 10

Os principais alvos são ambientes corporativos que utilizam SharePoint para armazenamento de documentos e colaboração interna. O impacto inclui vazamento de dados sensíveis, implantação de backdoors, movimentação lateral na rede e possível uso do acesso inicial em campanhas mais amplas, como ransomware.

Há evidências concretas de exploração ativa, com inclusão da vulnerabilidade no catálogo KEV da Cybersecurity and Infrastructure Security Agency. Pesquisadores confirmaram ataques em andamento, embora não haja atribuição pública a grupos APT específicos. Esse tipo de falha é altamente valorizado por initial access brokers, o que aumenta o risco de uso em diferentes cadeias de ataque.


Mitigação e Prevenção

- **Ações imediatas:**

- Aplicar imediatamente as atualizações de segurança oficiais da Microsoft relacionadas ao CVE-2026-20963. Verifique o aviso de segurança da Microsoft e o Microsoft Update/WSUS/serviço de patch relevante.i
- **Seguir a diretiva da CISA/BOD 22-01:** para órgãos federais dos EUA, remediar ou mitigar todas as instâncias vulneráveis até 21 de março de 2026; adote cronograma agressivo similar no setor privado.
- **Reduzir exposição de rede:** restringir acesso ao SharePoint por meio de listas de controle de acesso (IP allowlists), VPNs ou soluções de acesso zero-trust; bloquear acesso público direto aos serviços SharePoint.
- **Implementar controles de perímetro:** configurar WAF/IPS com regras para bloquear payloads suspeitos e padrões de desserialização conhecidos; aplicar filtragem de entrada de dados.
- **Monitoramento e detecção:** ativar e afinar EDR/XDR, registrar eventos de aplicação e sistema, monitorar processos e conexões de rede suspeitas, revisar logs de IIS/SharePoint para requisições anômalas.
- **Resposta e contenção:** ter planos de resposta a incidentes prontos para isolar hosts comprometidos, coletar evidências e restaurar sistemas a partir de backups verificados.

- **Recomendações para diferentes públicos:**

- **Administradores de sistema:** priorizar inventário de instâncias SharePoint expostas, aplicar patches, revisar configurações de rede e privilégios, habilitar detecção contínua e criar regras de bloqueio no WAF.
- **Equipes de segurança/IR:** criar buscas por comportamento pós-exploração (novos serviços, scheduled tasks incomuns, conexões externas persistentes), preparar playbooks de contenção e remoção.

	Inteligência de Ameaças Cibernéticas Comite Editorial	Código
		SGSI-081
		Página
		9 de 10

- **Usuários finais / gestores:** garantir backups recentes e testados dos dados críticos, reportar qualquer comportamento inesperado do serviço, restringir compartilhamento público de sites/documentos até mitigação completa.

Para saber informações mais detalhadas sobre esta vulnerabilidade acesse: <https://cybersecuritynews.com/microsoft-sharepoint-vulnerability-exploited/>.

2.5. CISA alerta: Vulnerabilidade crítica em Zimbra (Classic UI) sendo explorada em ataques

O Zimbra Collaboration Suite (ZCS) sofreu uma falha de stored XSS (CVE-2025-66376) na Classic User Interface que já está sendo explorada ativamente. A exploração é feita por e-mails maliciosos que incluem CSS/@import embutido, permitindo execução de código no contexto da sessão do usuário — risco imediato de roubo de cookies, acesso a e-mails e ações não autorizadas.

Exploração

A vulnerabilidade é do tipo Stored Cross-Site Scripting na Classic UI do Zimbra, permitindo que código malicioso seja armazenado e executado no contexto da aplicação quando o conteúdo é acessado. O vetor de ataque envolve o envio de e-mails contendo HTML com diretivas CSS @import e código embutido. Quando a mensagem é aberta na Classic UI, esse conteúdo é processado pelo cliente web, ativando o payload malicioso.

Os principais alvos são usuários que ainda utilizam a Classic UI do Zimbra, especialmente em ambientes corporativos que não aplicaram as atualizações de segurança. Administradores também são alvos críticos devido ao nível de acesso que possuem.


O impacto potencial inclui comprometimento de contas, exfiltração de dados sensíveis e uso do acesso para fraudes ou movimentação lateral na rede. Como o vetor é baseado em e-mail, a escalabilidade do ataque é elevada.

A falha foi adicionada ao catálogo KEV da Cybersecurity and Infrastructure Security Agency, com prazo de correção até 01/04/2026 para agências federais. Correções foram disponibilizadas nas versões 10.1.13 e 10.0.18, incluindo atualização da biblioteca AntiSamy para 1.7.8. A versão 10.0 entrou em fim de vida em 31/12/2025, aumentando o risco para ambientes que permanecem desatualizados.

Mitigação e Prevenção

- **Recomendações imediatas:**

- **Aplicar patches oficiais:** atualizar zimbra para 10.1.13 (ou 10.0.18 se não puder migrar imediatamente), o patch corrige o stored XSS.
- **Migrar de versões EOL:** planejar e executar migração de 10.0 para 10.1 o quanto antes; versões EOL não recebem correções.
- **Se não puder aplicar o patch:** descontinuar o uso da Classic UI ou bloquear o acesso a ela até a correção ser aplicada.

	Inteligência de Ameaças Cibernéticas Comite Editorial	Código
		SGSI-081
		Página
		10 de 10

- **Recomendações para públicos específicos:**

- **Administradores de sistema:** aplicar patches, migrar fora de EOL, configurar gateways para sanitização de HTML, criar regras de detecção e revogar sessões quando necessário.
- **Equipe de segurança/IR:** habilitar monitoramento de anomalias, buscar indicadores de comprometimento (veja seção IOCs), preparar playbook de resposta para contaminação por XSS.
- **Usuários finais:** evitar abrir e-mails suspeitos, não clicar em links ou baixar conteúdo desconhecido, reportar mensagens estranhas ao time de segurança, usar Modern UI quando disponível e ativar MFA.

Para saber informações mais detalhadas sobre esta vulnerabilidade acesse: <https://cybersecuritynews.com/zimbra-vulnerability-exploited-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