



Your IT Company

Principais Vulnerabilidades e Ameaças (outubro/26)

Sumário

1. Objetivo	2
2. Vulnerabilidades e Ameaças descobertas	2
2.1. Atacantes usam golpes de suporte de TI do Microsoft Teams para implantar malware e ransomware ..	2
2.2. Hackers infectam 953 lojas online com JavaScript malicioso que escapa dos scanners de segurança ..	4
2.3. Vulnerabilidade crítica na Cisco Expressway possibilita ataques de execução remota de código	7
2.4. HTTP2Shell: Vulnerabilidade crítica expande superfície de ataque e afeta múltiplas tecnologias além do HTTP/2.....	8
2.5. Falha no Microsoft Authenticator permite que aplicativos Android maliciosos roubem tokens de conta sem nenhuma permissão.....	10
2.6. Hackers atacam falha crítica do Suíte E-Business da Oracle no RCE dias após atualização de segurança.	12
2.7. Falha crítica de backup e replicação de Veeam permite que atacantes não autenticados burlem a autorização.	13
2.8. Falha crítica do Oracle Java com CVSS 9.1 permite ataques remotos não autenticados.	15

	Inteligência de Ameaças Cibernéticas Comite Editorial	Código
		SGSI-081
		Página
		2 de 16

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. Atacantes usam golpes de suporte de TI do Microsoft Teams para implantar malware e ransomware

Pesquisadores identificaram uma campanha de engenharia social que utiliza o Microsoft Teams para se passar por equipes internas de suporte técnico. Os criminosos criam ou utilizam contas de locatários Microsoft 365 com nomes que aparentam pertencer ao departamento de TI, explorando a confiança dos funcionários em comunicações corporativas. A campanha combina mensagens externas no Teams, possíveis ataques de mail bombing, envio massivo de mensagens para sobrecarregar a caixa de entrada, e técnicas de persuasão para convencer as vítimas a aceitar assistência remota. A atividade foi associada a incidentes envolvendo a implantação de ransomware Chaos.

Exploração

O ataque ocorre principalmente por meio das seguintes etapas:

- O criminoso utiliza uma conta externa com nome semelhante a “IT Support” ou “Help Desk”.
- A vítima recebe mensagens que simulam um atendimento legítimo, frequentemente após uma enxurrada de e-mails.
- O atacante convence o funcionário a iniciar uma sessão de assistência remota, utilizando ferramentas legítimas como Quick Assist, AnyDesk, TeamViewer ou ScreenConnect.
- Com acesso interativo, o invasor pode executar comandos, coletar informações, instalar ferramentas adicionais e movimentar-se pela rede.
- Em determinadas ocorrências, a cadeia de ataque evolui para implantação de backdoors, exfiltração de dados e ransomware.

Impactos potenciais

- Comprometimento de estações de trabalho e contas corporativas.
- Roubo de credenciais e informações confidenciais.
- Movimentação lateral para servidores e controladores de domínio.

	Inteligência de Ameaças Cibernéticas Comite Editorial	Código
		SGSI-081
		Página
		3 de 16

- Instalação de backdoors e ferramentas de acesso remoto persistente.
- Exfiltração de dados e possível implantação de ransomware.
- Interrupção de operações e custos de recuperação do ambiente.

Mitigação e Prevenção

- **Recomendações imediatas:**

- Alertar os colaboradores sobre contatos externos que se apresentam como suporte técnico.
- Bloquear ou restringir sessões externas no Teams quando não forem necessárias.
- Investigar sessões recentes de Quick Assist e de outras ferramentas de acesso remoto fora do padrão.
- Revisar alertas de execução de PowerShell, downloads de instaladores MSI e conexões com domínios desconhecidos.
- Isolar endpoints com evidências de execução de payloads e acionar o processo de resposta a incidentes.

- **Recomendações para Administradores de Sistema:**

- Aplicar políticas de acesso externo e de comunicação federada no Teams, com permissões mínimas necessárias.
- Exigir aprovação por canais internos autenticados para qualquer solicitação de suporte remoto.
- Implementar EDR com monitoramento de PowerShell, criação de processos, persistência e ferramentas RMM.
- Correlacionar logs do Microsoft 365, Teams, Entra ID, endpoints e firewall.
- Restringir o uso de ferramentas de acesso remoto a soluções corporativas aprovadas.
- Monitorar tentativas de descoberta do Active Directory e conexões incomuns entre estações e servidores.

- **Recomendações para usuários finais:**

- Confirmar solicitações de suporte por um canal corporativo conhecido.
- Não executar comandos recebidos por chat sem validação da equipe de TI.
- Não instalar ferramentas de acesso remoto a pedido de contatos não verificados.
- Comunicar imediatamente episódios de mail bombing acompanhados de mensagens de suposto suporte técnico.

	Inteligência de Ameaças Cibernéticas Comite Editorial	Código
		SGSI-081
		Página
		4 de 16

IoCs e artefatos

- Domínio de locatário
 - helpdeskteam365.onmicrosoft[.]com
 - itendpoint365.onmicrosoft[.]com
 - itcoreportal.onmicrosoft[.]com
 - itadmin922.onmicrosoft[.]com
 - corporateitservicellc.onmicrosoft[.]com
- Nomes de exibição
 - IT Support, Help Desk, HelpDesk Manager

Para saber informações mais detalhadas sobre esta vulnerabilidade acesse: [Atacantes usam golpes de suporte de TI do Microsoft Teams para implantar malware e ransomware](#)

2.2. Hackers infectam 953 lojas online com JavaScript malicioso que escapa dos scanners de segurança

Uma campanha criminososa comprometeu 953 lojas virtuais desde julho de 2025, atingindo principalmente instalações do Magento. O código malicioso é inserido no conteúdo das páginas da loja e utiliza mecanismos para evitar a detecção por scanners automatizados. A campanha permanece ativa segundo a publicação de outubro de 2026. O grupo alterna domínios utilizados para carregar o JavaScript malicioso, dificultando a identificação baseada exclusivamente em listas de bloqueio.

Exploração

O comprometimento pode ocorrer por meio de falhas em aplicações, mecanismos de upload de arquivos inseguros ou acesso indevido ao servidor e ao banco de dados. O código identificado foi armazenado na tabela cms_block do Magento, utilizada para conteúdo de blocos estáticos. A campanha emprega técnicas de fingerprinting para distinguir visitantes reais de ferramentas automatizadas de análise.

Entre os comportamentos descritos estão:

- Verificação de propriedades do navegador para identificar automação.
- Coleta de informações como resolução de tela, fuso horário e características da GPU.
- Carregamento seletivo de scripts maliciosos.
- Armazenamento de valores no localStorage, permitindo reutilizar dados de execução em visitas posteriores.
- Uso de domínios externos e redirecionamentos para entregar componentes adicionais.

	Inteligência de Ameaças Cibernéticas Comite Editorial	Código
		SGSI-081
		Página
		5 de 16

Impacto

- Roubo de dados de clientes e informações inseridas durante o checkout.
- Comprometimento da integridade das páginas da loja virtual.
- Possível captura de informações de pagamento, dependendo do código injetado.
- Redirecionamento de compradores para páginas fraudulentas.
- Perda de confiança dos consumidores e danos reputacionais.
- Exposição a fraudes financeiras, investigações e obrigações de notificação.

Mitigação e Prevenção

- **Recomendações imediatas:**
 - Inspecionar as tabelas cms_block e cms_page em busca de código JavaScript desconhecido.
 - Verificar referências a fpCode, se_referrer e localStorage.getItem em conteúdo do CMS.
 - Investigar contas administrativas desconhecidas, processos suspeitos e arquivos inesperados em diretórios de upload.
 - Revisar os logs do servidor web, do banco de dados e das operações administrativas.
 - Se houver evidências de comprometimento ativo, retirar a loja de exposição ou aplicar controles temporários, preservando os registros necessários à investigação.
 - Acionar o provedor de pagamento e a equipe de resposta a incidentes quando houver suspeita de captura de dados financeiros.
- **Recomendações para Administradores de Sistema:**
 - Atualizar Magento, extensões, temas e componentes de terceiros para versões corrigidas.
 - Verificar a aplicabilidade das correções oficiais relacionadas a PolyShell e SessionReaper.
 - Restringir permissões de escrita no banco de dados e nos diretórios da aplicação.
 - Exigir MFA para contas administrativas e eliminar contas obsoletas.
 - Implementar monitoramento de integridade de arquivos, análise de alterações no CMS e WAF.
 - Investigar o vetor de entrada e rotacionar credenciais administrativas, de banco de dados e de APIs após a contenção.
 - Realizar uma nova avaliação de segurança após a limpeza; um scanner sem alertas não comprova que a loja esteja íntegra.

	Inteligência de Ameaças Cibernéticas Comite Editorial	Código
		SGSI-081
		Página
		6 de 16

- **Recomendações para usuários finais:**

- Evitar salvar dados de pagamento em lojas com sinais de comprometimento.
- Monitorar transações financeiras e comunicar movimentações suspeitas à instituição responsável.
- Utilizar meios de pagamento que ofereçam mecanismos de contestação e proteção contra fraude.
- Caso exista suspeita de exposição, seguir as orientações da loja e do banco para proteger os dados afetados.

IoCs e artefatos

- Loader
 - deepveindrilling[.]com/?s=d35c5031
 - deepveindrilling[.]com/?s=49b7ca5f&fp=
- URL de redirecionamento
 - additionalver[.]com/Mb2z8J
 - lanhd6549tdhse[.]top/KZtBscgb
 - neswnsssn[.]click/PKgJDPfF
 - manulfie[.]click/GKTD8cBz
 - hdfdsi84j3h[.]top/sFnnPFHm
 - c85grt98sd[.]com/1kYrdH
- Payload
 - crypto-insider[.]top/ssl/
 - leqdger[.]click/ssl/
- Chaves/strings
 - fpCode, 136c1e07507f4a97, 136c1e07507f4a98
- Local de persistência
 - cms_block.content no banco de dados Magento
- Diretório a investigar
 - pub/media/custom_options/

Para saber informações mais detalhadas sobre esta vulnerabilidade acesse: [Hackers infectam 953 lojas online com JavaScript malicioso que escapa dos scanners de segurança](#)

	Inteligência de Ameaças Cibernéticas Comite Editorial	Código
		SGSI-081
		Página
		7 de 16

2.3. Vulnerabilidade crítica na Cisco Expressway possibilita ataques de execução remota de código

A Cisco publicou correções para a CVE-2026-76466, vulnerabilidade crítica que afeta o Cisco Expressway-C e o Expressway-E quando configurados em cluster e executando versões vulneráveis. A falha está relacionada ao serviço de banco de dados, ao tratamento de cookies persistentes e à validação inadequada de certificados de cliente em determinadas configurações de TLS Verify Mode. A exploração bem-sucedida pode permitir a execução de comandos no sistema operacional com privilégios de root

Exploração

Segundo as informações divulgadas, um atacante com acesso de rede ao dispositivo afetado e que possua os cookies necessários pode interagir com o serviço de banco de dados e invocar determinadas chamadas de procedimento remoto. A falha de validação de certificados reduz a efetividade dos controles de confiança esperados em configurações específicas do cluster. A publicação não esclarece como os cookies necessários seriam obtidos; portanto, não é correto afirmar que qualquer dispositivo acessível pela internet possa ser explorado automaticamente.

Impacto

- Execução de comandos com privilégios máximos no dispositivo.
- Possível comprometimento da integridade e da disponibilidade dos serviços de comunicação.
- Alteração de configurações e exposição de informações armazenadas no equipamento.
- Possibilidade de utilização do dispositivo como ponto de apoio para outras atividades maliciosas.
- Interrupção de serviços corporativos que dependem da infraestrutura de comunicação.

Mitigação e Prevenção

- **Recomendações imediatas:**
 - Identificar todas as instâncias Cisco Expressway-C e Expressway-E, incluindo appliances físicos e máquinas virtuais.
 - Verificar a configuração de cluster e a versão instalada.
 - Atualizar para a versão corrigida recomendada pela Cisco, respeitando os requisitos de compatibilidade.
 - Restringir temporariamente o acesso de rede ao serviço de administração e aos componentes internos relevantes.

	Inteligência de Ameaças Cibernéticas Comite Editorial	Código
		SGSI-081
		Página
		8 de 16

- Revisar logs e configurações em busca de conexões inesperadas, alterações administrativas e eventos fora do padrão.
- **Recomendações para Administradores de Sistema:**
 - Priorizar a atualização para o Expressway X15.5.20 ou uma versão posterior aprovada pela Cisco.
 - Planejar a migração de versões X14 ou anteriores para uma versão corrigida suportada.
 - Aplicar as recomendações adicionais do comunicado de reforço de segurança da Cisco de outubro de 2026.
 - Segmentar a rede e permitir acesso aos serviços de gerenciamento somente a partir de redes administrativas confiáveis.
 - Validar a configuração de certificados TLS e a comunicação entre os nós do cluster.
 - Após a atualização, testar a operação do cluster e revisar as evidências de acesso ao serviço vulnerável.

Para saber informações mais detalhadas sobre esta vulnerabilidade acesse [Vulnerabilidade crítica na Cisco Expressway Possibilita Ataques de Execução Remota de Código](#)

2.4. HTTP2Shell: Vulnerabilidade crítica expande superfície de ataque e afeta múltiplas tecnologias além do HTTP/2

A HTTP2Shell, também inicialmente referida como Node2Shell, é uma vulnerabilidade na biblioteca de descompressão Brotli, identificada como CVE-2026-111497. Apesar do nome, a falha não está restrita ao protocolo HTTP/2: ela pode afetar aplicações que utilizam a biblioteca para descomprimir dados.

A falha envolve um estado inválido do decodificador e uma escrita fora dos limites da memória prevista. Dependendo do software e do caminho de execução, o resultado pode ser uma falha do processo, corrupção de memória ou outros comportamentos inseguros. A pesquisa publicada identificou caminhos de impacto em Node.js, .NET, FFmpeg, ClickHouse e Apache Arrow.

Exploração

A exploração depende de uma aplicação vulnerável processar dados Brotli especialmente preparados. O fluxo de dados pode chegar ao decodificador por meio de respostas HTTP, requisições, arquivos ou APIs de processamento de conteúdo.

A pesquisa identificou diferentes cenários:

- Node.js: dados Brotli malformados podem atingir o decodificador vulnerável.
- NET: determinados caminhos de descompressão podem provocar corrupção de memória e encerramento do processo.

	Inteligência de Ameaças Cibernéticas Comite Editorial	Código
		SGSI-081
		Página
		9 de 16

- FFmpeg: metadados de uma imagem JPEG XL processados por libjxl podem atingir o caminho vulnerável; o estudo demonstrou corrupção de memória, mas não estabeleceu uma exploração completa para execução remota de código nesse caso.
- ClickHouse: uma requisição HTTP com conteúdo Brotli malformado provocou falha do servidor durante os testes.
- Apache Arrow: um fluxo de descompressão pode entrar em um ciclo que consome CPU continuamente.

Impacto

- Indisponibilidade de serviços por falha ou encerramento de processos.
- Consumo excessivo de CPU e degradação de desempenho.
- Corrupção de memória e potencial exposição de informações, dependendo do contexto.
- Possibilidade de execução de código em determinados cenários, conforme a aplicação afetada e a viabilidade da exploração.
- Interrupção de APIs, serviços de processamento de dados e pipelines de mídia.

Mitigação e Prevenção

- **Recomendações imediatas:**
 - Inventariar aplicações que utilizam Brotli, inclusive dependências transitivas e bibliotecas embarcadas.
 - Atualizar os componentes afetados para versões corrigidas fornecidas pelos respectivos fabricantes.
 - Priorizar serviços expostos que processem dados comprimidos não confiáveis.
 - Monitorar encerramentos inesperados, falhas de memória, consumo anormal de CPU e erros de descompressão.
 - Se não for possível atualizar imediatamente, restringir temporariamente a entrada de conteúdo não confiável nos caminhos vulneráveis, quando operacionalmente viável.
- **Recomendações para administradores de sistema:**
 - Validar os avisos de segurança de cada fornecedor, evitando avaliar a exposição somente pela versão nominal da Brotli.
 - Atualizar as linhas afetadas do Node.js para versões corrigidas; a publicação indica Node.js 22.23.4, 24.22.1 e 26.12.1.
 - Para PHP em Windows, aplicar os builds corrigidos indicados pela equipe PHP: 8.5.12-1, 8.4.27-1, 8.3.36-1 ou 8.2.35-1, conforme a linha utilizada.
 - Verificar as atualizações aplicáveis ao .NET, FFmpeg, ClickHouse e Apache Arrow.

	Inteligência de Ameaças Cibernéticas Comite Editorial	Código
		SGSI-081
		Página
		10 de 16

- Recompilar ou atualizar aplicações que incorporem bibliotecas vulneráveis, quando necessário.
- Utilizar testes de regressão e monitoramento de estabilidade após as atualizações.
- **Recomendações para usuários finais:**
 - Evitar abrir arquivos ou conteúdos suspeitos em aplicações desatualizadas.
 - Manter atualizados navegadores, clientes e ferramentas de processamento de arquivos.
 - Reportar falhas repetidas de aplicações que processem arquivos ou conteúdos recebidos de fontes externas.

Para saber informações mais detalhadas sobre esta vulnerabilidade acesse: [A vulnerabilidade do HTTP2Shell vai além do HTTP, afetando .NET, FFmpeg, ClickHouse e Apache Arrow](#)

2.5. Falha no Microsoft Authenticator permite que aplicativos Android maliciosos roubem tokens de conta sem nenhuma permissão

A Microsoft corrigiu a CVE-2026-80097, uma falha de autenticação no componente intermediário (broker) do Microsoft Authenticator para Android. A vulnerabilidade permitia que um aplicativo malicioso instalado no dispositivo tentasse se passar por um aplicativo Microsoft legítimo e obtivesse tokens associados a uma conta corporativa conectada. O problema foi classificado como elevação local de privilégios, com pontuação CVSS 8,6. O risco era especialmente relevante em dispositivos Android que possuíam o Authenticator instalado e uma conta corporativa autenticada.

Exploração

O problema estava relacionado à atividade Android exportada com.microsoft.identity.client.AccountChooserActivity, que processava solicitações de autenticação de outros aplicativos. A validação utilizava informações declaradas na própria solicitação, como identidade do pacote, identificador do cliente, URI de redirecionamento e UID do chamador. Um aplicativo malicioso podia manipular esses valores e alegar ser um aplicativo legítimo, como o Microsoft Teams. Como a validação não confirmava adequadamente a identidade real do aplicativo solicitante, o fluxo vulnerável poderia devolver tokens de autenticação sem exigir a aprovação do usuário para aquela solicitação específica.

Impacto

- Acesso indevido a recursos associados à conta corporativa.
- Possível exposição de e-mails, calendários, arquivos do OneDrive e conteúdos do SharePoint.

	Inteligência de Ameaças Cibernéticas Comite Editorial	Código
		SGSI-081
		Página
		11 de 16

- Acesso a recursos do Microsoft Teams e Microsoft Graph conforme as permissões do token.
- Uso indevido de sessões autenticadas, mesmo sem conhecer diretamente a senha da vítima.
- de exposição de informações empresariais e comprometimento de contas de trabalho.

Mitigação e Prevenção

- **Recomendações imediatas:**
 - Atualizar o Microsoft Authenticator para Android para a versão corrigida ou posterior. A publicação indica a versão 6.2606.4246 como corrigida.
 - Identificar dispositivos corporativos que utilizavam versões vulneráveis durante o período de exposição.
 - Investigar atividades incomuns de Microsoft Graph e acessos a recursos corporativos provenientes de dispositivos suspeitos.
 - a revogação de sessões e tokens de usuários potencialmente afetados, conforme o procedimento corporativo de resposta a incidentes.
 - houver indícios de comprometimento, revisar os registros de autenticação e os acessos aos dados corporativos.
- **Recomendações para Administradores de Sistema:**
 - Aplicar a atualização por meio de MDM/EMM ou dos mecanismos corporativos de gerenciamento de aplicativos.
 - Restringir a instalação de aplicativos por sideloading e utilizar listas de aplicativos permitidos quando adequado.
 - Exigir dispositivos em conformidade com as políticas de acesso condicional.
 - Monitorar acessos anormais a Microsoft Graph, alterações de sessão e uso de tokens em contextos inesperados.
 - Revisar as permissões delegadas concedidas aos aplicativos e a atividade das contas afetadas.
 - um processo de atualização rápida para componentes de autenticação e identidade.
- **Recomendações para Usuários Finais:**
 - Atualizar o Microsoft Authenticator pela loja oficial de aplicativos.
 - Evitar instalar APKs de fontes desconhecidas.
 - Reportar comportamentos inesperados de autenticação ou acesso a dados.

	Inteligência de Ameaças Cibernéticas Comite Editorial	Código
		SGSI-081
		Página
		12 de 16

- Seguir as instruções da equipe de TI caso seja necessário renovar sessões ou credenciais.

Para saber informações mais detalhadas sobre esta vulnerabilidade acesse: [Falha no Microsoft Authenticator Permite que Aplicativos Android Maliciosos Roubem Tokens de Conta sem Nenhuma Permissão.](#)

2.6. Hackers atacam falha crítica do Suíte E-Business da Oracle no RCE dias após atualização de segurança.

Em 28 de outubro de 2026, foi publicada uma notícia sobre tentativas de exploração de uma vulnerabilidade crítica no Oracle E-Business Suite (EBS), identificada como CVE-2026-101767. A falha está associada à autenticação inadequada no Oracle Application Object Library e recebeu pontuação CVSS 9,8. A vulnerabilidade havia sido corrigida pela Oracle no Critical Patch Update de outubro de 2026. Segundo a notícia, sensores de pesquisa da Defused Cyber registraram tentativas exploratórias em 27 de outubro, poucos dias após a disponibilização da correção.

Exploração

Uma solicitação especialmente construída pode explorar a injeção SQL sem autenticação, permitindo executar consultas no banco de dados com os privilégios do usuário APPS. Em uma cadeia bem-sucedida, o atacante pode alcançar a execução de comandos no sistema operacional com os privilégios da conta da aplicação EBS. A exploração depende de acesso de rede ao endpoint vulnerável. Sistemas expostos à internet apresentam maior risco, mas instâncias internas também podem estar vulneráveis se forem alcançáveis a partir de uma estação ou segmento de rede comprometido.

Impacto

- Acesso indevido a dados financeiros, de folha de pagamento, recursos humanos e compras.
- Alteração ou extração de registros corporativos acessíveis ao usuário APPS.
- Execução de comandos no host da aplicação.
- Comprometimento da integridade e confidencialidade do ambiente EBS.
- Possível movimentação lateral e utilização do servidor como ponto de apoio para ataques adicionais.

Mitigação e Prevenção

- **Recomendações imediatas:**

	Inteligência de Ameaças Cibernéticas Comite Editorial	Código
		SGSI-081
		Página
		13 de 16

- Aplicar o Critical Patch Update da Oracle de outubro de 2026, verificando a versão e os componentes instalados.
- Se a atualização não puder ser realizada imediatamente, remover /OA_HTML/AppsTCFServer da lista de URLs permitidas no firewall da aplicação, conforme orientação citada pela pesquisa.
- Restringir o acesso ao web tier do EBS a redes confiáveis.
- logs web, atividade do banco de dados e eventos do sistema operacional.
- Priorizar instâncias expostas à internet e realizar triagem de eventuais sinais de exploração anteriores à correção.
- **Recomendações para Administradores de Sistema:**
 - Validar o nível de patch de todas as instâncias Oracle EBS, inclusive ambientes de contingência e homologação.
 - Correlacionar requisições HTTP sem autenticação com consultas SQL e atividade de processos no host.
 - Investigar arquivos inesperados em \$APPLPTMP.
 - Monitorar a conta oracle e o Concurrent Manager em busca de processos de shell ou comandos fora do padrão.
 - Revisar os privilégios da conta APPS e limitar o acesso administrativo ao host.
 - Preservar evidências e considerar rotação de credenciais se houver suspeita de comprometimento.

Para saber informações mais detalhadas sobre esta vulnerabilidade acesse: [Hackers Atacam Falha Crítica do Suíte E-Business da Oracle no RCE Dias Após Atualização de Segurança](#)

2.7. Falha crítica de backup e replicação de Veeam permite que atacantes não autenticados burlem a autorização.

A Veeam publicou atualizações de segurança para corrigir a CVE-2026-108142, uma vulnerabilidade crítica de bypass de autorização no CDP Coordinator Service do Veeam Backup & Replication. A falha recebeu pontuação CVSS v4.0 de 9,1 e afeta implantações Windows e o Veeam Software Appliance. Diferentemente de vulnerabilidades que exigem uma conta autenticada, a falha descrita permite que um atacante não autenticado contorne controles de autorização. A publicação informa que versões 13.1.1.18 e anteriores da linha 13.1 e versões 13.0.2.29 e anteriores da linha 13.0 são afetadas. As versões 12.x não foram apontadas como vulneráveis a essa falha específica.

	Inteligência de Ameaças Cibernéticas Comite Editorial	Código
		SGSI-081
		Página
		14 de 16

Exploração

A falha está relacionada ao processamento de autorização no CDP Coordinator Service. A publicação não apresenta uma sequência técnica completa de exploração nem identifica um endpoint específico que permita reproduzir o ataque. Por isso, a análise deve se limitar ao que foi divulgado: um atacante não autenticado pode contornar a autorização do serviço vulnerável. Não há base suficiente nessa fonte para afirmar que a CVE, por si só, permita execução remota de código, exclusão de backups ou comprometimento total do servidor. A notícia também menciona duas vulnerabilidades de travessia de diretórios, CVE-2026-108140 e CVE-2026-108141, que possuem pré-requisitos diferentes e não devem ser confundidas com o bypass de autorização.

Impacto

- Acesso não autorizado a funcionalidades protegidas do serviço CDP.
- Possível exposição de operações e informações de infraestrutura de backup, conforme o alcance do bypass.
- Risco à integridade dos controles de proteção e recuperação de dados.
- Possível aumento do risco operacional caso a falha seja combinada com outras vulnerabilidades ou credenciais comprometidas.

Mitigação e Prevenção

- **Recomendações imediatas:**
 - Identificar a versão e a edição de cada instalação Veeam Backup & Replication.
 - Atualizar a linha 13.1 para a versão corrigida 13.1.2.57 ou posterior aplicável.
 - Atualizar a linha 13.0 para a versão corrigida 13.0.3.63 ou posterior aplicável.
 - Confirmar a aplicação das atualizações para as vulnerabilidades adicionais cobertas pelo mesmo comunicado.
 - Restringir temporariamente o acesso de rede aos serviços de backup, especialmente a partir de redes de usuários comuns.
 - Revisar logs de autenticação, autorização e atividade do CDP Coordinator Service.
- **Recomendações para Administradores de Sistema:**
 - Manter a infraestrutura de backup em segmentos de rede dedicados.
 - Limitar o acesso administrativo a estações privilegiadas e redes de gerenciamento.
 - Aplicar o princípio do menor privilégio e revisar as contas de serviço.
 - Proteger cópias de backup com mecanismos de imutabilidade e isolamento, quando suportados.

	Inteligência de Ameaças Cibernéticas Comite Editorial	Código
		SGSI-081
		Página
		15 de 16

- Monitorar alterações de configuração, tarefas de proteção, operações de recuperação e atividade administrativa atípica.
- Testar regularmente a recuperação de dados para validar a resiliência após atualizações.

Para saber informações mais detalhadas sobre esta vulnerabilidade acesse: [Falha crítica de backup e replicação de Veeam permite que atacantes não autenticados burlam a autorização.](#)

2.8. Falha crítica do Oracle Java com CVSS 9.1 permite ataques remotos não autenticados.

A Oracle publicou um alerta de segurança para a CVE-2026-91403, uma vulnerabilidade crítica relacionada ao Java Secure Socket Extension (JSSE), componente utilizado no processamento de conexões seguras e certificados digitais. O problema está associado à confiança em determinados certificados intermediários de autoridade certificadora vinculados à eMudhra. A vulnerabilidade recebeu pontuação CVSS de 9,1 e pode ser explorada remotamente sem autenticação em contextos aplicáveis. É importante destacar que o alerta trata de confiança em certificados, e não de uma vulnerabilidade de corrupção de memória. A publicação não afirma que todos os sistemas Java afetados sejam automaticamente vulneráveis à execução remota de código

Exploração

O risco surge quando uma aplicação utiliza APIs do JSSE em um contexto no qual dados fornecidos por um serviço ou origem remota são processados pelo componente vulnerável. A falha pode comprometer a avaliação de confiança relacionada aos certificados afetados. A orientação da Oracle inclui atualizar o Java ou implementar medidas alternativas para bloquear a confiança nos certificados intermediários impactados e reforçar a verificação de revogação.

Impacto

- Comprometimento da confidencialidade e da integridade em aplicações que utilizem o componente vulnerável em condições afetadas.
- Risco de confiança indevida em certificados intermediários comprometidos.
- Possibilidade de comprometer comunicações ou dados processados por aplicações dependentes do JSSE.
- Exposição de aplicações que executem código não confiável em ambientes Java Web Start ou applets que dependam do sandbox, conforme os cenários descritos pela Oracle.

	Inteligência de Ameaças Cibernéticas Comite Editorial	Código
		SGSI-081
		Página
		16 de 16

Mitigação e Prevenção

- **Recomendações imediatas:**

- Atualizar o Java SE e o GraalVM para versões corrigidas suportadas pela Oracle.
- Identificar aplicações Java que dependam do JSSE para comunicação com serviços remotos.
- Se a atualização imediata não for possível, seguir as instruções oficiais para bloquear os certificados intermediários afetados.
- Avaliar a ativação da verificação de revogação de certificados.
- Priorizar serviços expostos e aplicações que processam dados de origens não confiáveis.

- **Recomendações para Administradores de Sistema:**

- Inventariar versões de Java, JDKs incorporados, runtimes de aplicações e distribuições GraalVM.
- Substituir o arquivo de certificados bloqueados conforme a orientação oficial, preservando entradas personalizadas.
- Observar a diferença de nomenclatura: em Java 8, a publicação indica o uso de `blacklisted.certs`; nas demais situações, seguir a orientação específica da Oracle para `blocked.certs`.
- Para aplicações TLS, avaliar as propriedades indicadas pela Oracle:
- Validar os ajustes em ambiente de testes antes de aplicá-los amplamente, pois alterações de confiança e revogação podem afetar conexões legítimas.
- Atualizar runtimes fora de suporte para versões suportadas, quando viável.

- **Recomendações para Usuários Finais:**

- Manter atualizadas as aplicações Java instaladas e utilizar apenas versões distribuídas por canais confiáveis.
- Não ignorar avisos de certificados inválidos ou inesperados.
- Reportar erros de certificados em sistemas corporativos à equipe de TI, sem tentar contorná-los manualmente.

Para saber informações mais detalhadas sobre esta vulnerabilidade acesse: [Falha crítica do Oracle Java com CVSS 9.1 permite ataques remotos não autenticados](#).

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 semanalmente.