



Your IT Company

Principais Vulnerabilidades e Ameaças (setembro/26)

Sumário

1. Objetivo	2
2. Vulnerabilidades e Ameaças descobertas	2
2.1. CVE-2026-89775 - Vulnerabilidade no Linux KVM/ARM64 permite escape de máquina virtual e acesso ao host	2
2.2. GitLab - Exposição de Token de Incoming Email Pode Permitir Inserção de Código em Repositórios Privados	3
2.3. CVE-2026-94384 - AWS Lambda Permite Bypass de Permissões IAM	4
2.4. CVE-2026-94545 - Falha Crítica no Next.js Permite Execução Remota de Código por SVG Malicioso ..	5
2.5. Windows Defender - Zero-Day BigDiskBuster Pode Impedir Atualizações do Antivírus	7
2.6. CVE-2026-87902 — WordPress: Falha Crítica de RCE Explorada Ativamente	8

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

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-2026-89775 - Vulnerabilidade no Linux KVM/ARM64 permite escape de máquina virtual e acesso ao host

A CVE-2026-89775 é uma vulnerabilidade no KVM para arquiteturas ARM64 que pode permitir um ataque de guest-to-host escape quando a virtualização aninhada (nested virtualization) está habilitada. O problema está relacionado ao tratamento incorreto de níveis negativos durante a avaliação do tamanho de TLB no mecanismo VNCR. A vulnerabilidade foi introduzida no kernel Linux 6.16 e corrigida nas versões 6.18.51, 7.2.5 e 7.3-rc1.

Exploração

Em determinadas configurações, uma máquina virtual pode explorar a falha no KVM para obter acesso de leitura e escrita a uma página de memória pertencente ao kernel do host. Em ambientes ARM64 que disponibilizam nested virtualization, isso pode permitir que um atacante escape da VM e execute código com privilégios elevados no host.

O risco é particularmente relevante em ambientes multi-tenant, nos quais usuários não confiáveis possuem acesso a máquinas virtuais.

Impacto

- Escape da máquina virtual;
- Acesso à memória do host;
- Comprometimento do hypervisor;
- Comprometimento de outras VMs hospedadas no mesmo servidor;
- Escalada de privilégios para root em determinadas configurações.

Mitigação e Prevenção

- **Recomendações imediatas:**
 - Atualizar o kernel Linux para uma versão corrigida.
 - Priorizar hosts ARM64 que utilizam KVM.
 - Identificar hosts com nested virtualization habilitada.
 - Desabilitar nested virtualization quando ela não for necessária.
 - Priorizar ambientes multi-tenant ou que executem código não confiável.
- **Recomendações para Administradores de Sistema:**
 - Utilizar kernels corrigidos disponibilizados pela distribuição.

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

- Verificar se os patches foram incorporados ao kernel utilizado pelo fornecedor.
- Restringir o acesso a /dev/kvm somente a usuários e grupos autorizados.
- Evitar a disponibilização de virtualização para workloads não confiáveis.
- Monitorar processos privilegiados executados no host.
- Monitorar alterações inesperadas em módulos, processos e arquivos do sistema.
- Manter isolamento entre workloads de diferentes níveis de confiança.
- Não aplicar apenas o commit individual quando houver possibilidade de atualização completa; o próprio Linux CVE Team recomenda atualizar para uma versão estável suportada.

Para saber informações mais detalhadas sobre esta vulnerabilidade acesse: [Linux KVM/arm64 Vulnerability Lets Attackers Escape Virtual Machines and Gain Host Access](#).

2.2. GitLab - Exposição de Token de Incoming Email Pode Permitir Inserção de Código em Repositórios Privados

A funcionalidade “Email work item to this project” do GitLab utiliza um endereço de e-mail privado contendo um token glimt-. Esse endereço funciona como uma credencial: quem obtiver o token pode enviar mensagens que resultam na criação de issues e, em determinadas condições, merge requests em nome do proprietário do token.

O comportamento foi tratado pelo GitLab como uma característica da funcionalidade, e não como uma CVE convencional. Entretanto, a exposição do endereço pode representar um risco significativo para projetos privados e ambientes CI/CD.

Exploração

Um atacante que obtenha o endereço pode substituir o sufixo relacionado a issue por -merge-request e enviar um patch por e-mail. O GitLab pode aplicar esse patch utilizando as permissões do proprietário do token. Se o atacante modificar o .gitlab-ci.yml, o código inserido pode ser executado pelos pipelines CI/CD. Como o token é associado à conta, e não exclusivamente a um projeto, sua exposição pode afetar outros projetos aos quais o usuário possui acesso.

Impacto

- Alteração de código-fonte;
- Criação de merge requests;
- Modificação de branches;
- Alteração de .gitlab-ci.yml;
- Execução de código controlado pelo atacante em pipelines;
- Exposição de variáveis e secrets;
- Comprometimento de tokens de CI/CD;
- Alterações realizadas aparentemente pelo usuário legítimo.

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

Mitigação e Prevenção

- **Recomendações imediatas:**

- Procurar endereços contendo glimt- em documentação, tickets, repositórios e páginas públicas.
- Tratar o endereço como uma credencial, e não como um simples e-mail.
- Se houver suspeita de exposição, realizar o reset do incoming email token.
- Revisar commits e merge requests recentes dos usuários potencialmente afetados.
- Verificar alterações recentes no .gitlab-ci.yml.

- **Recomendações para Administradores de Sistema:**

- Revisar permissões dos usuários que possuem incoming email habilitado.
- Auditar branches protegidas.
- Exigir revisão/aprovação para alterações em pipelines.
- Monitorar criação inesperada de branches e merge requests.
- Auditar pipelines executados após uma possível exposição.
- Revisar CI/CD variables, job tokens e secrets.
- Monitorar eventos de auditoria do GitLab.
- Evitar publicar endereços de incoming email em documentação ou sistemas acessíveis externamente.
- Utilizar princípio do menor privilégio para usuários e projetos.

IOCs

- **O principal indicador é a exposição de endereços contendo:**

- glimt-
- .gitlab-ci.yml

Para saber informações mais detalhadas sobre esta vulnerabilidade acesse: [GitLab Email Feature Vulnerability Lets Attackers Push Code Into Private Repositories](#).

2.3. CVE-2026-94384 - AWS Lambda Permite Bypass de Permissões IAM

A CVE-2026-94384 é uma falha de autorização na função `sfExecuteAWSService` do `AmazonConnectSalesforceLambda`. A função recebe parâmetros fornecidos pelo solicitante e os encaminha para APIs privilegiadas da AWS sem validar adequadamente se o solicitante possui autorização para realizar aquela operação. A falha afeta versões 5.15 até 5.24.16.

Exploração

Uma principal IA que possua a permissão **lambda:InvokeFunction** sobre a função vulnerável pode utilizá-la para executar operações AWS que suas próprias permissões IAM não permitiriam.

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

Na prática, a Lambda pode atuar como um **proxy para uma IAM execution role privilegiada**, permitindo a um usuário de menor privilégio realizar operações com permissões superiores às suas.

Impacto

- Escalada de privilégios;
- Acesso a recursos AWS;
- Alteração ou exclusão de recursos;
- Acesso a dados armazenados em serviços AWS;
- Manipulação de configurações cloud;
- Comprometimento de outros recursos da conta.

Mitigação e Prevenção

- **Recomendações imediatas:**
 - Atualizar o **AmazonConnectSalesforceLambda** para a versão **5.26** ou superior.
 - Após a configuração inicial, **excluir ou desabilitar a função sfExecuteAWSService**.
 - Se a função precisar permanecer ativa, restringir `lambda:InvokeFunction` ao usuário IAM utilizado pelo CTI Adapter.
- **Recomendações para Administradores de Sistema:**
 - Revisar a execution role da Lambda.
 - Remover permissões AWS desnecessárias.
 - Auditar quem possui `lambda:InvokeFunction`.
 - Utilizar SCPs ou permission boundaries para restringir operações críticas.
 - Revisar políticas de recursos da Lambda.
 - Monitorar chamadas realizadas pela execution role no **AWS CloudTrail**.
 - Investigar operações realizadas pela Lambda que não correspondam ao funcionamento esperado.
 - Confirmar que `SalesforceExecuteAWSServiceUser` corresponde ao usuário IAM autorizado.

Para saber informações mais detalhadas sobre esta vulnerabilidade acesse: [AWS Lambda Flaw Lets Attackers Bypass IAM Permissions and Access Cloud Services](#).

2.4. CVE-2026-94545 - Falha Crítica no Next.js Permite Execução Remota de Código por SVG Malicioso

A CVE-2026-94545, também identificada pelo advisory GHSA-vcvr-r3jv-pc5j, é uma vulnerabilidade crítica no componente Node.js ImageResponse do pacote next/og.

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

A falha afeta Next.js 16.2.0 até versões anteriores à 16.3.6 e pode resultar em execução remota de código quando dados controlados pelo atacante são inseridos em conteúdo SVG processado pelo servidor.

Exploração

A exploração ocorre quando uma aplicação utiliza o ImageResponse baseado em Node.js para gerar imagens dinamicamente e incorpora dados não confiáveis em elementos, atributos ou estilos SVG.

Um atacante pode enviar conteúdo especialmente elaborado por meio de parâmetros HTTP, formulários ou APIs. Se esse conteúdo chegar ao processo de renderização vulnerável, poderá ocorrer execução de código no servidor.

Aplicações que utilizam a implementação **Edge** do ImageResponse não são afetadas, segundo o advisory.

Impacto

- Execução remota de código;
- Comprometimento do servidor Next.js;
- Acesso a dados e secrets;
- Roubo de credenciais cloud;
- Alteração de conteúdo hospedado;
- Comprometimento de serviços internos;
- Utilização do servidor como ponto inicial para movimentação lateral.

Mitigação e Prevenção

- **Recomendações imediatas:**
 - Atualizar o Next.js para **16.3.6 ou superior**.
 - Identificar aplicações que utilizam next/og e ImageResponse.
 - Priorizar endpoints expostos à Internet.
 - Identificar parâmetros ou entradas de usuário que sejam inseridos em SVG.
- **Recomendações para administradores de sistema:**
 - Não inserir diretamente dados não confiáveis em SVG.
 - Validar e sanitizar entradas antes de processá-las.
 - Evitar que o processo de geração de imagens possua acesso desnecessário a secrets ou credenciais.
 - Utilizar princípio do menor privilégio para a aplicação.
 - Monitorar processos filhos inesperados do servidor Node.js.
 - Monitorar conexões de saída iniciadas pela aplicação.
 - Utilizar WAF para detectar requisições anômalas.

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

- Não considerar validação de entrada isoladamente como solução permanente; o advisory recomenda a atualização do componente.

Para saber informações mais detalhadas sobre esta vulnerabilidade acesse: <https://cybersecuritynews.com/critical-next-js-flaw-allows-remote-code-execution/>.

2.5. Windows Defender - Zero-Day BigDiskBuster Pode Impedir Atualizações do Antivírus

Pesquisadores divulgaram publicamente um exploit denominado BigDiskBuster, que pode impedir o Microsoft Defender Antivirus de realizar atualizações de plataforma e assinaturas.

Segundo o pesquisador, o método funciona nas versões suportadas do Windows e precisa permanecer executando em segundo plano para bloquear as atualizações. Diferentemente das vulnerabilidades tradicionais de RCE, o principal impacto divulgado é uma negação de serviço contra o mecanismo de atualização do Defender, deixando o sistema preso à versão atual das proteções enquanto o mecanismo estiver bloqueado.

Exploração

O exploit interfere no funcionamento do Microsoft Defender de forma que as atualizações de plataforma e assinaturas não sejam aplicadas. Isso pode ser utilizado como etapa de um ataque maior: após desabilitar ou impedir a atualização das proteções, um malware pode tentar permanecer ativo utilizando técnicas que seriam posteriormente detectadas por assinaturas mais recentes.

Impacto

- Impedimento de atualizações do Defender;
- Proteções antivírus potencialmente desatualizadas;
- Aumento da janela de exposição a malware;
- Redução da capacidade de detecção de ameaças recentes;
- Possível utilização como etapa de defesa-evasão.

Mitigação e Prevenção

- **Recomendações imediatas:**
 - Garantir que o Microsoft Defender esteja atualizado.
 - Monitorar falhas inesperadas de atualização.
 - Investigar endpoints que apresentem alterações persistentes no funcionamento do Defender.
 - Não executar ferramentas ou PoCs relacionados ao **BigDiskBuster** em endpoints corporativos.
- **Recomendações para Administradores de Sistema:**
 - Monitorar o status do Microsoft Defender por meio do Microsoft Defender for Endpoint ou ferramenta equivalente.

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

- Criar alertas para interrupção ou alteração inesperada dos serviços de segurança.
- Monitorar alterações em configurações do Defender.
- Correlacionar falhas de atualização com execução de processos desconhecidos.
- Utilizar EDR para detectar processos que tentem interferir em componentes de segurança.
- Manter políticas de proteção contra adulteração (*Tamper Protection*) habilitadas quando disponíveis.
- Restringir privilégios administrativos locais.
- Monitorar endpoints que apresentem repetidas falhas de atualização.
- Manter mecanismos complementares de detecção, como EDR, IDS/IPS e análise comportamental.
- Acompanhar os advisories da Microsoft para uma eventual correção oficial.

Para saber informações mais detalhadas sobre esta vulnerabilidade acesse: <https://www.bleepingcomputer.com/news/security/new-windows-defender-zero-day-blocks-microsoft-antivirus-updates/>.

2.6. CVE-2026-87902 - WordPress: Falha Crítica de RCE Explorada Ativamente

A CVE-2026-87902 é uma vulnerabilidade crítica no WordPress, com CVSS 9.2, que pode permitir execução remota de código sem autenticação em determinadas configurações. A exploração começou poucas horas após a divulgação da correção e evoluiu de reconhecimento para tentativa de gravação de arquivos maliciosos nos servidores afetados.

Exploração

A falha está relacionada à resolução de templates da função `get_page_template()`, que pode fazer com que um arquivo PHP local legível pelo servidor seja incluído fora dos diretórios esperados do tema. Para a exploração funcionar, determinadas condições precisam estar presentes, incluindo um diretório de nível superior iniciado por `page-` no tema ativo e um arquivo PHP local que possa ser lido pelo usuário do servidor web. Atacantes observados em campanhas reais utilizaram o `pearcmd.php` para gravar arquivos PHP controlados pelo atacante no sistema.

Impacto

- Execução remota de código;
- Instalação de web shells;
- Alteração do website;
- Comprometimento de credenciais;
- Persistência no servidor;
- Redirecionamento de visitantes;
- Comprometimento de dados;
- Utilização do servidor em ataques posteriores.

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

Mitigação e Prevenção

- **Recomendações imediatas:**

- Atualizar imediatamente para WordPress 7.1.2 ou versão corrigida correspondente à branch utilizada.
- A correção também foi disponibilizada para branches antigas até a versão 4.7; versões anteriores a 4.6 não recebem correção para essa falha.
- Revisar os logs HTTP imediatamente.
- Verificar arquivos criados recentemente em /tmp e /var/tmp.
- Procurar arquivos PHP desconhecidos no servidor.
- Caso haja indícios de exploração, isolar o servidor para investigação.

- **Recomendações para Administradores de Sistema:**

- Atualizar WordPress, temas e plugins.
- Revisar os diretórios dos temas em busca de estruturas page-* inesperadas.
- Monitorar criação e alteração de arquivos PHP.
- Verificar usuários administrativos do WordPress.
- Revisar tarefas cron e mecanismos de persistência.
- Utilizar WAF para bloquear requisições suspeitas.
- Restringir permissões de escrita do usuário do servidor web.
- Monitorar execução de processos iniciados pelo PHP/web server.
- Rotacionar credenciais caso haja evidência de comprometimento.
- Validar integridade dos arquivos do WordPress.
- Restaurar arquivos comprometidos a partir de uma fonte confiável quando necessário.

Para saber informações mais detalhadas sobre esta vulnerabilidade acesse: <https://cybersecuritynews.com/translatepress-wordpress-plugin-vulnerability/>

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