Your IT Company

Principais Vulnerabilidades e Ameaças (outubro/26)

Sumário

1. Objetivo 2
2. Vulnerabilidades e Ameaças descobertas 2
2.1. CVE-2026-72018 - Falha no Kernel Linux permite escalada de privilégios para root 2
2.2. SectopRAT - Variante oculta em software Windows adulterado 3
2.3. RedFlick - CosmicPulse distribuído por phishing e tarefas agendadas 4
2.4. Ferramentas de acesso remoto - Falsos instaladores de Zoom e PDF 5
2.5. Antino - Backdoor utiliza Microsoft 365 como canal de C2 6
2.6. WordPress - Backdoor autorreparável restaura malware removido 8
2.7. CVE-2026-96512 - Vulnerabilidade no Sudo permite bypass de restrições temporais 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-2026-72018 - Falha no Kernel Linux permite escalada de privilégios para root

A CVE-2026-72018 é uma vulnerabilidade de alta severidade no kernel Linux relacionada ao driver dibs_loopback, utilizado na implementação de comunicação SMC-D. A falha ocorre devido à ausência de validação adequada dos limites de memória durante operações de cópia, permitindo uma escrita fora dos limites de um buffer.

Exploração

A exploração requer acesso local e a capacidade CAP_NET_ADMIN. Um atacante pode manipular determinados campos da comunicação SMC-D e provocar uma escrita de 16 bytes em uma região controlada da memória do kernel.

Apesar da primitiva de exploração ser limitada, pesquisadores demonstraram que ela pode atingir estruturas de credenciais do kernel, alterando campos relacionados ao UID efetivo do processo e possibilitando a obtenção de privilégios root.

Impacto

A exploração bem-sucedida, pode permitir escalada local de privilégios, possibilitando a execução de comandos com privilégios administrativos e comprometendo a confidencialidade, integridade e disponibilidade do sistema.

Mitigação e Prevenção

- **Recomendações imediatas:**
  - Aplicar as atualizações de segurança do kernel disponibilizadas pela distribuição Linux.
  - Reiniciar os sistemas após a atualização, quando necessário.
  - Priorizar servidores e ambientes que permitam usuários ou workloads com CAP_NET_ADMIN.
- **Recomendações para Administradores de Sistema:**
  - Identificar contêineres e aplicações que possuem CAP_NET_ADMIN.
  - Remover essa capacidade quando não for necessária.
  - Monitorar atividades anômalas envolvendo namespaces, interfaces de rede e componentes SMC-D.
  - Validar se o kernel atualizado está efetivamente em execução após o reboot.

- **Recomendações para usuários finais:**
  - Evitar executar aplicações ou scripts de origem desconhecida em sistemas Linux corporativos.
  - Não conceder privilégios administrativos ou capacidades adicionais a aplicações sem necessidade operacional.

Para saber informações mais detalhadas sobre esta vulnerabilidade acesse: https://cybersecuritynews.com/ai-agent-finds-linux-kernel-bug/.

2.2. SectopRAT - Variante oculta em software Windows adulterado

A Fortinet identificou uma variante do SectopRAT (ArechClient2) escondida dentro de arquivos de um software legítimo para Windows que haviam sido adulterados. A ameaça utiliza componentes legítimos da aplicação para ocultar sua execução e arquivos criptografados para esconder o código malicioso.

Exploração

Os arquivos modificados incluem uma biblioteca que carrega componentes adicionais quando o aplicativo é executado. Uma tarefa agendada do Windows inicia o processo automaticamente.

Durante a execução, o malware utiliza múltiplas etapas de carregamento, descriptografa componentes armazenados em arquivos de banco de dados e carrega o SectopRAT diretamente na memória, dificultando sua detecção por análises convencionais de arquivos.

Impacto

O SectopRAT possui recursos de controle remoto e coleta de informações, podendo acessar dados de navegadores, clientes de e-mail, aplicativos, extensões de carteiras digitais e outros dados presentes no dispositivo.

Mitigação e Prevenção

- **Recomendações imediatas:**
  - Isolar máquinas que apresentem indicadores relacionados ao SectopRAT.
  - Realizar varredura com EDR/antivírus atualizado.
  - Verificar tarefas agendadas e bibliotecas carregadas por aplicações suspeitas.
  - Caso haja comprometimento confirmado, redefinir credenciais utilizadas no equipamento.
- **Recomendações para Administradores de Sistema:**
  - Distribuir softwares somente por canais oficiais e repositórios corporativos confiáveis.
  - Validar assinatura digital e integridade dos instaladores.
  - Monitorar criação de tarefas agendadas e carregamento incomum de DLLs.
  - Correlacionar processos, arquivos e conexões de rede no EDR/SIEM.

Classificação: Público

- **Recomendações para Usuários Finais:**
  - Não instalar programas obtidos por sites de terceiros, anúncios ou links desconhecidos.
  - Evitar versões modificadas, "crackeadas" ou distribuídas fora do canal oficial.
  - Comunicar imediatamente qualquer comportamento anormal após a instalação de um programa.

IOCs

- **C2:** 98.142.252[.]140:15847
- **Endpoint de fallback:** hxxps://bsc-dataseed1.binance[.]org/
- **Endpoint de fallback:** hxxps://bsc-dataseed2.binance[.]org/
- Bibliotecas adulteradas carregadas por executáveis legítimos.
- Tarefas agendadas associadas a aplicações que normalmente não necessitam de execução automática.

Para saber informações mais detalhadas sobre esta vulnerabilidade acesse: https://cybersecuritynews.com/fortinet-uncovers-sectoprat/.

2.3. RedFlick - CosmicPulse distribuído por phishing e tarefas agendadas

A campanha RedFlick, associada ao grupo Star Blizzard, utiliza campanhas de phishing para distribuir o backdoor CosmicPulse. A atividade observada em 2026 utiliza arquivos compactados protegidos por senha, imagens VHDX, atalhos maliciosos e tarefas agendadas para estabelecer a infecção.

Exploração

O ataque começa com mensagens que podem aparentar ser parte de uma conversa legítima. A vítima recebe um arquivo compactado protegido por senha contendo uma imagem VHDX.

Ao abrir o conteúdo, um arquivo LNK disfarçado de documento PDF executa um script BAT oculto. O script apresenta um documento legítimo como isca e utiliza componentes do Windows para baixar e executar o instalador malicioso.

Em campanhas posteriores, foram observadas três tarefas agendadas com nomes semelhantes a componentes legítimos, como Internet Quality Test Connection, Network Configuration Manager e System Health Monitor.

Impacto

A infecção pode estabelecer persistência no sistema, executar componentes adicionais e permitir o acesso remoto ao equipamento, possibilitando espionagem e comprometimento de informações corporativas.

Mitigação e Prevenção

- **Recomendações imediatas:**

Classificação: Público

- Bloquear ou colocar em quarentena anexos compactados protegidos por senha provenientes de fontes não confiáveis.
- Investigar tarefas agendadas criadas recentemente.
- Verificar execução de arquivos LNK, BAT, MSI e VHDX provenientes de e-mails.
- Isolar equipamentos com sinais de execução do CosmicPulse.

- **Recomendações para Administradores de Sistema:**
  - Monitorar criação de tarefas agendadas e execução de scripts por processos inesperados.
  - Restringir a execução de arquivos provenientes de diretórios temporários e anexos de e-mail.
  - Monitorar o uso de WebDAV, curl, SSH e outros componentes utilizados para baixar cargas.
  - Implementar regras de detecção para execução encadeada de LNK > BAT > MSI.
- **Recomendações para Usuários Finais:**
  - Não abrir anexos protegidos por senha quando a origem ou o contexto não forem esperados.
  - Não executar arquivos .lnk, .bat, .msi,. vhdx ou similares recebidos por e-mail sem validação.
  - Confirmar diretamente com o remetente solicitações inesperadas de abertura de arquivos.
  - Reportar mensagens suspeitas à equipe de segurança.

Para saber informações mais detalhadas sobre esta vulnerabilidade acesse: https://gbhackers.com/redflick-backdoor/.

2.4. Ferramentas de acesso remoto - Falsos instaladores de Zoom e PDF

Uma campanha identificada pela Microsoft utiliza falsos instaladores de Zoom, leitores de PDF e outros aplicativos para instalar ferramentas legítimas de acesso remoto, incluindo MSP360 RMM e ScreenConnect. O ataque não explora uma vulnerabilidade dessas ferramentas; os criminosos abusam de seus recursos legítimos para obter controle remoto dos dispositivos.

Exploração

As vítimas recebem mensagens de phishing relacionadas a reuniões, documentos, convites, processos seletivos ou notificações corporativas. Os links direcionam para páginas que simulam sites legítimos de download.

Após a execução do instalador e aprovação da solicitação de privilégios administrativos, o software de acesso remoto é instalado e configurado para inicialização automática. Em alguns casos, também é criada uma regra de firewall para permitir o funcionamento do agente.

Classificação: Público

Impacto

O atacante pode obter controle remoto do dispositivo, executar comandos, transferir arquivos e utilizar o acesso para roubo de credenciais ou movimentação lateral.

Mitigação e Prevenção

- **Recomendações imediatas:**
  - Identificar instalações não autorizadas de MSP360, ScreenConnect ou outras ferramentas RMM.
  - Isolar equipamentos nos quais uma dessas ferramentas tenha sido instalada sem autorização.
  - Remover softwares de acesso remoto não autorizados após a investigação.
  - Alterar credenciais potencialmente expostas.
- **Recomendações para administradores de sistema:**
  - Manter inventário atualizado das ferramentas RMM autorizadas.
  - Criar regras para detectar instalações ou execução de softwares de acesso remoto não aprovados.
  - Restringir privilégios administrativos para instalação de aplicações.
  - Monitorar criação de serviços, regras de firewall e mecanismos de inicialização associados a RMM.
  - Correlacionar eventos de instalação com conexões externas e autenticações.
- **Recomendações para administradores de sistema:**
  - Baixar aplicativos somente de sites oficiais.
  - Não instalar programas solicitados por links recebidos em e-mails inesperados.
  - Não aprovar solicitações de administrador sem confirmar a legitimidade da instalação.
  - Em caso de dúvida, procurar a equipe de TI antes de instalar o software.

Para saber informações mais detalhadas sobre esta vulnerabilidade acesse: https://cybersecuritynews.com/remote-access-tools/.

2.5. Antino - Backdoor utiliza Microsoft 365 como canal de C2

O Antino é um backdoor para Windows que utiliza Microsoft Graph, Outlook e OneDrive como infraestrutura de comando e controle (C2). Dessa forma, o malware consegue utilizar serviços legítimos do Microsoft 365 para receber comandos, enviar informações e transferir arquivos, dificultando a identificação de uma infraestrutura C2 tradicional.

Exploração

A infecção começa principalmente por phishing, documentos maliciosos e instaladores falsos. Após a execução, o malware pode utilizar técnicas como DLL Sideloading, PowerShell e componentes legítimos do Windows.

Classificação: Público

O Antino consulta uma caixa de e-mail controlada pelos atacantes para receber comandos e utiliza o OneDrive para enviar informações de status, armazenar dados coletados e receber ferramentas adicionais. A ameaça também pode executar comandos de shell e PowerShell, transferir arquivos e carregar código adicional em memória.

Impacto

O uso de serviços legítimos do Microsoft 365 como canal de comunicação pode dificultar a detecção baseada exclusivamente em bloqueio de domínios ou IPs. O comprometimento pode resultar em execução remota de comandos, coleta e exfiltração de arquivos, manutenção de acesso e comprometimento de informações corporativas.

Mitigação e Prevenção

- **Recomendações imediatas:**
  - Investigar endpoints que executem slc.dll, GatherOsState.exe, mshta.exe ou sdiagnhost.exe em contextos anômalos.
  - Verificar aplicações e credenciais utilizadas para acessar Microsoft Graph.
  - Investigar acessos incomuns ao Outlook e OneDrive associados a endpoints comprometidos.
  - Isolar máquinas com indicadores confirmados.
- **Recomendações para Administradores de Sistema:**
  - Monitorar aplicações do Entra ID e permissões concedidas ao Microsoft Graph.
  - Auditar acessos a caixas de e-mail e OneDrive.
  - Detectar DLL Sideloading e execução anômala de PowerShell/MSHTA.
  - Correlacionar logs de endpoint, Entra ID, Microsoft 365 e rede.
  - Restringir privilégios de aplicações que não necessitem acessar e-mail ou armazenamento corporativo.
- **Recomendações para Usuários Finais:**
  - Não abrir anexos ou links inesperados.
  - Confirmar a origem de documentos relacionados a assuntos institucionais ou administrativos.
  - Não executar instaladores recebidos por e-mail sem validação.
  - Reportar mensagens suspeitas à equipe de segurança.

IOCs

- **SHA-256:** 09ef7c736bccfafef44d9910d499173b88063b73b221fc0dc9e9105107e5cff
- **SHA-256:** e2eb7703047b37b28dc34e6990205d758a2454b39bc655b460606745fadcb530
- **Arquivo:** slc.dll

Classificação: Público

- **Arquivo:** GatherOsState.exe
- **Domínio:** osc-cdn[.]com
- **Domínio:** microsoft-flash[.]com
- **Domínio:** wps-cn[.]com
- **IP:** 103[.]27[.]110[.]220
- **Caminho OneDrive:** /antino/heartbeats/{id}.json
- **Assuntos de e-mail:** command_req_[session_id] e command_res_[session_id]

Para saber informações mais detalhadas sobre esta vulnerabilidade acesse: https://cybersecuritynews.com/remote-access-tools/.

2.6. WordPress - Backdoor autorreparável restaura malware removido

Uma campanha recente utiliza uma backdoor denominada SC, capaz de restaurar seus próprios componentes após tentativas de remoção. A ameaça distribui cópias do código malicioso entre arquivos do WordPress, banco de dados e memória do servidor, dificultando a limpeza convencional.

Exploração

A backdoor utiliza mecanismos de carregamento antecipado do PHP, plugins, temas, banco de dados, tarefas agendadas e outros componentes para manter múltiplos mecanismos de persistência.

Quando um dos arquivos maliciosos é removido, componentes sobreviventes podem recriá-lo. A ameaça também pode ocultar contas administrativas, coletar tokens de sessão e remover plugins de segurança. Para comunicação, utiliza consultas a gateways públicos relacionados à blockchain Ethereum.

Impacto

O comprometimento pode permitir manutenção de acesso administrativo, alteração do conteúdo do site, roubo de sessões, execução de código PHP e distribuição de scripts maliciosos aos visitantes. A simples remoção do arquivo identificado pode não eliminar a infecção.

Mitigação e Prevenção

- **Recomendações imediatas:**
  - Colocar o site em modo de manutenção ou restringir temporariamente o acesso administrativo.
  - Preservar evidências antes de iniciar a limpeza.
  - Identificar e remover todos os mecanismos de persistência de forma coordenada.
  - Alterar credenciais administrativas, FTP/SFTP, banco de dados e hospedagem após a contenção.
  - Executar nova varredura após a limpeza para verificar se os arquivos retornam.

Classificação: Público

- **Recomendações para Administradores de Sistema:**
  - Inspecionar .user.ini, php.ini, .htaccess, plugins normais e mu-plugins.
  - Verificar usuários administrativos diretamente no banco de dados.
  - Revisar tarefas cron, triggers e opções do WordPress.
  - Atualizar WordPress, plugins e temas.
  - Utilizar WAF e monitoramento de integridade dos arquivos.
  - Em ambientes compartilhados, verificar outros sites hospedados no mesmo servidor.

IOCs

- .user.ini, php.ini ou .htaccess contendo auto_prepend_file não autorizado.
- Diretório wp-content/mu-plugins.
- Plugin suspeito em wp-content/plugins.
- Arquivo observado: wp-content/plugins/hyper-engine-kit/hyper-engine-kit.php.
- Arquivos ou ZIPs de recuperação com nomes aleatórios.
- Constante SC_AUTO_PREPEND.
- Prefixo SC_ em componentes injetados.
- Registros de banco de dados contendo grandes blobs gzip/base64.
- Tarefas cron e triggers de banco de dados não autorizados.
- Conexões de saída para gateways públicos de RPC da Ethereum.

Para saber informações mais detalhadas sobre esta vulnerabilidade acesse: https://cybersecuritynews.com/wordpress-malware-2/.

2.7. CVE-2026-96512 - Vulnerabilidade no Sudo permite bypass de restrições temporais

A **CVE-2026-96512** é uma vulnerabilidade de alta severidade no **Sudo** que pode permitir que usuários locais contornem restrições temporais configuradas em regras do sudoers. A falha está relacionada ao processamento da variável de ambiente **TZ**, utilizada durante a interpretação de regras que possuem as condições NOTBEFORE e NOTAFTER.

Exploração

Um atacante precisa possuir uma conta local e uma regra do Sudo afetada por restrições temporais. Ao fornecer um valor de TZ especialmente elaborado, como TZ=XXX24, o atacante pode alterar a interpretação dos horários utilizados pelo Sudo.

Isso pode fazer com que uma autorização já expirada seja interpretada como válida ou que uma autorização futura seja considerada disponível antes do período definido. A falha não elimina a autenticação por senha ou PAM e depende da existência de regras temporais afetadas.

Classificação: Público

Impacto

A exploração pode permitir que um usuário local execute comandos privilegiados fora do período autorizado, enfraquecendo controles de acesso temporário e podendo resultar em escalada de privilégios.

Mitigação e Prevenção

- **Recomendações imediatas:**
  - Identificar sistemas que utilizam Sudo entre as versões afetadas.
  - Localizar regras NOTBEFORE e NOTAFTER configuradas no sudoers.
  - Aplicar as atualizações fornecidas pelo fabricante/distribuição assim que disponíveis.
  - Monitorar comandos sudo executados fora dos horários normalmente autorizados.
- **Recomendações para Administradores de Sistema:**
  - Revisar políticas temporais presentes em /etc/sudoers e /etc/sudoers.d/.
  - Utilizar timestamps com UTC ou deslocamento explícito de fuso horário nas regras temporais.
  - Restringir o acesso local a usuários confiáveis.
  - Monitorar alterações no sudoers e atividades administrativas incomuns.
  - Manter o pacote Sudo atualizado por meio dos repositórios oficiais da distribuição.

Para saber informações mais detalhadas sobre esta vulnerabilidade acesse: https://cybersecuritynews.com/sudo-security-vulnerability/#google_vignette.

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

Classificação: Público