Your IT Company

Principais Vulnerabilidades e Ameaças (janeiro/26)

Sumário

1. Objetivo 2
2. Vulnerabilidades e Ameaças descobertas 2
2.1. Vulnerabilidades de elevação de privilégios no Windows (Windows LPE) 2
2.2. Sites falsos do WinRAR que distribuem o malware Winzipper 3
2.3. Hackers exploram falha crítica no plugin Modular DS do WordPress para obter acesso administrativo .5
2.4. Hackers abusam de provedores de nuvem e CDN legítimos para hospedar kits de phishing 6
2.5. Falha no Windows Remote Assistance permite contornar Mark of the Web 7

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. Vulnerabilidades de elevação de privilégios no Windows (Windows LPE)

Pesquisadores de segurança destacaram a importância de identificar e mitigar vulnerabilidades de Elevação de Privilégios Locais (LPE – Local Privilege Escalation) em sistemas Microsoft Windows, dado o uso frequente dessas falhas em ataques avançados. As vulnerabilidades LPE permitem que agentes maliciosos com acesso inicial ao sistema (geralmente com privilégios baixos) possam obter o controle total do sistema operacional, contornando restrições de segurança como UAC (User Account Control) e políticas de acesso.

Exploração

Vulnerabilidades tipo LPE no Windows são frequentemente exploradas em sequências de ataque pós-comprometimento, onde o invasor já obteve um ponto de presença (por exemplo, via RDP, spearphishing, malware ou credenciais roubadas) e busca elevar seus privilégios para SYSTEM ou Administrador para expandir controle. As técnicas de hunting destacadas no artigo incluem:

- **Análise de Permissões de Serviços e Drivers:** Verificação de serviços com permissões excessivas, incluindo serviços que podem ser manipulados por usuários não-administradores.
- **Verificação de ACLs (Listas de Controle de Acesso):** Auditoria de arquivos, chaves de registro e objetos do sistema que possuem permissões incorretas permitindo sobrescrita ou manipulação.
- **Inspeção de Pacotes de Instalação e Atualizações:** Identificação de padrões falhos em instaladores que escrevem em caminhos protegidos sem validação de permissões.
- **Procura por Unquoted Service Paths:** Serviços instalados com caminhos de binários sem aspas podem permitir que um atacante injete executáveis maliciosos quando a cadeia de diretórios possui espaços.
- **Componentes COM Inadequadamente Registrados:** Objetos COM com interfaces inseguras podem ser acionados por processos de menor privilégio para executar código em contexto elevado.
- **Drivers e Interfaces do Kernel:** Verificação de drivers que expõem IOCTLs não seguros, que podem ser invocados para ler/gravar memória do kernel ou contornar verificações de segurança.

Classificação: Público

Mitigação e Prevenção

- Aplicar todos os patches de segurança do Microsoft Windows regularmente, incluindo atualizações cumulativas.
- Auditar permissões de serviços, chaves de registro e arquivos críticos, garantindo que apenas administradores possuam controle de escrita.
- Revisar ACLs em diretórios do sistema e binários essenciais, corrigindo exceções que permitam modificações inadequadas.
- Corrigir caminhos de serviços não citados (“unquoted service paths”), garantindo que tenham aspas corretas para prevenir injeção.
- Bloquear interfaces expostas de drivers inadequados ou com IOCTLs inseguros, se possível, removendo ou atualizando drivers de terceiros com falhas conhecidas.

Para saber informações mais detalhadas sobre esta vulnerabilidade acesse: https://gbhackers.com/hunting-windows-lpe-flaws/ .

2.2. Sites falsos do WinRAR que distribuem o malware Winzipper

Uma campanha de malware descobriu sites falsos de download do WinRAR para distribuir o trojan Winzipper a usuários que baixam o instalador de fontes não oficiais. A ameaça usa um instalador trojanizado e técnicas de execução em memória para evitar detecção, sendo relevante tanto para usuários domésticos quanto para ambientes corporativos.

Exploração

- **Vetor de ataque:** Links distribuídos em diversos sites chineses que apontam para instaladores trojanizados do WinRAR.
- **Técnica de entrega:** Arquivo original chamado winrar-x64-713scp.zip contém um executável empacotado com UPX e um SFX que, ao ser analisado, expõe o instalador legítimo do WinRAR e um arquivo protegido por senha chamado setup.hta.
- **Execução:** O setup.hta é o componente malicioso; permanece ofuscado até o runtime, quando é desempacotado diretamente na memória (execução em memória), evitando detecção baseada em arquivos. Em análise dinâmica, o malware gera o processo nimasila360.exe, associado à família Winzipper.
- **Capacidades do Winzipper:** Funciona como um trojan backdoor, permitindo acesso remoto, roubo de dados e instalação de payloads secundários. O malware também perfila o sistema (acesso a informações do perfil do Windows) para escolher o payload mais eficaz para cada vítima, aumentando a taxa de sucesso.
- **Impacto potencial:** Comprometimento de contas e dados, controle remoto de máquinas, movimento lateral em redes corporativas e instalação de outras ameaças.

Classificação: Público

Mitigação e Prevenção

- Recomendações gerais:
  - Faça download do WinRAR apenas do site oficial (https://www.rarlab.com) e verifique assinaturas e checksums quando disponíveis.
  - Mantenha soluções antivírus/EDR atualizadas e ative proteção em tempo real.
  - Evite abrir arquivos SFX/EXE obtidos de sites de terceiros ou links não verificados.
  - Desative a execução automática de HTA/Script quando possível e bloqueie extensões executáveis recebidas via download não confiável.
- Recomendações para administradores de TI/Segurança:
  - Bloqueie/domine o acesso às seguintes domains maliciosas nos proxies/filtragem DNS (ver IOCs).
  - Monitore e crie regras SIEM/EDR para processos suspeitos: execução de arquivos a partir de diretórios temporários, presença de nimasila360.exe, e execução em memória de HTA/PEs empacotados com UPX.
  - Implementar inspeção de arquivos compactados em gateways de e-mail/web e sandboxing de instaladores desconhecidos.
  - Aplicar políticas de aplicação restritiva (whitelisting/APP-Locker) para impedir execução de instaladores não aprovados.
  - Procedimentos de resposta a incidentes: isolar sistemas suspeitos, coletar logs/IOCs, realizar varredura forense de memória e discos, e reimaginar sistemas comprometidos quando necessário.
- Recomendações para usuários finais:
  - Verifique sempre a fonte do download e prefira o site oficial.
  - Não execute arquivos extraídos de ZIP/SFX sem confirmar a origem.
  - Mantenha backups atualizados e use autenticação multifator nas contas críticas.

IOCs

- domínios maliciosos: winrar-tw.com, winrar-x64.com, winrar-zip.com
- nomes de arquivos / artefatos: winrar-x64-713scp.zip, setup.hta, nimasila360.exe
- Observação: hashes de arquivos e endereços IP não foram fornecidos no artigo.

Para saber informações mais detalhadas sobre esta vulnerabilidade acesse: https://cybersecuritynews.com/beware-of-fake-winrar-website/.

Classificação: Público

2.3. Hackers exploram falha crítica no plugin Modular DS do WordPress para obter acesso administrativo

O Modular DS, plugin de gerenciamento para WordPress com mais de 40.000 instalações, contém uma falha de gravidade máxima (CVE-2026-23550) que permite bypass de autenticação e login automático como administrador. A exploração ativa foi detectada em 13 de janeiro de 2026 e exige ação imediata dos administradores para evitar comprometimento total dos sites gerenciados.

Exploração

O Modular DS (versões 2.5.1 e anteriores) permite gerenciar múltiplos sites WordPress a partir de uma única interface, executar updates, gerenciar usuários, acessar informações do servidor e efetuar login remoto. A vulnerabilidade decorre de falhas de design e implementação, quando o modo "direct request" está ativo o plugin aceita requisições como confiáveis sem verificação criptográfica de origem, expondo rotas sensíveis.

Essa vulnerabilidade permite acesso administrativo remoto, permite instalação de backdoors, criação de contas administrativas rogue, modificação de conteúdo, mineração de dados dos sites e comprometimento da infraestrutura de hospedagem gerenciada.

Mitigação e Prevenção

- Ações imediatas:
  - Atualizar o plugin modular DS para a versão *2.5.2* ou superior o mais rápido possível.
  - Se não for possível atualizar imediatamente, desative o plugin até que seja possível aplicar a correção.
- Verificações e remediação pós-atualização:
  - Revisar logs de acesso do servidor e do WordPress em busca de requisições suspeitas às rotas do Modular DS (especialmente requisições que acionem login sem user_id).
  - Auditar usuários administrativos: remover contas desconhecidas ou suspeitas e forçar troca de senhas para contas administrativas.
  - Regenerar os WordPress salts (AUTH_KEY, SECURE_AUTH_KEY, etc.) conforme recomendado pelo fornecedor.
  - Verificar integridade dos arquivos do site e procurar por webshells, arquivos modificados ou scripts maliciosos.
  - Rotacionar credenciais sensíveis (senhas, chaves API) associadas às contas afetadas.
- Recomendações para proteção adicional (administradores e provedores):
  - Restringir o acesso a endpoints de gerenciamento (ex.: via regras de WAF, bloqueio por IP ou autenticação adicional).
  - Implementar monitoramento e alertas para atividades suspeitas relacionadas ao plugin (criação de usuários, logins incomuns).

Classificação: Público

- Manter um processo de atualização e resposta a incidentes, com backups recentes antes de aplicar mudanças.
- Aplicar princípio do menor privilégio nas contas usadas para gerenciamento remoto.

Para saber informações mais detalhadas sobre esta vulnerabilidade acesse: https://www.bleepingcomputer.com/news/security/hackers-exploit-modular-ds-wordpress-plugin-flaw-for-admin-access/.

2.4. Hackers abusam de provedores de nuvem e CDN legítimos para hospedar kits de phishing

Atacantes passaram a hospedar kits de phishing em plataformas de nuvem e CDN legítimas (Google, Microsoft Azure, AWS CloudFront, Firebase, Google Sites), dificultando a detecção por filtros que se baseiam em reputação de domínio. A técnica mira principalmente credenciais corporativas e aumenta a probabilidade de vítimas fornecerem logins por exibir domínios familiares e confiáveis.

Exploração

Em vez de usar domínios recém-registrados e claramente maliciosos, os operadores hospedam páginas de phishing em serviços legítimos (Azure Blob, Firebase Storage, CloudFront, Google Sites). O conteúdo HTML malicioso é servido a partir de infraestrutura legítima, portanto checagens simples de reputação do domínio frequentemente não disparam alertas. O alvo principal são usuários corporativos, as campanhas filtram contas grátis para focar em e-mails empresariais e credenciais de trabalho.

O ataque apresenta impactos potenciais significativos, incluindo a coleta de credenciais corporativas, possível acesso a e-mails e recursos internos, movimentação lateral e comprometimento da organização. Além disso, o phishing hospedado em infraestrutura legítima dificulta bloqueios automáticos e procedimentos de resposta, podendo atrasar as ações de contenção e remoção.

Mitigação e Prevenção

- Recomendações gerais:
  - Adotar análise comportamental e inspeção do conteúdo (HTML/JS) em tempo real, não apenas checagem de reputação de domínio.
  - Usar sandboxing e análise dinâmica de páginas suspeitas para identificar kits de phishing (ex.: ferramentas que executam interações e detectam páginas de login falsificadas).
  - Implementar filtros de URL avançados que reescrevam/inspecionem links em e-mails e navegação (URL rewriting + click-time analysis).
  - Integrar inteligência de ameaça que busque padrões de abuso em serviços de nuvem (Azure Blob, Firebase, CloudFront, Google Sites).
  - Ativar bloqueio e takedown automático/reportar para provedores de nuvem (Google, Microsoft, AWS) quando IOCs forem identificados.

Classificação: Público

- Para administradores de sistema:
  - Exigir e reforçar MFA resistente a phishing (chaves FIDO2 / autenticação baseada em hardware) e reduzir dependência de OTPs que podem ser proxyados.
  - Implementar Single Sign-On (SSO) com políticas de verificação de origem e detecção de anomalias de sessão.
  - Configurar políticas de detecção de exfiltração e monitoramento de credenciais vazadas em logs de autenticação.
  - Habilitar proteção avançada de e-mail (ATP, Safe Links, sandboxing de anexos e links) e regras que bloqueiem links para armazenamento público de nuvem quando improdutivos.
  - Treinar equipes de SOC para analisar padrões comportamentais (ex.: páginas que solicitam credenciais em domínios de armazenamento).
- Recomendações para usuários finais:
  - Verificar com atenção a barra de endereços e suspeitar de páginas de login não iniciadas a partir do fluxo usual da empresa (mesmo que o domínio pareça familiar).
  - Nunca inserir credenciais em páginas acessadas por links em e-mails sem confirmar com o remetente.
  - Relatar tentativas de phishing ao time de segurança imediatamente.
  - Preferir métodos de autenticação phishing-resistant (chaves físicas) quando oferecido.

Para saber informações mais detalhadas sobre esta vulnerabilidade acesse: https://cybersecuritynews.com/hackers-abusing-legitimate-cloud/.

2.5. Falha no Windows Remote Assistance permite contornar Mark of the Web

A CVE-2026-20824 é uma vulnerabilidade de security feature bypass no Windows Remote Assistance que permite a invasores locais, mediante interação do usuário, contornar a proteção Mark of the Web (MOTW). A falha afeta diversas versões do Windows, desde o Windows 10 até o Windows Server 2025, sendo necessária a aplicação das atualizações de segurança disponibilizadas pela Microsoft para mitigação do risco.

Exploração

O Mark of the Web (MOTW) é um mecanismo que marca arquivos baixados de fontes não confiáveis para restringir ações potencialmente perigosas ao abri-los. A falha decorre de uma falha na validação/processamento de conteúdo baixado pelo componente Windows Remote Assistance, permitindo que arquivos maliciosos sejam tratados como confiáveis se o exploit for conduzido corretamente.

Classificação: Público

Os vetores comuns desta vulnerabilidade, visam ataques de engenharia social, especialmente e-mails com anexos atraentes e sites comprometidos ou controlados por atacantes que induzem o usuário a baixar e abrir arquivos maliciosos.

Os requisitos para exploração incluem acesso local ao sistema (ou a indução do usuário a executar o arquivo) e interação do usuário. A exploração em larga escala é considerada tecnicamente menos provável no momento (classificada pela Microsoft como “Exploitation Less Likely”); entretanto, caso explorada, pode permitir a evasão de controles baseados em MOTW, possibilitando execução de código ou o comprometimento da confidencialidade.

Foram identificadas múltiplas edições e versões afetadas, incluindo Windows 10, Windows 11 e Windows Server 2012, 2016, 2019, 2022 e 2025.

Mitigação e Prevenção

- Ações imediatas (prioridade alta):
  - Aplicar os patches Microsoft listados para sua versão/arquitetura conforme os KBs fornecidos abaixo. Trate os updates como “Required”.
  - Testar e aplicar atualizações dentro das janelas de manutenção padrão; priorizar servidores e estações críticas.
- Recomendações para administradores de TI:
  - **Mapear inventário e aplicar o KB correspondente:**
    1. Windows 10 (1607, 1809, 21H2, 22H2): KB5073722, KB5073723, KB5073724 (22H2 — x86/ARM64/x64 → KB5073724).
    2. Windows 11 (23H2, 24H2, 25H2): KB5073455, KB5074109 (escolher conforme arquitetura).
    3. Windows Server 2012 / 2012 R2: KB5073696, KB5073698.
    4. Windows Server 2016: KB5073722.
    5. Windows Server 2019: KB5073723.
    6. Windows Server 2022 (todas, 23H2 Edition): KB5073457, KB5073450.
    7. Windows Server 2025: KB5073379.
  - Se o Remote Assistance não for necessário, desabilitar o recurso via políticas de grupo ou inventário de software.
  - **Implementar/reforçar controles de prevenção:** Application Control (AppLocker/WDAC), políticas de execução restrita, e regras de bloqueio para tipos de arquivo comumente usados em engenharia social (ex.: .exe, .msi, .scr) quando apropriado.
  - **Fortalecer detecção e resposta:** Atualizar assinaturas de EDR/antivírus e criar regras para monitorar abertura de arquivos vindos de fontes externas sem marcação de MOTW.

Classificação: Público

- **Filtragem de e-mail e web:** Bloquear anexos suspeitos, ampliar sandboxing de anexos e uso de preview em vez de download/execução; treinar regras de detecção para campanhas de phishing.
- Testar patches em ambiente controlado antes de deploy em produção; documentar rollback procedures.

- Recomendações para usuários finais:
  - Não abrir anexos ou arquivos baixados de fontes desconhecidas ou inesperadas.
  - Verificar remetente e confirmar via outro canal antes de abrir arquivos solicitados por e-mail.
  - Manter o sistema e software antivírus atualizados; aplicar atualizações quando liberadas pela TI.

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

Classificação: Público