Your IT Company

Principais Vulnerabilidades e Ameaças (Fevereiro/25)

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. Vulnerabilidade crítica de desvio de autenticação de contas da Microsoft permite que invasores obtenham acesso remoto

A Microsoft emitiu um comunicado de segurança para uma vulnerabilidade crítica de desvio de autenticação que pode permitir que invasores falsifiquem credenciais e obtenham acesso não autorizado a contas da Microsoft. A vulnerabilidade identificada como CVE-2025-21396, foi classificada pela NIST com uma pontuação de nível crítica CVSS 3.1:9.8 e possui a seguinte descrição. “A falta de autorização na conta da Microsoft permite que um invasor não autorizado eleve privilégios em uma rede.”

A vulnerabilidade está ligada ao CWE-290, Authentication Bypass by Spoofing, uma fraqueza bem documentada que afeta os mecanismos de autenticação que dependem de métodos de validação insuficientes ou falhos. Essa falha pode afetar particularmente os sistemas em que a confiança é depositada em fontes como endereços IP ou nomes DNS, ambos suscetíveis à manipulação por invasores.

Exploração

O Authentication Bypass by Spoofing define um cenário em que um invasor pode enganar o sistema para aceitá-lo como um usuário autenticado, apresentando credenciais falsas ou manipulando parâmetros de autenticação. O problema surge de mecanismos de autenticação projetados incorretamente que não conseguem validar de forma robusta as solicitações recebidas.

As explorações podem envolver:

Falsificação de IP: o invasor forja seu endereço IP de origem para se passar por um sistema confiável.

Falsificação de DNS: envenenar o cache DNS para apresentar um domínio controlado pelo invasor como legítimo.

Solicitações malformadas ou manipuladas: exploração de lógica de validação fraca em protocolos de camada de aplicativo.

Exemplos de vetores de ataque

Os invasores que aproveitam essa vulnerabilidade podem explorar:

Uso de validação de origem baseada em endereço IP.
Exemplo em Java:

```
String sourceIP = request.getRemoteAddr();
if (sourceIP != null && sourceIP.equals(APPROVED_IP)) {
    authenticated = true;
```

```
}
```

Nesse caso, um invasor falsificando o endereço IP pode ignorar a autenticação.

A verificação de host baseada em DNS é onde o invasor manipula as respostas DNS para criar uma falsa sensação de confiança.
Exemplo em C:

```
struct hostent *hp;
struct in_addr myaddr;
char *tHost = "trustme.example.com";
myaddr.s_addr = inet_addr(ip_addr_string);
hp = gethostbyaddr((char *)&myaddr, sizeof(struct in_addr), AF_INET);
if (hp && !strncmp(hp->h_name, tHost, sizeof(tHost))) {
    trusted = true;
}
```

Um invasor envenenando o cache DNS pode explorar isso para se passar por uma fonte confiável. Devido à facilidade de executar falsificação de IP ou envenenamento de cache DNS em determinados cenários, essa vulnerabilidade é categorizada como tendo uma alta probabilidade de exploração.

Mitigação e Prevenção

A Microsoft lançou patches abordando a causa raiz do CVE-2025-21396. Os clientes são aconselhados a tomar as seguintes medidas preventivas:

Aplique atualizações de segurança: atualize regularmente os sistemas operacionais e o software para as versões mais recentes. Consulte o Guia de Atualização de Segurança da Microsoft para obter instruções específicas.

Adote mecanismos de autenticação mais fortes: Evite depender apenas de endereços IP ou nomes DNS para mecanismos de confiança. Em vez disso, use alternativas seguras, como autenticação multifator (MFA), tokens criptográficos para validação de identidade, TLS mútuo para conexões seguras.

Monitore redes em busca de anomalias: configure sistemas de detecção de intrusão (IDS) para identificar pacotes falsificados ou comportamento incomum de DNS.

Fortaleça a infraestrutura de DNS: implemente o DNSSEC para mitigar os riscos de falsificação de DNS.

Ativar registro: mantenha registros detalhados de tentativas de autenticação para análise forense em caso de tentativas de exploração.

Para ver mais detalhes sobre esta vulnerabilidade você pode acessar os endereços a seguir: https://cybersecuritynews.com/crtical-microsoft-accounts-authentication-bypass-vulnerability/ e https://nvd.nist.gov/vuln/detail/CVE-2025-21396

2.2. Vulnerabilidade na ferramenta no plugin WPSpins Post/Page Copying Tool do WordPress

Uma vulnerabilidade crítica foi descoberta na plugin WPSpins Post/Page Copying Tool, que costuma ser amplamente utilizada no WordPress. A falha, foi classificada como uma execução remota de código (RCE), ela permite que atacantes injetem e executem comandos remotos maliciosos em um site vulnerável. A vulnerabilidade foi identificada até a versão 2.0.3 do plugin, sendo corrigida na versão 2.0.4.

A falha ocorre devido a um controle inadequado na geração de código, permitindo que atacantes explorem a vulnerabilidade para executar comandos maliciosos. Isso pode resultar em acessos backdoor, comprometimento do site e possível controle total pelo invasor.

A vulnerabilidade identificada como CVE-2025-24677, foi classificada pela Patchstack com uma pontuação de nível crítica CVSS:3.1:9.9 e possui a seguinte descrição. “A vulnerabilidade de controle inadequado da geração de código ('injeção de código') no plugin WPSpins Post/Page Copying Tool permite a inclusão remota de código.” A CVE em questão, ainda não foi classificada pela NIST.

Exploração

Atualmente, não há evidências de que exista uma prova de conceito (PoC) pública ou exploração conhecida para a vulnerabilidade.

Entretanto, a vulnerabilidade possui um alto potencial de exploração, permitindo que agentes mal-intencionados assumam o controle do site e injetem códigos prejudiciais. Isso pode comprometer a integridade dos dados, afetar a privacidade dos usuários e até levar à desativação completa do site.

Mitigação e Prevenção

Os administradores de sites WordPress que utilizam o plug-in WPSpins devem tomar as seguintes medidas imediatamente:

Atualizar o plug-in: A versão 2.0.4 corrige a falha e deve ser instalada o mais rápido possível.

Aplicar o vPatch: O Patchstack lançou um patch virtual para mitigar o problema temporariamente.

Além disso, implementar validação e sanitização de entrada, utilizar um firewall de aplicações web (WAF) e aplicar o princípio do menor privilégio podem ajudar a mitigar os riscos associados a essa vulnerabilidade.

Para ver mais detalhes sobre esta vulnerabilidade você pode acessar os endereços a seguir: https://www.tenable.com/cve/CVE-2025-24677 e https://patchstack.com

2.3. Vulnerabilidades de dia zero nas ferramentas do Microsoft Sysinternals, permitem ataques de injeção de DLL no Windows.

As ferramentas Sysinternals formam um conjunto essencial de utilitários avançados projetados para auxiliar administradores e desenvolvedores de TI na análise e diagnóstico de sistemas Windows. Entre os principais componentes, destacam-se o Process Explorer, Autoruns, Bginfo e diversas outras soluções que oferecem visibilidade sobre processos, serviços e configurações do sistema.

Apesar de sua importância, esses utilitários não são integrados ao Windows Update, impossibilitando a aplicação automática de correções de segurança. Isso cria um vetor de risco significativo, uma vez que vulnerabilidades exploráveis podem permanecer ativas até que as atualizações sejam identificadas e aplicadas manualmente, exigindo vigilância contínua por parte dos profissionais de segurança.

Vulnerabilidade

Uma vulnerabilidade crítica de dia zero foi descoberta nas ferramentas Microsoft Sysinternals, representando um risco significativo para sistemas Windows. Esses utilitários, amplamente utilizados por administradores de TI e desenvolvedores, apresentam falhas no mecanismo de carregamento de bibliotecas de vínculo dinâmico (DLL), tornando-os suscetíveis a ataques de injeção de DLL.

A vulnerabilidade permite que invasores injetem e executem código malicioso no contexto do processo alvo, potencialmente levando ao comprometimento total do sistema, escalonamento de privilégios e persistência de ameaças. A vulnerabilidade em questão, ainda não possui uma CVE identificada.

Exploração

A vulnerabilidade decorre da maneira como as ferramentas Sysinternals, incluindo Process Explorer, Autoruns e Bginfo, lidam com o carregamento de bibliotecas de vínculo dinâmico (DLLs), possibilitando a execução de código não autorizado caso exploradas por invasores. Em vez de acessar estritamente caminhos confiáveis do sistema, esses aplicativos geralmente priorizam o diretório de trabalho atual (CWD) ou outros caminhos predefinidos. Esse comportamento permite que os invasores coloquem DLLs mal-intencionadas no mesmo diretório que o arquivo executável.

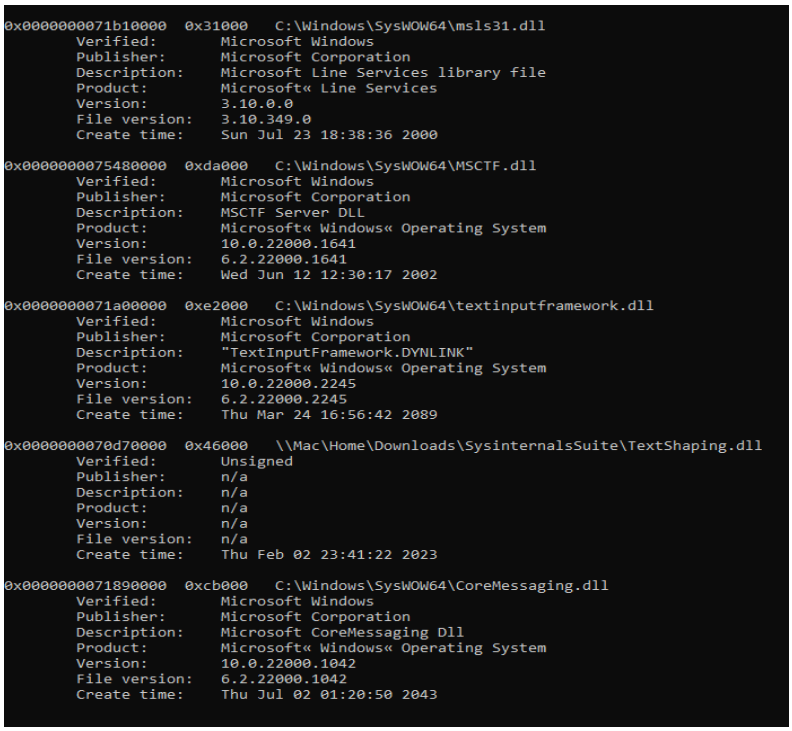

Figura 1 - As DLLs carregadas por um processo podem ser exibidas usando "Listdlls" – Fonte: https://gbhackers.com/zero-day-vulnerabilities-in-microsoft-sysinternals-tools/

Um invasor pode colocar uma DLL maliciosa em um diretório compartilhado de rede, como \\server1\share2\, ao lado de um aplicativo legítimo, como Bginfo.exe. Quando um usuário executa o aplicativo a partir desse diretório, a DLL maliciosa é carregada automaticamente, permitindo a execução do código malicioso no contexto do processo legítimo. Esse vetor de ataque pode levar ao comprometimento completo do sistema, incluindo escalonamento de privilégios e execução de código arbitrário, colocando em risco a integridade e a segurança do ambiente.

Sequência do ataque

O invasor cria uma DLL maliciosa que explora uma vulnerabilidade no aplicativo.cryptbase.dllTextShaping.dll

Essa DLL é copiada para o mesmo diretório que o executável legítimo.

O usuário executa o aplicativo, que carrega a DLL maliciosa em vez da original.

O código da DLL maliciosa é executado com os direitos do usuário.

Colocando a DLL e iniciando o aplicativo no mesmo diretório:

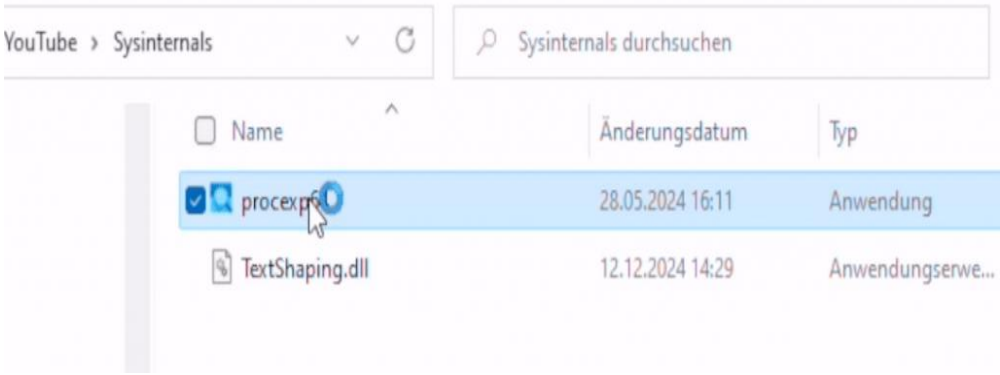

Figura 2 - Diretório Sysinternals, adicionando o DLL – Fonte: https://www.foto-video-it.de/2025/allgemein/disclosure-sysinternals/

O aplicativo é iniciado e a DLL é carregada (função DLL aqui: "Calculadora" foi executada com sucesso – > execução do código foi bem-sucedida):

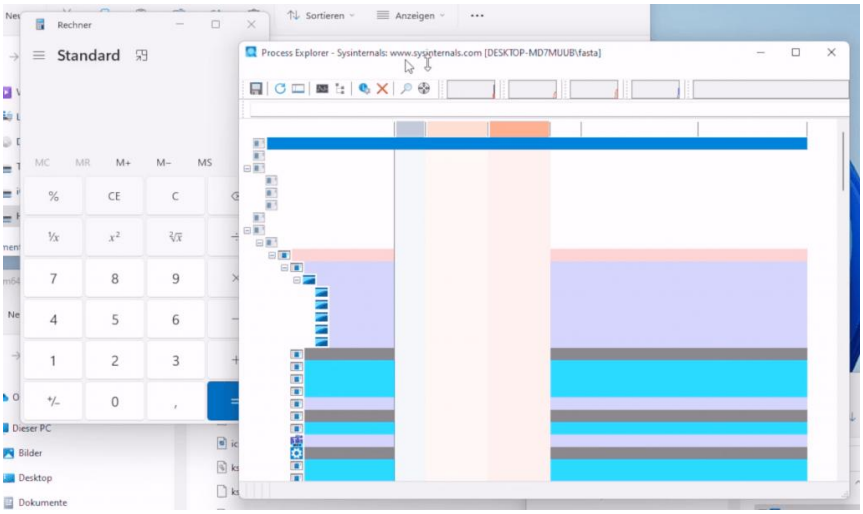

Figura 3 - Código DLL executado com sucesso – Fonte: https://www.foto-video-it.de/2025/allgemein/disclosure-sysinternals/

Mitigação e Prevenção

Apesar das atualizações de algumas ferramentas do Sysinternals em dezembro de 2024, o problema central permanece sem uma solução definitiva. Administradores e usuários devem adotar medidas de mitigação para reduzir a exposição a possíveis ataques:

Evite executar ferramentas diretamente de armazenamento de rede: Sempre copie os executáveis para um diretório local antes da execução.

Verifique a integridade dos aplicativos: Utilize soluções de segurança que garantam que apenas DLLs confiáveis sejam carregadas.

Monitore vulnerabilidades: Realize auditorias regulares nos ambientes para identificar ferramentas afetadas e aplique atualizações assim que disponíveis.

Esta vulnerabilidade destaca os riscos de ferramentas amplamente utilizadas e confiáveis, que, quando mal configuradas, podem se tornar vetores críticos de ataque, embora as ferramentas Sysinternals sejam essenciais para análise de malware e diagnóstico de sistemas, suas falhas agora as tornam alvos viáveis para exploração maliciosa.

Este incidente reforça a importância de práticas rigorosas de codificação segura e validação de caminhos de carregamento de DLLs durante o desenvolvimento de software, com a evolução das técnicas de exploração, as organizações devem adotar uma postura proativa e manter vigilância constante para mitigar riscos e proteger seus sistemas.

Enquanto a Microsoft não fornece uma correção aprofundada, os usuários devem se manter atualizados e seguir as melhores práticas de segurança para mitigar as ameaças emergentes. A vulnerabilidade de dia zero descoberta mostra como é importante não negligenciar a segurança, mesmo com ferramentas confiáveis. As ferramentas do Sysinternals são ferramentas poderosas, mas sua vulnerabilidade a ataques de injeção de DLL as torna um alvo para invasores.

Para ver mais detalhes sobre esta vulnerabilidade você pode acessar os endereços a seguir: https://www.foto-video-it.de/2025/allgemein/disclosure-sysinternals/ e https://gbhackers.com/zero-day-vulnerabilities-in-microsoft-sysinternals-tools/

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: Comitê Editorial de Segurança da Service Sec