TLP: CLEAR

BOLETIM DE SEGURANÇA

Falha em pacote do Node.js expõe sistemas a ataques RCE

heimdall
security research

Acesse a nossa nova comunidade através do WhatsApp!

Heimdall Security Research

Acesse boletins diários sobre agentes de ameaças, *malwares*, indicadores de comprometimentos, TTPs e outras informações no *site* da ISH.

Boletins de Segurança – Heimdall

SUMÁRIO

LISTA DE TABELAS

1 INFORMAÇÕES SOBRE A VULNERABILIDADE

A vulnerabilidade CVE-2024-56334 de injeção de comando foi descoberta no popular pacote **npm systeminformation**, colocando milhões de sistemas em risco de ataques de remote code execution (**RCE**) e privilege escalation. A falha está na função getWindowsIEEE8021x do pacote systeminformation, afetando versões até a **5.23.6**. O problema ocorre devido à falta de higienização adequada do campo SSID do Wi-Fi, que é passado diretamente como parâmetro para o cmd.exe do Windows. Isso permite que invasores injetem comandos maliciosos que podem ser executados pelo sistema operacional.

Segundo relatórios do GitHub, a falha foi identificada na forma como o SSID é obtido e processado. O SSID é recuperado usando o comando netsh wlan show interface e depois passado para **cmd.exe /d /s /c "netsh wlan show profiles"**. Como o campo SSID não é higienizado antes de ser passado para o comando, invasores podem criar nomes SSID maliciosos que executam comandos arbitrários no sistema da vítima.

Status da versão	Versão	Detalhes
Versões afetadas	≤ 5,23,6	Vulnerável à falha de injeção de comando.
Versão corrigida	5.23.7	Vulnerabilidade corrigida; higienização implementada.

Tabela 1 – Versão afetadas e corrigida.

Invasores podem explorar um SSID Wi-Fi malicioso para injetar comandos arbitrários, o que pode resultar em acesso não autorizado a sistemas, roubo de dados sensíveis ou interrupção de operações.

2 RECOMENDAÇÕES

Aplicar patches e atualizações

- Mantenha todos os sistemas e softwares atualizados com os patches de segurança mais recentes fornecidos pelos fabricantes.

Configurar firewalls e sistemas de detecção de intrusão (IDS)

- Utilize firewalls e IDS para monitorar e bloquear atividades suspeitas na rede.

Implementar autenticação multifator (MFA)

- Adote MFA para adicionar uma camada extra de segurança ao processo de login.

Realizar auditorias de segurança regulares

- Conduza auditorias de segurança periódicas para identificar e corrigir vulnerabilidades.

Treinar funcionários em práticas de segurança

- Eduque os funcionários sobre as melhores práticas de segurança, como reconhecer e evitar phishing.

Segregar redes e dados sensíveis

- Separe redes e dados críticos para minimizar o impacto de uma possível violação.

Monitorar logs e atividades

- Mantenha um monitoramento contínuo dos logs e atividades do sistema para detectar comportamentos anômalos.

3 REFERÊNCIAS

- **Heimdall *by* ISH Tecnologia**
- **GBHacker**
- **Github**
- **NVD**

4 AUTORES

- **Leonardo Oliveira Silva**

heimdall
security research
A DIVISION OF ISH