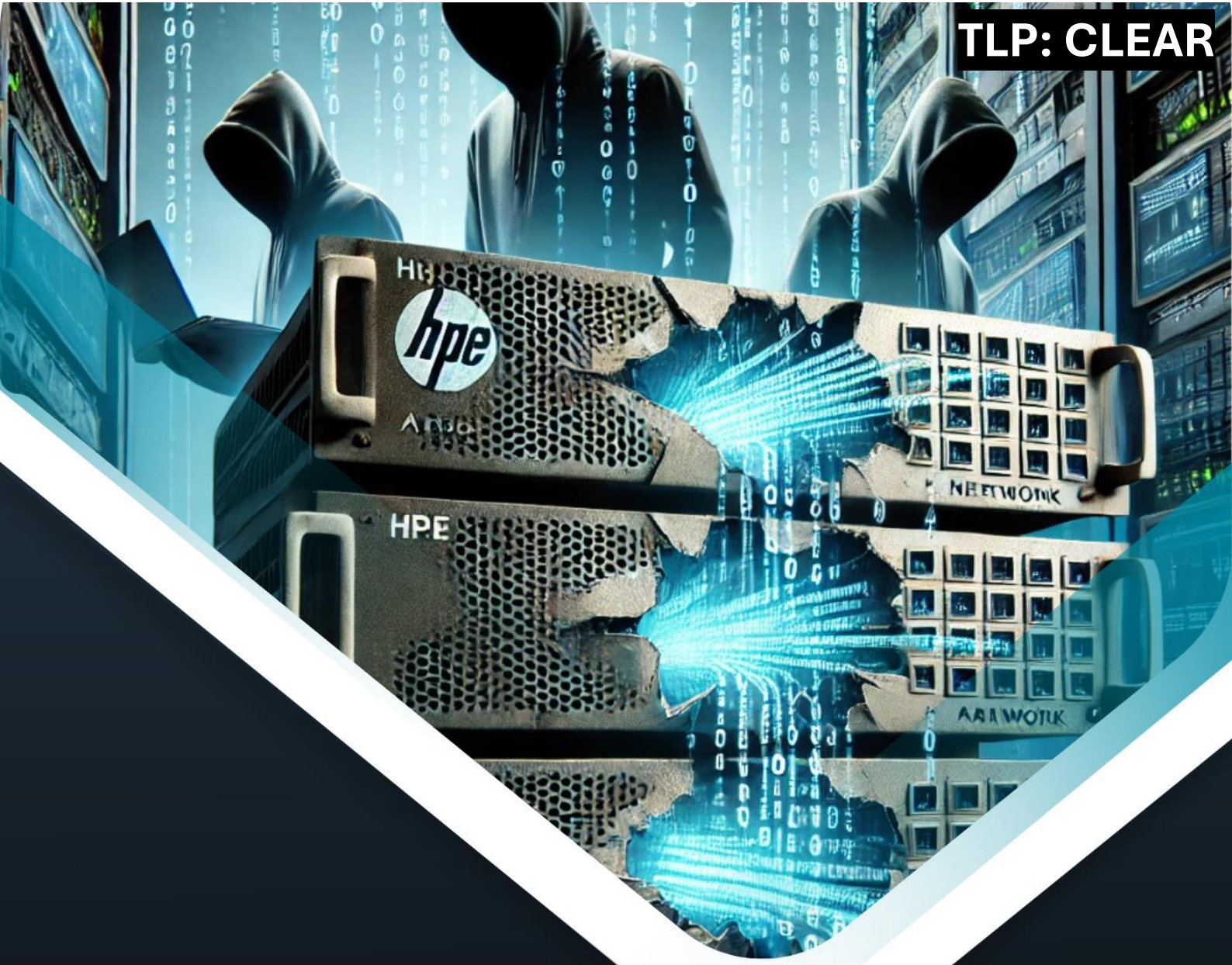
TLP: CLEAR



BOLETIM DE SEGURANÇA

Vulnerabilidades no HPE Aruba Networking permitindo execução remota de código

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

1 INTRODUÇÃO EXECUTIVA

Recentemente, foram identificadas vulnerabilidades nos produtos **HPE Aruba Networking** que podem permitir a execução remota de código arbitrário. Essas falhas, catalogadas como **CVE-2025-23051** e **CVE-2025-23052**, afetam versões específicas dos sistemas operacionais AOS-8 e AOS-10, impactando diretamente os Mobility Conductors, Controllers e Gateways WLAN e SD-WAN gerenciados.

2 INFORMAÇÕES SOBRE AS VULNERABILIDADES

A seguir, são apresentadas as duas vulnerabilidades identificadas e reportadas pela HPE, acompanhadas de uma breve descrição de cada uma. Essas informações visam fornecer um entendimento mais detalhado sobre as possíveis implicações e as ações recomendadas para mitigar os riscos associados.

CVE-2025-23051

- Vulnerabilidade de injeção de parâmetros na interface de gerenciamento web dos sistemas AOS. Um invasor autenticado pode explorar essa falha para sobrescrever arquivos críticos do sistema, levando à potencial execução de código não autorizado.

CVE-2025-23052

- Vulnerabilidade que permite a execução de comandos arbitrários com privilégios elevados através da CLI. Um invasor autenticado pode obter controle não autorizado sobre funções críticas do sistema.

2.1 SISTEMAS E PRODUTOS AFETADOS

As seguintes versões dos sistemas operacionais são afetadas:

- *AOS-10.4.x.x*: versões *10.4.1.4* e anteriores.
- *AOS-8.12.x.x*: versões *8.12.0.2* e anteriores.
- *AOS-8.10.x.x*: versões *8.10.0.14* e anteriores.

Além disso, versões mais antigas que já atingiram o fim do suporte também estão vulneráveis, incluindo todas as versões de *AOS-10.6.x.x*, *AOS-10.5.x.x* e várias versões de *AOS-8.9.x.x* e anteriores.

2.2 IMPACTO DA VULNERABILIDADE

A exploração dessas vulnerabilidades pode resultar em:

- Comprometimento total da infraestrutura de rede afetada.
- Execução de código não autorizado com privilégios elevados.
- Sobrescrita de arquivos críticos do sistema, potencialmente causando interrupções significativas nos serviços de rede.

3 RECOMENDAÇÕES

Para mitigar os riscos associados a essas vulnerabilidades, é altamente recomendável que os administradores de rede:

Atualizem os sistemas operacionais para as versões corrigidas

- *AOS-10.7.x.x*: versão *10.7.0.0* ou superior.
- *AOS-10.4.x.x*: versão *10.4.1.5* ou superior.
- *AOS-8.12.x.x*: versão *8.12.0.3* ou superior.
- *AOS-8.10.x.x*: versão *8.10.0.15* ou superior.

Implementem controles de acesso rigorosos

- Isolando as interfaces de gerenciamento CLI e web em uma VLAN dedicada ou segmento.
- Aplicando políticas de firewall robustas nas camadas 3 e superiores para restringir o acesso não autorizado.

4 REFERÊNCIAS

- **Heimdall *by* ISH Tecnologia**
- **HPE**
- **NVD**
- **GBHackers**

5 AUTORES

- **Rafael Salomé**

heimdall
security research
A DIVISION OF ISH