BOLETIM DE SEGURANÇA

Aruba lança atualizações de segurança para solucionar falhas críticas no ArubaOS

heimdall
security research
A DIVISION OF ISH

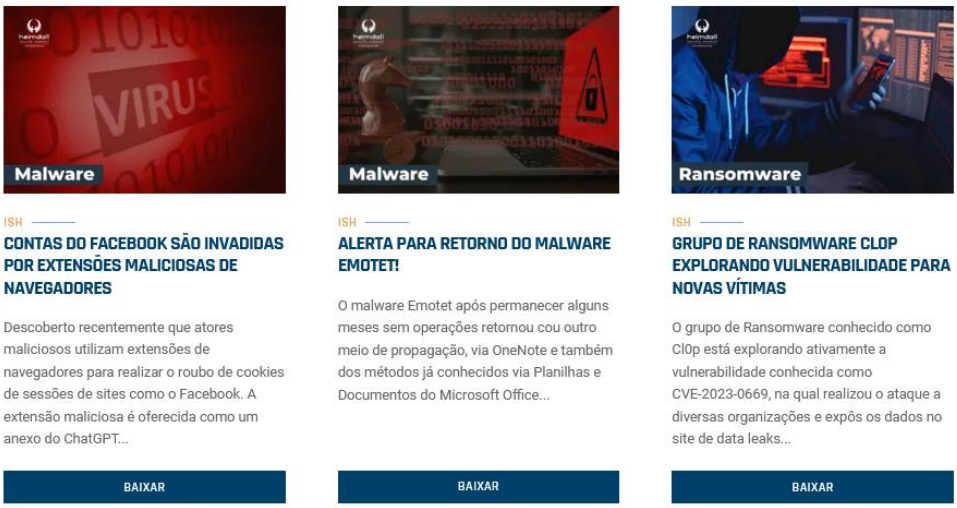
TLP: CLEAR

Receba alertas e informações sobre segurança cibernética e ameaças rapidamente, por meio do nosso **X**.

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 SUMÁRIO EXECUTIVO

A HPE Aruba Networking, divulgou recentemente atualizações de segurança que visam corrigir as vulnerabilidades CVE-2024-26304, CVE-2024-26305, CVE-2024-33511, CVE-2024-33512 classificadas como críticas presentes no ArubaOS, as quais, se exploradas, poderiam permitir a execução remota de código nos sistemas comprometidos.

2 DETALHES SOBRE AS VULNERABILIDADES

A Vulnerabilidade CVE-2024-26304 trata-se de um buffer overflow não autenticado no Serviço de gerenciamento L2/L3 acessado por meio do protocolo PAPI. Esse serviço pode levar a execução de código remoto não autenticado enviando pacotes especialmente criados destinados a porta 8211 UDP do protocolo PAPI. A exploração bem-sucedida desta vulnerabilidade resulta na capacidade de executar código arbitrário como um usuário privilegiado no sistema operacional subjacente.

A Vulnerabilidade CVE-2024-26305 refere-se de um buffer overflow não autenticado no Daemon acessado através do protocolo PAPI. Essa vulnerabilidade pode levar à execução remota de código não autenticado, enviando pacotes especialmente criados destinados a porta 8211 UDP do protocolo PAPI. Com a exploração bem-sucedida resulta na capacidade de executar código arbitrário como um usuário privilegiado no subjacente sistema operacional.

A Vulnerabilidade CVE-2024-33511, também é um buffer overflow não autenticado no serviço de relatório automático acessado por meio do protocolo PAPI. Essa vulnerabilidade pode levar a informações não autenticadas e na execução remota de código enviando pacotes especialmente criados destinados a porta 8211 UDP do protocolo PAPI. A exploração bem-sucedida desta vulnerabilidade resulta na capacidade de executar código arbitrário como um usuário privilegiado no sistema operacional subjacente.

A Vulnerabilidade CVE-2024-33512, se refere a um buffer overflow não autenticado no banco de dados de autenticação de usuário local acessado por meio do protocolo PAPI. Essa vulnerabilidade no serviço de banco de dados de autenticação de usuário local que pode levar a execução remota de código não autenticado, enviando códigos especialmente criados e enviar pacotes destinados a porta 8211 UDP do protocolo PAPI. A exploração bem-sucedida desta vulnerabilidade resulta na capacidade de executar código arbitrário como um usuário privilegiado no sistema operacional subjacente.

Produtos afetados	Versões de software afetadas	Versões em fim de manutenção
HPE Aruba Networking: MobilityConductor MobilityControllers WLANGatewaysandSD-WANGatewaysmanagedbyArubaCentral	ArubaOS10.5.x.x:10.5.1.0andbelow ArubaOS10.4.x.x:10.4.1.0andbelow ArubaOS8.11.x.x:8.11.2.1andbelow ArubaOS8.10.x.x:8.10.0.10andbelow	ArubaOS10.3.x.x:all ArubaOS8.9.x.x:all ArubaOS8.8.x.x:all ArubaOS8.7.x.x:all ArubaOS8.6.x.x:all ArubaOS6.5.4.x:all SD-WAN8.7.0.0-2.3.0.x:all SD-WAN8.6.0.4-2.2.x.x:all

Tabela 1 – Tabela de produtos e versões.

3 RECOMENDAÇÕES

A Aruba recomenda que você corrija cada uma das aplicações afetadas para uma das versões mais recente.

Atualização de software

- Verifique se há atualizações de segurança disponíveis para os sistemas afetados e aplique-as imediatamente.

Bloqueio de portas

- Considere bloquear o tráfego da porta 8211/UDP que é usada pelo protocolo PAPI (Aruba's access point management protocol), que é o vetor de ataque para essas vulnerabilidades.

Firewalls e anti-malware

- Utilize ativos de segurança, como firewalls e anti-malware, mantendo-os sempre atualizados para proteção contra ameaças.

Política de mínimo privilégio

- Implemente uma política de mínimo privilégio, permitindo aos usuários exercerem ações na rede restritas ao desempenho de suas funções organizacionais.

Monitoramento e detecção

- Monitore os sistemas para detectar atividades suspeitas e implemente sistemas de detecção de intrusão para identificar tentativas de exploração dessas vulnerabilidades.

Educação de usuários

- Oriente os usuários sobre práticas seguras de navegação e conscientize-os sobre os riscos associados a essas vulnerabilidades.

4 REFERÊNCIAS

- **Heimdall *by* ISH Tecnologia**
- Aruba_Networks
- Thehackernews

heimdall
security research
A DIVISION OF ISH