مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

RADIUS Protocol Vulnerability in HP Products

Tracking #:432316777

Date:23-01-2025

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a critical vulnerability has been identified in the RADIUS protocol, which is used for device and user authentication. This vulnerability allows attackers to bypass authentication and gain unauthorized access to sensitive network resources.

TECHNICAL DETAILS:

A critical vulnerability has been identified in the RADIUS protocol, which is used for device and user authentication. The attack targets the Response Authenticator in the RADIUS/UDP protocol, specifically exploiting a forgery vulnerability against RFC 2865. The RADIUS protocol forgery attack (CVE-2024-3596) allows attackers to exploit the MD5 chosen-prefix collision vulnerability, giving them the ability to forge valid responses and bypass authentication mechanisms.

- CVE ID:**CVE-2024-3596**
- CVSS Score: 9.0 (Critical)
- Attack Vector: Network
- Attack Complexity: High (requires man-in-the-middle access)
- Privileges Required: None (no prior authentication needed)

Attack Method:

- A man-in-the-middle attacker can forge a valid Access-Accept response to a client's Access-Request that was initially rejected by the RADIUS server.
- By manipulating the MD5 hash and crafting a collision between an Access-Reject message and the forged Access-Accept message, attackers can gain unauthorized network access.
- The attack requires the attacker to be between the RADIUS client and server and to trigger an Access-Request from the client.

Affected Products:

The vulnerability impacts several HPE Aruba Networking products across multiple platforms and software releases:

- EdgeConnect SD-WAN Gateways: All supported software releases
- EdgeConnect SD-WAN Orchestrators: All supported software releases
- Switches running AOS-CX: All supported software releases
- WLAN Gateways and SD-WAN Gateways running AOS-10:
  - AOS-10.6.0.2 and below
  - AOS-10.4.1.3 and below
- Mobility Controllers running AOS-8:
  - AOS-8.12.0.1 and below
  - AOS-8.10.0.13 and below
- Access Points running Instant AOS-8 and AOS-10: All supported software releases
- AirWave Management Platform: 8.3.0.2 and below
- ClearPass Policy Manager: 6.12.1 and below, 6.11.8 and below
- Aruba Fabric Composer: 7.1.0 and below
- Networking Instant On: Switches (1930, 1960) and Access Points with firmware versions ≤ 3.0.0.0 in local mode.

Fixed Versions:
HPE has released patches for some affected products to fix this vulnerability:

- AirWave Management Platform: Version 8.3.0.3 and above
- ClearPass Policy Manager: Versions 6.12.2 and above, 6.11.9 and above
- Switches running AOS-CX: Versions 10.14.1010 and above, 10.13.1040 and above
- WLAN Gateways and SD-WAN Gateways running AOS-10: Version AOS-10.6.0.3 and above
- Mobility Controllers running AOS-8: Versions AOS-8.12.0.2 and above, AOS-8.10.0.14 and above
- EdgeConnect SD-WAN Orchestrator: Refer to official documentation.

Mitigation Recommendations
HPE advises immediate action to mitigate this vulnerability. Recommended steps include:

- Use of EAP-TLS or RadSec:
  - For both RADIUS clients and servers, use EAP-TLS or RadSec for a more secure version of the protocol.
  - These methods help ensure that RADIUS communications are protected against such forgery attacks.
- Message-Authenticator Configuration:
  - Ensure that Message-Authenticator is enabled in ClearPass Policy Manager. This adds additional protection to prevent unauthorized message modification.
  - Steps to enable Message-Authenticator:
  - Go to Administration > Server Manager > Server Configuration in ClearPass.
  - Enable Message-Authenticator from the Service Parameters tab.
- Network Isolation and Secure VPN Tunnel:
  - If upgrades are not possible, ensure network isolation for RADIUS communication and use secure VPN tunnels to restrict access to these services from untrusted sources.

RECOMMENDATIONS:

The UAE Cyber Security Council recommends customers using affected products should upgrade their systems to secure versions to resolve the vulnerability.

Kindly circulate this information to your subsidiaries and partners as well as share with us any relevant information and findings.

The UAE Cyber Security Council extends its appreciation for the continued collaboration.

REFERENCES:

- https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbnw04662en_us&docLocale=en_US#dceContent