July 30, 2024

# Overall Rating: Critical

BRITISH COLUMBIA

**This is a technical bulletin intended for technical audiences.**

## Summary

The Vulnerability and Risk Management (VRM) Team is aware of HPE published a security advisory to address vulnerabilities in the following products:

- ClearPass Policy Manager 6.12.x – version 6.12.1 and prior
- ClearPass Policy Manager 6.11.x – version 6.11.8 and prior

**Technical Details**

A forgery attack has been discovered against the Response Authenticator in RADIUS/UDP, specifically targeting RFC 2865. This attack allows a man-in-the-middle to forge a valid Access-Accept response to a client request that was initially rejected by the RADIUS server, thereby granting unauthorized network access. The vulnerability exploits a chosen-prefix collision attack on MD5, manipulating the first byte and packet attributes of Access-Reject messages to match the Response Authenticator of a forged Access-Accept message. The attack requires appending a minimal amount of collision block gibberish to the Access-Request, which is then encapsulated in Proxy-State attributes and processed by the server, ensuring the computed Response Authenticator matches for both the legitimate Access-Reject and the forged Access-Accept.

This vulnerability is rated as a **CRITICAL** risk. Software updates exist to address these risks.

## Action Required

- Locate the device or application and investigate.
- Notify business owner(s).
- Perform mitigating actions, as required.

Please notify VRM with any questions or concerns you may have at vulnerabilityandriskmanagement@gov.bc.ca

**References**

- CVE-2024-3596 CVE-2024-41915 CVE-2024-41916 CVE-2024-5486
- HPE Security Bulletin - hpesbnw04675en_us
- HPE Security Bulletin Library