August 15, 2024

Overall Rating: High

This is a technical bulletin intended for technical audiences.

Summary

The Vulnerability and Risk Management (VRM) Team has been made aware of a vulnerability in the RADIUS protocol allows an attacker allows an attacker to forge an authentication response in cases where a Message-Authenticator attribute is not required or enforced. This vulnerability results from a cryptographically insecure integrity check when validating authentication responses from a RADIUS server.

Technical Details

A vulnerability in the verification of RADIUS Response from a RADIUS server has been disclosed. An attacker, with access to the network where the RADIUS protocol is being transmitted, can spoof a UDP-based RADIUS Response packet to modify any valid Response (Access-Accept, Access-Reject, or Access-Challenge) to any other response, with almost any content, completely under the attacker's control. This allows the attacker to transform a Reject into an Accept without knowledge of the shared secret between the RADIUS client and server. The attack is possible due to a basic flaw in the RADIUS protocol specification that uses a MD5 hash to verify the response, along with the fact that part of the hashed text is predictable allowing for a chosen-prefix collision. The widespread use of RADIUS and its adoption into the cloud allows for such attacks to pose a reasonable threat to the authentication verification process that relies on RADIUS.

RADIUS servers that only perform Extensible Authentication Protocol (EAP), as specified in RFC 3579, are unaffected by this attack. The EAP authentication messages require the Message-Authenticator attribute, which will prevent these attacks from succeeding. The use of TLS (or DTLS) encryption can also prevent such attacks from succeeding. However, RADIUS over TCP itself can still be susceptible to this attack, with more advanced man-in-the-middle scenarios, to successfully attack the TCP connection.

Network operators who rely on the RADIUS-based protocol for device and/or user authentication should update their software and configuration to a secure form of the protocol for both clients and servers. This can be done by enforcing TLS or DTLS encryption to secure the communications between the RADIUS client and server. Where possible, network isolation and secure VPN tunnel communications should be enforced for the RADIUS protocol to restrict access to these network resources from untrusted sources.

This vulnerability is rated as a **HIGH** risk. A software update exists to address this risk.

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
- RADIUS protocol susceptible to forgery attacks
- VRM Vulnerability Reports