CIRT.GY Guyana National Computer Incident Response Team

AL2024_19 RADIUS protocol susceptible to forgery attacks (18th July 2024)

Summary

On the 7th of July 2024, security researchers disclosed a spoofing vulnerability affecting the RADIUS protocol utilized by multiple vendor clients and servers.

Details

RADIUS is a widely used, lightweight authentication protocol for networking devices, used for authentication of both users and devices. RADIUS supports a broad range of networking devices, from basic network switches to advanced VPN solutions. As of recent, RADIUS has been adopted in many cloud services to provide tiered, role-based access control to resources. As a client-server protocol, RADIUS employs a Request-Response model to verify authentication requests and manage role-based access using Group

A team of researchers from UC San Diego and their partners have disclosed a vulnerability in the verification of RADIUS Responses from a RADIUS server. An attacker with access to the network where the RADIUS protocol is being transmitted can spoof a UDP-based RADIUS Response packet, altering any valid Response (Access-Accept, Access-Reject, or Access-Challenge) to any other response with nearly any content, completely under the attacker's control. This enables the attacker to convert a Reject into an Accept without knowing the shared secret between the RADIUS client and server. This vulnerability arises from a fundamental flaw in the RADIUS protocol specification, which uses an MD5 hash to verify the response, along with the predictability of part of the hashed text, allowing for a chosen-prefix collision. The vulnerability is currently being tracked as CVE-2024-3596.

The widespread use of RADIUS, especially in the cloud, makes such attacks a significant threat to the authentication verification process that relies on RADIUS. However, RADIUS servers that solely perform Extensible Authentication Protocol (EAP) are not affected by this attack. EAP authentication messages require the Message-Authenticator attribute, which prevents these attacks from succeeding. Additionally, using TLS (or DTLS) encryption can prevent such attacks. Nevertheless, RADIUS over TCP can still be vulnerable to this attack in more advanced man-in-the-middle scenarios that target the TCP connection.

Affected Products

Various network and security companies are currently investigating their product line to determine the products and services affected by this vulnerability. At the time of this article, there are 17 confirmed affected vendors including Microsoft, RedHat and Juniper Network among others. For an update on the affected vendors, please see the following URL:

https://www.kb.cert.org/vuls/id/456537#vendor-information

Remediation

Network operators using the RADIUS protocol for device and user authentication should update their software and configurations to a more secure version of the protocol for both clients and servers. This can be achieved by enforcing TLS or DTLS encryption to secure communications between the RADIUS client and server. Additionally, network isolation and secure VPN tunnel communications should be implemented wherever possible to restrict access to RADIUS resources from untrusted sources.

The Guyana National CIRT recommends that users and administrators review this alert and apply it where necessary.

References

- CERT/CC Vulnerability Note VU#456537. (2024, July 9). https://www.kb.cert.org/vuls/id/456537
- RADIUS Protocol Spoofing Vulnerability (Blast-RADIUS): July 2024. (2024, July 17). https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-radius-spoofing-july-2024-87cCDwZ3