Security Advisory 2024-074

RADIUS Vulnerability Impacts Cisco Products

July 29, 2024 — v1.0

TLP:CLEAR

History:

- *29/07/2024 — v1.0 – Initial publication*

Summary

A critical vulnerability, identified as CVE-2024-3596, has been discovered in the RADIUS (Remote Authentication Dial-In User Service) protocol, allowing for man-in-the-middle (MitM) attacks that bypass authentication mechanisms [1]. Dubbed the *Blast-RADIUS* attack, this vulnerability leverages an MD5 collision attack to forge authentication responses, potentially granting unauthorised access to network resources.

In particular multiple CISCO products are impacted by this vulnerability [2, 3]. Other platforms are impacted as well, although the exact severity varies [4, 5] Due to the high severity of this vulnerability, CERT-EU strongly recommends patching as soon as possible.

Technical Details

The Blast-RADIUS attack targets the RADIUS/UDP protocol, which is widely used for authentication in various network services. The vulnerability arises from the use of MD5 in the RADIUS protocol's Response Authenticator. An attacker can exploit this by intercepting and modifying RADIUS messages between the client and server.

This process can be completed in 3 to 6 minutes, though advanced hardware could significantly reduce this time, making the attack feasible within the typical RADIUS timeout period of 30 to 60 seconds.

Affected Products

The vulnerability impacts any system utilising RADIUS/UDP for authentication without the Message-Authenticator attribute enabled. This includes a wide range of network devices and services.

The list of impacted Cisco products is available in [2]. Other vendors are also impacted, including WatchGuard [4], Palo-Alto [5], or Microsoft [6], and many others.

Recommendations

To mitigate the risk of exploitation, the following measures are recommended:

- **Enable Message-Authenticator Attribute**: Ensure that all RADIUS communications include the Message-Authenticator attribute, which uses HMAC-MD5 to provide stronger protection against MitM attacks.
- **Update RADIUS Implementations**: Apply patches and updates provided by RADIUS software vendors that address this vulnerability.

References

[1] https://www.bleepingcomputer.com/news/security/new-blast-radius-attack-bypasses-widely-used-radius-authentication/

[2] https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-radius-spoofing-july-2024-87cCDwZ3

[3] https://cybersecuritynews.com/radius-protocol-vulnerability-cisco/

[4] https://www.watchguard.com/wgrd-psirt/advisory/wgsa-2024-00013

[5] https://security.paloaltonetworks.com/CVE-2024-3596

[6] https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2024-3596