RADIUS Protocol Spoofing Vulnerability (Blast-RADIUS): July 2024

Summary

On July 7, 2024, security researchers disclosed the following vulnerability in the RADIUS protocol and assigned a CVSS base score of 8.1, CVE-2024-3596. This vulnerability may impact any RADIUS client and server. For a full description and list of affected Cisco products, please see the Cisco Security Advisory here.

CVE-2024-3596: RADIUS Protocol under RFC 2865 is susceptible to forgery attacks by an on-path attacker who can modify any valid Response (Access-Accept, Access-Reject, or Access-Challenge) to any other response using a chosen-prefix collision attack against MD5 Response Authenticator signature.

The Cisco Security Advisory was first published on July 10. This article will focus on the impact on Meraki products.

Vulnerability Information

An attacker with access to the network segment where the RADIUS protocol messages are 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 an MD5 hash to verify the response.

Scope

Affected Cisco Meraki Products:

Product	Details
Meraki Splash Service when using customer hosted RADIUS	The connection between Meraki's Splash service and the customer's RADIUS server IS VULNERAB PAP and also does not require Message-Authenticator attributes to be used.
MX	**Features:** Anyconnect Client VPN, L2TP Client VPN • **Not Vulnerable:** Communication between the client and the MX is protected in an IPSec Tunnel • **Vulnerable**: Communication between the MX and the RADIUS server. The MX uses PAP and d message-authenticator attribute.

Impact

The bug described by CVE-2024-3596 could allow a malicious party sitting on the network path between the customer-owned RADIUS Server and the Splash service could have an attacker gain access to the network without possessing valid authentication credentials, and the same is true between the MX device and the customer-owned RADIUS server. An unauthorized attacker could gain access to a protected network for their clients and devices.

Fix Information

Please see the table below for fix information for each affected product:

Product Line	Fixed Releases
Meraki Splash Service when using customer hosted RADIUS	Firmware upgrade is not required to support Message-Authenticator attribute. Fix not deployed as of July 30, 2024
MX	Firmware upgrade required to support Message-Authenticator attribute for Client VPN. Fixed Versions: • TBD. Not Available as of July 30, 2024

Note: This section will be updated with additional fix information when it becomes available.

Mitigation

To mitigate this issue it is important to use the **message authenticator** RADIUS attribute and secure the network path between the Authenticator (e.g. MX) and the RADIUS Server. Potential mitigation steps will vary depending on the network path between the Authenticator and RADIUS Server.

Customers should determine the applicability and effectiveness of this mitigation in their own environment and under their own use conditions. Customers should be aware that any workaround or mitigation that is implemented may negatively impact the functionality or performance of their network based on intrinsic customer deployment scenarios and limitations. Customers should not deploy any workarounds or mitigations before first evaluating the applicability to their own environment and any impact to such environment.

Secure Practice Examples

- If the RADIUS Server is on the same LAN as the Authenticator, implementing secure network practices such as port authentication, VLANs that separate users from management traffic, Firewall rules that restrict user traffic, and other secure practices can help reduce the attack surface on the LAN.
- If the RADIUS Server is remote from the Authenticator, implementing secure technologies like VPN encryption between the Authenticator and RADIUS Server can help prevent attacks by an on-path attacker

FAQ

Is Cisco Meraki aware of any exploitation or public discussion of this vulnerability?

Cisco Meraki PSIRT is aware that public proof-of-concept code is available, but is not aware of any malicious use of the vulnerability that is described in this

advisory.

How was this vulnerability found?

A vulnerability in the verification of RADIUS Response from a RADIUS server has been disclosed by a team of researchers from UC San Diego and their partners.

How complex is it to execute this exploit?

The Common Vulnerability Scoring System (CVSS) base score for this vulnerability has an attack complexity of High. It is important to note that it is not possible to exploit this vulnerability from a fully remote location; a malicious attacker would need to place their device within the network path of a RADIUS Server and Authenticator to exploit this vulnerability.

How can I upgrade my firmware to a fixed release?

Customers can use the Firmware Upgrade Tool to schedule firmware upgrades. We have a document detailing the steps here.

Are there any devices that will not have the fix available?

All currently supported Cisco Meraki devices will receive the firmware when the fix is available.

Are Radius Proxy workflows impacted?

No, this service uses EAP between Meraki nodes and the Meraki Cloud and is not vulnerable.

Are networks using Meraki authentication impacted?
No, this is an encrypted tunnel to the Meraki Cloud and is not vulnerable.