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 security researchers disclosed vulnerability in the RADIUS protocol. This vulnerability may impact any RADIUS client and server.

Technical Details

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.

Product	Cisco Bug ID
Endpoint Clients and Client Software	
Duo Authentication Proxy	CSCwk87884
Network and Content Security Devices	
Adaptive Security Appliance (ASA)	CSCwk71992
Firepower Device Manager (FDM)	CSCwk69454
Firepower Management Center (FMC) Software	CSCwk71817
Firepower Threat Defense (FTD) Software	CSCwk67902
Meraki MX Series	Notes
Identity Services Engine (ISE)	CSCwk67747
Secure Email Gateway	CSCwk70832
Secure Email and Web Manager	CSCwk70833
Secure Firewall	CSCwk67859
Secure Network Analytics	CSCwk73619
Secure Web Appliance	CSCwk70834
Network Management and Provisioning	
Application Policy Infrastructure Controller (APIC)	CSCwk70836
Crosswork Network Controller	CSCwk70850
Nexus Dashboard, formerly Application Services Engine	CSCwk70840
Prime Infrastructure	CSCwk79727
Routing and Switching - Enterprise and Service Provider	
ASR 5000 Series Routers	CSCwk70831
Catalyst Center	CSCwk70845
Catalyst SD-WAN Controller, formerly SD-WAN vSmart	CSCwk70854
Catalyst SD-WAN Manager, formerly SD-WAN vManage	CSCwk70854
Catalyst SD-WAN Validator, formerly SD-WAN vBond	CSCwk70854
GGSN Gateway GPRS Support Node	CSCwk70831
IOS Software	CSCwk78278
IOS XE Software	CSCwk70852
IOS XR Software	CSCwk70236

IOx Fog Director	CSCwk70851
MDS 9000 Series Multilayer Switches	CSCwk70837
Nexus 1000V Series Switches	CSCwk79691
Nexus 3000 Series Switches	CSCwk70839
Nexus 5500 Platform Switches	CSCwk79692
Nexus 5600 Platform Switches	CSCwk79692
Nexus 6000 Series Switches	CSCwk79692
Nexus 7000 Series Switches	CSCwk70838
Nexus 9000 Series Fabric Switches in ACI Mode	CSCwk83051
Nexus 9000 Series Switches in standalone NX-OS mode	CSCwk70839
PGW Packet Data Network Gateway	CSCwk70831
SD-WAN vEdge Routers	CSCwk70854
System Architecture Evolution (SAE) Gateway	CSCwk70831
Ultra Packet Core	CSCwk70831
Unified Computing	
Enterprise NFV Infrastructure Software (NFVIS)	CSCwk79647
UCS Central Software	CSCwk71967
UCS Manager	CSCwk70842
WirelessUnified Computing	
AireOS Wireless LAN Controllers	CSCwk70846

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
- CISCO - RADIUS Protocol Spoofing Vulnerability (Blast-RADIUS): July 2024
- VRM Vulnerability Reports