Advisory Alert

Alert Number: AAA20250123 **Date:** January 23, 2025

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
HPE	**Critical**	RADIUS Protocol Vulnerability
Cisco	**Critical**	Privilege Escalation Vulnerability
Cisco	**High**, **Medium**	Multiple Vulnerabilities
FortiGuard	**Medium**	An allocation of resources without limits or throttling Vulnerability

Description

Affected Product	**HPE**
Severity	**Critical**
Affected Vulnerability	RADIUS Protocol Vulnerability (CVE-2024-3596)
Description	HPE has released security updates to address a RADIUS Protocol Authentication Bypass Vulnerability affecting HPE Aruba Networking Products. **CVE-2024-3596 -** A forgery attack has been discovered against the Response Authenticator in RADIUS/UDP, specifically targeting RFC 2865. This attack allows a man-in-the-middle to forge a valid Access-Accept response to a client request that was initially rejected by the RADIUS server, thereby granting unauthorized network access. HPE advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Multiple Products
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbnw04662en_us&docLocale=en_US

Affected Product	**Cisco**
Severity	**Critical**
Affected Vulnerability	Privilege Escalation Vulnerability (CVE-2025-20156)
Description	Cisco has released security update addressing a Privilege Escalation Vulnerability affecting Cisco Meeting Management **CVE-2025-20156-** A vulnerability in the REST API of Cisco Meeting Management, caused by improper enforcement of authorization for REST API users, could allow a remote, authenticated attacker with low privileges to elevate their privileges to administrator on an affected device by sending specially crafted API requests to a specific endpoint. A successful exploit could grant the attacker administrator-level control over edge nodes managed by Cisco Meeting Management. Cisco advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Cisco Meeting Management 3.8 and earlier Cisco Meeting Management 3.9
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cmm-privesc-uy2Vf8pc

Affected Product	**Cisco**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-20165, CVE-2025-20128)
Description	Cisco has released security updates to address multiple vulnerabilities in their products. **CVE-2025-20165 -** A vulnerability in the SIP processing subsystem of Cisco BroadWorks, caused by improper memory handling for certain SIP requests, could allow an unauthenticated, remote attacker to halt the processing of incoming SIP requests and create a denial of service (DoS) condition. By sending a high volume of SIP requests to an affected system, an attacker could exploit this vulnerability to exhaust the memory allocated to the Cisco BroadWorks Network Servers handling SIP traffic. Once the memory is fully consumed, the Network Servers would be unable to process incoming requests, leading to a DoS condition that requires manual intervention to restore functionality. **CVE-2025-20128** - A vulnerability in the Object Linking and Embedding 2 (OLE2) decryption routine of ClamAV, caused by an integer underflow in a bounds check leading to a heap buffer overflow read, could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. An attacker could exploit this vulnerability by submitting a crafted file containing OLE2 content for scanning by ClamAV. A successful exploit could terminate the ClamAV scanning process, resulting in a DoS condition on the affected software. Cisco advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	• Cisco BroadWorks Release Independent (RI) before RI.2024.11 • Secure Endpoint Connector for Linux version before 1.25.1 • Secure Endpoint Connector for Mac version before 1.24.4 • Secure Endpoint Connector for Windows version before 7.5.20 / 8.4.3 • Secure Endpoint Private Cloud version before 4.2.0
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-bw-sip-dos-mSySbrmt • https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-clamav-ole2-H549rphA

Affected Product	**FortiGuard**
Severity	**Medium**
Affected Vulnerability	An allocation of resources without limits or throttling Vulnerability (CVE-2024-46666)
Description	FortiGuard has released a security update to address an Allocation of Resources Without Limits or Throttling vulnerability in FortiOS. This vulnerability could allow a remote, unauthenticated attacker to disrupt access to the GUI by sending specially crafted requests to specific endpoints. FortiGuard advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	• FortiOS 7.6.0 • FortiOS 7.4.0 through 7.4.4 • FortiOS 7.2 all versions • FortiOS 7.0 all versions • FortiOS 6.4 all versions
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.fortiguard.com/psirt/FG-IR-24-250

Disclaimer

The information provided are gathered from official service provider's websites and portals. FinCSIRT strongly recommends members to apply security fixes as per the given guidelines, following the organization's patch and change management procedures to protect systems from potential threats.