Advisory Alert

Alert Number: AAA20250609 **Date:** June 9, 2025

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Cisco	**Critical**	Multiple Vulnerabilities
QNAP	**High**, Medium	Multiple Vulnerabilities

Description

Affected Product	**Cisco**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-32433, CVE-2025-20188)
Description	Cisco has released security updates addressing multiple vulnerabilities that exist in their products. **CVE-2025-32433** - Vulnerability in Erlang/OTP SSH server that may allow an attacker to perform unauthenticated remote code execution. By exploiting a flaw in SSH protocol message handling, a malicious actor could gain unauthorized access to affected systems and execute arbitrary commands without valid credentials. **CVE-2025-20188** - This vulnerability is due to the presence of a hard-coded JSON Web Token (JWT) on an affected system. An attacker could exploit this vulnerability by sending crafted HTTPS requests to the AP file upload interface. A successful exploit could allow the attacker to upload files, perform path traversal, and execute arbitrary commands with root privileges. Cisco advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Cisco Network Application, Service, and Acceleration • ConfD, ConfD Basic - Versions prior to 7.7.19.1, 8.0.17.1, 8.1.16.2, 8.2.11.1, 8.3.8.1, 8.4.4.1 Cisco Network Management and Provisioning • Network Services Orchestrator (NSO) - Versions prior to 5.7.19.1, 6.1.16.2, 6.2.11.1, 6.3.8.1, 6.4.1.1, 6.4.4.1 Cisco products if they are running a release of Cisco IOS XE Software for WLCs, • Catalyst 9800-CL Wireless Controllers for Cloud • Catalyst 9800 Embedded Wireless Controller for Catalyst 9300, 9400, and 9500 Series Switches • Catalyst 9800 Series Wireless Controllers • Embedded Wireless Controller on Catalyst APs
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-erlang-otp-ssh-xyZZy • https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-wlc-file-uplpd-rHZG9UfC

Affected Product	**QNAP**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-22484, CVE-2025-22490, CVE-2025-29871, CVE-2025-29872, CVE-2025-29873, CVE-2025-29876, CVE-2025-29877, CVE-2025-33035, CVE-2025-30279, CVE-2025-33031, CVE-2025-22481, CVE-2024-56805, CVE-2024-6387, CVE-2024-13087, CVE-2024-13088, CVE-2024-50406, CVE-2025-22482, CVE-2025-29892, CVE-2025-22486, CVE-2025-29883, CVE-2025-29884, CVE-2025-29885, CVE-2025-26465, CVE-2025-26466, CVE-2023-28370)
Description	QNAP has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to cause denial-of-service, NULL pointer dereference, out-of-bounds read, command injection, buffer overflow. QNAP advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	QNAP QuTS hero h5.2.x QNAP QuRouter 2.4.x and 2.5.x QNAP QTS 5.2.x QNAP Qsync Central 4.5.x QNAP QES 2.2.0 QNAP License Center 1.9.x QNAP File Station 5 version 5.5.x
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.qnap.com/en/security-advisory/qsa-25-16 • https://www.qnap.com/en/security-advisory/qsa-25-15 • https://www.qnap.com/en/security-advisory/qsa-25-13 • https://www.qnap.com/en/security-advisory/qsa-25-12 • https://www.qnap.com/en/security-advisory/qsa-25-11 • https://www.qnap.com/en/security-advisory/qsa-25-10 • https://www.qnap.com/en/security-advisory/qsa-25-09 • https://www.qnap.com/en/security-advisory/qsa-25-14 • https://www.qnap.com/en/security-advisory/qsa-25-17

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.