Advisory Alert

Alert Number: AAA20260105 **Date:** January 5, 2026

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
IBM	**Critical**	Improper Origin Validation Vulnerability
NetApp	**High**, Medium	Multiple Vulnerabilities
QNAP	**High**, Medium	Multiple Vulnerabilities

Description

Affected Product	**IBM**
Severity	**Critical**
Affected Vulnerability	Improper Origin Validation Vulnerability (CVE-2024-57965)
Description	IBM has released a security update addressing an improper origin validation vulnerability that exists in Grafana which is used by IBM Storage Ceph. **CVE-2024-57965**: In axios before 1.7.8, lib/helpers/isURLSameOrigin.js does not use a URL object when determining an origin, and has a potentially unwanted setAttribute('href',href) call. NOTE: some parties feel that the code change only addresses a warning message from a SAST tool and does not fix a vulnerability. IBM advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	IBM Storage Ceph versions: • 8.1, 8.0z0-z5 • 7.1z0-z8, 7.0z0-z2 • 6.1z1-z9, 6.0
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/7256167

Affected Product	**NetApp**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-50182, CVE-2025-6965, CVE-2025-50181)
Description	NetApp has released a security update addressing multiple vulnerabilities that exists in their products. **CVE-2025-50182**: Multiple NetApp products incorporate urllib3. Urllib3 versions 2.2.0 prior to 2.5.0 are susceptible to a vulnerability which when successfully exploited could lead to disclosure of sensitive information. **CVE-2025-6965**: Multiple NetApp products incorporate SQLite. SQLite versions prior to 3.50.2 are susceptible to a vulnerability which when successfully exploited could lead to disclosure of sensitive information, addition or modification of data, or Denial of Service (DoS). **CVE-2025-50181**: Multiple NetApp products incorporate urllib3. Urllib3 versions prior to 2.5.0 are susceptible to a vulnerability which when successfully exploited could lead to disclosure of sensitive information. NetApp advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	NetApp Data Classification Active IQ Unified Manager for VMware vSphere
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://security.netapp.com/advisory/ntap-20260102-0004 • https://security.netapp.com/advisory/ntap-20260102-0013 • https://security.netapp.com/advisory/ntap-20260102-0005

Affected Product	**QNAP**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-44013, CVE-2025-52426, CVE-2025-52430, CVE-2025-52431, CVE-2025-53405, CVE-2025-53414, CVE-2025-53589, CVE-2025-53590, CVE-2025-53592, CVE-2025-53596, CVE-2025-52863, CVE-2025-52864, CVE-2025-52872, CVE-2025-53593, CVE-2025-53591, CVE-2025-54164, CVE-2025-54165, CVE-2025-54166, CVE-2025-47208, CVE-2025-57705, CVE-2025-52871, CVE-2025-53597, CVE-2025-9110, CVE-2025-48721, CVE-2025-62852, CVE-2025-59380, CVE-2025-59381, CVE-2025-59387, CVE-2025-53594)
Description	QNAP has released security updates addressing multiple vulnerabilities that exists in their products. These vulnerabilities could be exploited by malicious users to conduct Denial of Service (DoS), Unauthorized Remote Access, Memory Modification, Information Disclosure, and Path Traversal. QNAP advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	QTS version 5.2.x QuTS hero version h5.2.x QuTS hero version h5.3.x License Center version 2.0.x MARS (Multi-Application Recovery Service) version 1.2.x Qfinder Pro (for Mac) version 7.13.x Qsync (for Mac) version 5.1.x QVPN Device Client (for Mac) version 2.2.x
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.qnap.com/en/security-advisory/qsa-25-50 • https://www.qnap.com/en/security-advisory/qsa-25-52 • https://www.qnap.com/en/security-advisory/qsa-25-51 • https://www.qnap.com/en/security-advisory/qsa-25-53 • https://www.qnap.com/en/security-advisory/qsa-25-55

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.