Advisory Alert

Alert Number: **AAA20251027** **Date:** **October 27, 2025**

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
QNAP	**High**	HTTP Request Smuggling Vulnerability
SUSE	**High**	Multiple Linux Kernel Vulnerabilities
NetApp	**High**, **Medium**, **Low**	Multiple Vulnerabilities

Description

Affected Product	**QNAP**
Severity	**High**
Affected Vulnerability	HTTP Request Smuggling Vulnerability (CVE-2025-55315)
Description	QNAP has released security updates addressing an HTTP request smuggling vulnerability that exists in Microsoft ASP.NET Core. **CVE-2025-55315 -** Microsoft has disclosed a security vulnerability affecting ASP.NET Core that could allow an attacker to bypass security controls through HTTP Request Smuggling. If successfully exploited, an authenticated attacker could send specially crafted HTTP requests to the web server, resulting in unauthorized access to sensitive data, modification of server files, or limited denial-of-service conditions. QNAP advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	QNAP NetBak PC Agent
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.qnap.com/en/security-advisory/qsa-25-44

Affected Product	**SUSE**
Severity	**High**
Affected Vulnerability	Multiple Linux Kernel Vulnerabilities (CVE-2025-21971, CVE-2025-38110, CVE-2025-38206, CVE-2025-38396, CVE-2025-38471, CVE-2025-38499, CVE-2025-38566, CVE-2025-38644, CVE-2025-38678)
Description	SUSE has released security updates addressing multiple linux kernel vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users in order to compromise the affected systems. SUSE advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	OpenSUSE Leap 15.4, 15.6 SUSE Linux Enterprise High Performance Computing 15 SP4 SUSE Linux Enterprise Live Patching 15-SP4, 15-SP6, 15-SP7 SUSE Linux Enterprise Micro 5.3, 5.4 SUSE Linux Enterprise Real Time 15 SP4, 15 SP6, 15 SP7 SUSE Linux Enterprise Server 15 SP4, 15 SP6, 15 SP7 SUSE Linux Enterprise Server for SAP Applications 15 SP4, 15 SP6, 15 SP7
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.suse.com/support/update/announcement/2025/suse-su-20253765-1/ • https://www.suse.com/support/update/announcement/2025/suse-su-20253768-1/ • https://www.suse.com/support/update/announcement/2025/suse-su-20253770-1/ • https://www.suse.com/support/update/announcement/2025/suse-su-20253771-1/ • https://www.suse.com/support/update/announcement/2025/suse-su-20253772-1/ • https://www.suse.com/support/update/announcement/2025/suse-su-20253769-1/

Affected Product	**NetApp**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2022-21618, CVE-2022-21619, CVE-2022-21624, CVE-2022-21626, CVE-2022-21628, CVE-2022-39399, CVE-2022-40303, CVE-2022-40304, CVE-2022-41881, CVE-2022-41915, CVE-2020-15522)
Description	NetApp has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users in order to conduct denial of service, sensitive information disclosure, addition or modification of data. NetApp advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	ONTAP 9 SnapCenter OnCommand Insight NetApp Manageability SDK ONTAP Antivirus Connector OnCommand Workflow Automation Active IQ Unified Manager for Linux SANtricity Storage Plugin for vCenter NetApp SolidFire & HCI Management Node Active IQ Unified Manager for VMware vSphere Active IQ Unified Manager for Microsoft Windows E-Series SANtricity OS Controller Software 11.x NetApp SolidFire & HCI Storage Node (Element Software) E-Series SANtricity Unified Manager and Web Services Proxy
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://security.netapp.com/advisory/ntap-20221209-0003 • https://security.netapp.com/advisory/ntap-20221028-0012 • https://security.netapp.com/advisory/ntap-20230113-0004 • https://security.netapp.com/advisory/ntap-20210622-0007

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.