Advisory Alert

Alert Number: AAA20260119 **Date:** January 19, 2026

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Red Hat	**Critical**	Multiple Vulnerabilities
NetApp	**Critical**	Multiple Vulnerabilities
Red Hat	**High**	Multiple Vulnerabilities
SUSE	**High**	Multiple Vulnerabilities
NetApp	**High**, **Medium**, **Low**	Multiple Vulnerabilities
HPE	**Medium**	Hardware CPU State Corruption Vulnerability

Description

Affected Product	**Red Hat**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-52999, CVE-2025-55163)
Description	Red Hat has released a security update addressing multiple vulnerabilities that exist in the JBoss Enterprise Application. **CVE-2025-52999**: jackson-core contains core low-level incremental ("streaming") parser and generator abstractions used by Jackson Data Processor. In versions prior to 2.15.0, if a user parses an input file and it has deeply nested data, Jackson could end up throwing a StackoverflowError if the depth is particularly large. **CVE-2025-55163**: Netty is an asynchronous, event-driven network application framework. Prior to versions 4.1.124.Final and 4.2.4.Final, Netty is vulnerable to MadeYouReset DDoS. This is a logical vulnerability in the HTTP/2 protocol, that uses malformed HTTP/2 control frames in order to break the max concurrent streams limit - which results in resource exhaustion and distributed denial of service. Red Hat advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	JBoss Enterprise Application Platform 7.1 EUS 7.1 x86_64
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://access.redhat.com/errata/RHSA-2026:0742

Affected Product	**NetApp**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2022-0318, CVE-2025-49794, CVE-2025-49796, CVE-2022-37434, CVE-2024-45491, CVE-2022-3520)
Description	NetApp has released a security update addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to conduct Sensitive Information Disclosure, Data Modification and Denial of Service (DoS). NetApp advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	Active IQ Unified Manager for Microsoft Windows Active IQ Unified Manager for VMware vSphere Management Services for Element Software and NetApp HCI NetApp Manageability SDK OnCommand Workflow Automation ONTAP Select Deploy administration utility ONTAP tools for VMware vSphere 10 StorageGRID (formerly StorageGRID Webscale)
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://security.netapp.com/advisory/ntap-20241115-0004 • https://security.netapp.com/advisory/ntap-20250718-0003 • https://security.netapp.com/advisory/ntap-20250718-0004 • https://security.netapp.com/advisory/ntap-20220901-0005 • https://security.netapp.com/advisory/ntap-20241018-0003 • https://security.netapp.com/advisory/ntap-20241115-0010

Affected Product	**Red Hat**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-37869), CVE-2025-40141, CVE-2025-40176, CVE-2025-68285)
Description	Red Hat has released a security update addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to compromise the affected system. Red Hat advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	Red Hat Enterprise Linux for x86_64 - Extended Update Support 10.0 x86_64 Red Hat Enterprise Linux for IBM z Systems - Extended Update Support 10.0 s390x Red Hat Enterprise Linux for Power, little endian - Extended Update Support 10.0 ppc64le Red Hat Enterprise Linux for ARM 64 - Extended Update Support 10.0 aarch64 Red Hat CodeReady Linux Builder for x86_64 - Extended Update Support 10.0 x86_64 Red Hat CodeReady Linux Builder for Power, little endian - Extended Update Support 10.0 ppc64le Red Hat CodeReady Linux Builder for IBM z Systems - Extended Update Support 10.0 s390x Red Hat CodeReady Linux Builder for ARM 64 - Extended Update Support 10.0 aarch64 Red Hat Enterprise Linux for ARM 64 - 4 years of updates 10.0 aarch64 Red Hat Enterprise Linux for IBM z Systems - 4 years of updates 10.0 s390x Red Hat Enterprise Linux for Power, little endian - 4 years of support 10.0 ppc64le Red Hat Enterprise Linux for x86_64 - 4 years of updates 10.0 x86_64
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://access.redhat.com/errata/RHSA-2026:0747

Affected Product	**SUSE**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities
Description	SUSE has released a security update addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to compromise the affected system. SUSE advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	SUSE Linux Enterprise High Performance Computing 15 SP4 SUSE Linux Enterprise Live Patching 15-SP4 SUSE Linux Enterprise Micro 5.3 SUSE Linux Enterprise Micro 5.4 SUSE Linux Enterprise Real Time 15 SP4 SUSE Linux Enterprise Server 15 SP4 SUSE Linux Enterprise Server for SAP Applications 15 SP4
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.suse.com/support/update/announcement/2026/suse-su-20260140-1/

Affected Product	**NetApp**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities
Description	NetApp has released a security update addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to conduct Sensitive Information Disclosure, Data Modification and Denial of Service (DoS). NetApp advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	Active IQ Unified Manager for Linux Active IQ Unified Manager for Microsoft Windows Active IQ Unified Manager for VMware vSphere Brocade SAN Navigator (SANnav) Data Infrastructure Insights Acquisition Unit Data Infrastructure Insights Storage Workload Security Agent Data Infrastructure Insights Storage Workload Security Agent Management Services for Element Software and NetApp HCI NetApp Console NetApp HCI Compute Node (Bootstrap OS) NetApp Manageability SDK OnCommand Insight OnCommand Workflow Automation ONTAP 9 ONTAP Select Deploy administration utility ONTAP tools for VMware vSphere 10 SnapCenter Trident Autosupport
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://security.netapp.com/advisory/

Affected Product	**HPE**
Severity	**Medium**
Affected Vulnerability	Hardware CPU State Corruption Vulnerability (CVE-2025-29943)
Description	HPE has released a security update addressing a hardware CPU state corruption vulnerability that exists in HPE Proliant AMD Servers. **CVE-2025-29943**: Improper access control within AMD CPUs may allow an admin-privileged attacker to modify the configuration of the CPU pipeline, potentially resulting in the corruption of the stack pointer inside an SEV-SNP guest. HPE advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	HPE ProLiant Compute DL325 Gen12 - Prior to 1.20_07-11-2025 HPE ProLiant Compute DL345 Gen12 - Prior to 1.20_07-11-2025 HPE ProLiant DL145 Gen11 - Prior to 1.72_10-03-2025 HPE ProLiant DL325 Gen11 Server - Prior to 2.82_10-03-2025 HPE ProLiant DL345 Gen11 Server - Prior to 2.82_10-03-2025 HPE ProLiant DL365 Gen11 Server - Prior to 2.82_10-03-2025 HPE ProLiant DL385 Gen11 Server - Prior to 2.82_10-03-2025 HPE ProLiant DL325 Gen10 Plus v2 server - Prior to 3.90_10-03-2025 HPE ProLiant DL345 Gen10 Plus server - Prior to 3.90_10-03-2025 HPE ProLiant DL365 Gen10 Plus server - Prior to 3.90_10-03-2025 HPE ProLiant DL385 Gen10 Plus v2 server - Prior to 3.90_10-03-2025 HPE ProLiant XL225n Gen10 Plus 1U Node - Prior to 3.90_10-03-2025 HPE ProLiant XL645d Gen10 Plus Server - Prior to 3.90_10-03-2025 HPE ProLiant XL675d Gen10 Plus Server - Prior to 3.90_10-03-2025
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbhf04991en_us&docLocale=en_US

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.