Advisory Alert

Alert Number: **AAA20251111** **Date:** **November 11, 2025**

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
NetApp	**Critical**	Security Update
SUSE	**High**	Multiple Vulnerabilities
F5	**High**	BIND Cache Poisoning Vulnerability
Dell	**High**, **Medium**	Multiple Vulnerabilities
Red Hat	**High**, **Medium**	Multiple Vulnerabilities

Description

Affected Product	**NetApp**
Severity	**Critical**
Affected Vulnerability	Security Update (CVE-2025-7783)
Description	NetApp has released a security update addressing an insufficiently random value vulnerability in the Form-Data component present in NetApp products. **CVE-2025-7783 -** Multiple NetApp products incorporate form-data. Form-data versions prior to 4.0.4, prior to 3.0.4 and prior to 2.5.4 are susceptible to a vulnerability which when successfully exploited could lead to disclosure of sensitive information or addition or modification of data. NetApp advises to apply this security fix at your earliest to protect your systems from potential threats.
Affected Products	NetApp Shift Toolkit
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://security.netapp.com/advisory/ntap-20250801-0002

Affected Product	**SUSE**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2022-50248, CVE-2022-50252, CVE-2025-38664, CVE-2025-38453, CVE-2025-38511, CVE-2025-38617, CVE-2025-38618, CVE-2024-53164, CVE-2025-38618,)
Description	SUSE has released security updates addressing a multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users 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 15.3 openSUSE Leap 15.4 openSUSE Leap 15.5 SUSE Linux Enterprise High Performance Computing 12 SP5 SUSE Linux Enterprise High Performance Computing 15 SP3 SUSE Linux Enterprise High Performance Computing 15 SP4 SUSE Linux Enterprise High Performance Computing 15 SP5 SUSE Linux Enterprise Live Patching 12-SP5 SUSE Linux Enterprise Live Patching 15-SP3 SUSE Linux Enterprise Live Patching 15-SP4 SUSE Linux Enterprise Live Patching 15-SP5 SUSE Linux Enterprise Live Patching 15-SP7 SUSE Linux Enterprise Micro 5.1 SUSE Linux Enterprise Micro 5.2 SUSE Linux Enterprise Micro 5.3 SUSE Linux Enterprise Micro 5.4 SUSE Linux Enterprise Micro 5.5 SUSE Linux Enterprise Real Time 15 SP4 SUSE Linux Enterprise Real Time 15 SP5 SUSE Linux Enterprise Real Time 15 SP7 SUSE Linux Enterprise Server 12 SP5 SUSE Linux Enterprise Server 15 SP3 SUSE Linux Enterprise Server 15 SP4 SUSE Linux Enterprise Server 15 SP5 SUSE Linux Enterprise Server 15 SP7 SUSE Linux Enterprise Server for SAP Applications 12 SP5 SUSE Linux Enterprise Server for SAP Applications 15 SP3 SUSE Linux Enterprise Server for SAP Applications 15 SP4 SUSE Linux Enterprise Server for SAP Applications 15 SP5 SUSE Linux Enterprise Server for SAP Applications 15 SP7
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.suse.com/support/update/announcement/2025/suse-su-20254004-1/ • https://www.suse.com/support/update/announcement/2025/suse-su-20254003-1/ • https://www.suse.com/support/update/announcement/2025/suse-su-20254001-1/ • https://www.suse.com/support/update/announcement/2025/suse-su-20254040-1/ • https://www.suse.com/support/update/announcement/2025/suse-su-20254036-1/ • https://www.suse.com/support/update/announcement/2025/suse-su-20254031-1/ • https://www.suse.com/support/update/announcement/2025/suse-su-20254016-1/ • https://www.suse.com/support/update/announcement/2025/suse-su-20254024-1/

Affected Product	**F5**
Severity	**High**
Affected Vulnerability	BIND Cache Poisoning Vulnerability (CVE-2025-40778)
Description	F5 has released a security update addressing a cache poisoning vulnerability that exists in the BIND component present in their products. **CVE-2025-40778** - Under certain circumstances, BIND is too lenient when accepting records from answers, allowing an attacker to inject forged data into the cache. F5 advises to apply this security fix at your earliest to protect your systems from potential threats.
Affected Products	BIG-IP DNS • Versions 17.5.0 – 17.5.1 and 17.1.0 – 17.1.3 • Versions 16.1.0 – 16.1.6 • Versions 15.1.0 – 15.1.10 F5OS-A Versions 1.8.0 – 1.8.3 and 1.5.1 – 1.5.4 F5OS-C Versions 1.8.0 – 1.8.2 and 1.6.0 – 1.6.4
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://my.f5.com/manage/s/article/K000157334

Affected Product	**Dell**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-32414, CVE-2025-32415, CVE-2025-4207, CVE-2023-38709, CVE-2025-46802, CVE-2025-46805, CVE-2025-7425, CVE-2025-7424)
Description	Dell has released a security update addressing multiple vulnerabilities that exist in the third-party components present in their products. These vulnerabilities could be exploited by malicious users to compromise the affected systems. Dell advises to apply this security fix at your earliest to protect your systems from potential threats.
Affected Products	• NetWorker Management Console, NetWorker Server, NetWorker Client and Storage Node versions prior to 19.12.0.3 • PowerScale OneFS versions prior to 9.12.0.0
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.dell.com/support/kbdoc/en-us/000390068/ • https://www.dell.com/support/kbdoc/en-us/000390206/

Affected Product	**Red Hat**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-7254, CVE-2021-3629, CVE-2021-3717, CVE-2021-30129, CVE-2021-37714, CVE-2021-20289, CVE-2021-40690)
Description	Red Hat has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to conduct StackOverflow, Denial of Service (DoS) and Information Disclosure. Red Hat advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	JBoss Enterprise Application Platform 7.4 ELS 7.4 for RHEL 9 x86_64 JBoss Enterprise Application Platform 7.4 ELS 7.4 for RHEL 8 x86_64 JBoss Enterprise Application Platform 7.4 ELS 7.4 for RHEL 7 x86_64 JBoss Enterprise Application Platform 7.4 ELS 7 x86_64 JBoss Enterprise Application Platform Text-Only Advisories x86_64
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://access.redhat.com/errata/RHSA-2025:20052 • https://access.redhat.com/errata/RHSA-2025:20057 • https://access.redhat.com/errata/RHSA-2021:4679

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.