Advisory Alert

Alert Number: AAA20260624 **Date:** June 24, 2026

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Vendor	Severity	Vulnerability
Dell	**Critical**	Multiple Vulnerabilities
SUSE	**High**	Multiple Vulnerabilities
IBM	**High**, **Medium**, **Low**	Multiple Vulnerabilities

Description

Vendor	**Dell**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities
Description	Dell 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 systems. Dell advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	Dell Networking OS10 versions prior to 10.6.1.2
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.dell.com/support/kbdoc/en-us/000480864/dsa-2026-240-security-update-for-dell-networking-os10-vulnerabilities

Vendor	**SUSE**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities
Description	SUSE has released security updates addressing 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	SUSE Linux Enterprise 12 SP5 (SLES, SLES for SAP, HPC, Live Patching) SUSE Linux Enterprise 15 SP4 (SLES, SLES for SAP, HPC, Live Patching, Real Time) SUSE Linux Enterprise 15 SP5 (SLES, SLES for SAP, HPC, Live Patching, Real Time) SUSE Linux Enterprise 15 SP6 (SLES, SLES for SAP, Live Patching, Real Time) SUSE Linux Enterprise 15 SP7 (SLES, SLES for SAP, Live Patching, Real Time, Real Time Module) SUSE Linux Enterprise Micro (Versions 5.3, 5.4, 5.5) openSUSE Leap (Versions 15.4, 15.5, 15.6)
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.suse.com/support/update/announcement/2026/suse-su-20262549-1/ https://www.suse.com/support/update/announcement/2026/suse-su-20262553-1/ https://www.suse.com/support/update/announcement/2026/suse-su-20262567-1/ https://www.suse.com/support/update/announcement/2026/suse-su-20262532-1/ https://www.suse.com/support/update/announcement/2026/suse-su-20262559-1/ https://www.suse.com/support/update/announcement/2026/suse-su-20262588-1/ https://www.suse.com/support/update/announcement/2026/suse-su-20262591-1/ https://www.suse.com/support/update/announcement/2026/suse-su-20262592-1/ https://www.suse.com/support/update/announcement/2026/suse-su-20262571-1/ https://www.suse.com/support/update/announcement/2026/suse-su-20262594-1/

Vendor	**IBM**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities
Description	IBM has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to compromise the affected systems. IBM advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	WebSphere Application Server WebSphere Application Server - Liberty WebSphere Remote Server IBM Db2
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/bulletin/

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.