Advisory Alert

Alert Number: AAA20250613 **Date:** June 13, 2025

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
SUSE	**High**	Multiple Vulnerabilities
Dell	**High**, Medium	Multiple Vulnerabilities
Palo Alto Networks	**High**, Medium, Low	Multiple Vulnerabilities
IBM	Medium	Multiple Vulnerabilities

Description

Affected Product	**SUSE**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-49855, CVE-2024-57996, CVE-2024-58013, CVE-2025-21680, CVE-2022-49080)
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 system. SUSE advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	openSUSE Leap 15.3, 15.4, 15.6 SUSE Linux Enterprise High Performance Computing 12 SP5, 15 SP3, 15 SP4 SUSE Linux Enterprise Live Patching 12-SP5, 15-SP3, 15-SP4, 15-SP6 SUSE Linux Enterprise Micro 5.1, 5.2, 5.3, 5.4 SUSE Linux Enterprise Real Time 15 SP4, 15 SP6 SUSE Linux Enterprise Server 12 SP5, 15 SP3, 15 SP4, 15 SP6 SUSE Linux Enterprise Server for SAP Applications 12 SP5, 15 SP3, 15 SP4, 15 SP6
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.suse.com/support/update/announcement/2025/suse-su-202501930-1/ • https://www.suse.com/support/update/announcement/2025/suse-su-202501929-1/ • https://www.suse.com/support/update/announcement/2025/suse-su-202501928-1/ • https://www.suse.com/support/update/announcement/2025/suse-su-202501927-1/ • https://www.suse.com/support/update/announcement/2025/suse-su-202501922-1/ • https://www.suse.com/support/update/announcement/2025/suse-su-202501906-1/

Affected Product	**Dell**
Severity	**High**, Medium
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-27689, CVE-2025-2884)
Description	Dell has released security updates addressing multiple vulnerabilities that exist in Dell iDRAC Tools and Dell PowerEdge Server Firmware. **CVE-2025-27689** - Dell iDRAC Tools, version(s) prior to 11.3.0.0, contain(s) an Improper Access Control vulnerability. A low privileged attacker with local access could potentially exploit this vulnerability, leading to Elevation of privileges. **CVE-2025-2884** - An out-of-bounds (OOB) read vulnerability exists in Trusted Platform Module (TPM) 2.0 Library specification. An attacker who can successfully exploit this vulnerability can potentially lead the TPM to a failure state causing a Denial of Service. Dell advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Dell iDRAC Tools Versions prior to 11.3.0.0 Firmware Versions prior to 7.2.5.0 of PowerEdge R770, PowerEdge R670, PowerEdge R570, PowerEdge R470, PowerEdge XE7740, PowerEdge R6715, PowerEdge R7715, PowerEdge R6725, PowerEdge R7725, PowerEdge M7725, PowerEdge XE7745, PowerEdge R660, PowerEdge R760, PowerEdge C6620, PowerEdge MX760c, PowerEdge R860, PowerEdge R960, PowerEdge HS5610, PowerEdge HS5620, PowerEdge R660xs, PowerEdge R760xs, PowerEdge R760xd2, PowerEdge T560, PowerEdge R760xa, PowerEdge XE9680, PowerEdge XE9680L, PowerEdge XR5610, PowerEdge XR8610t, PowerEdge XR8620t, PowerEdge XR7620, PowerEdge XE8640, PowerEdge XE9640, PowerEdge T160, PowerEdge T360, PowerEdge R260, PowerEdge R360, PowerEdge R6615, PowerEdge R6625, PowerEdge R7615, PowerEdge R7625, PowerEdge XE9685l, PowerEdge C6615, PowerEdge R650, PowerEdge R750, PowerEdge R750XA, PowerEdge C6520, PowerEdge MX750C, PowerEdge R550, PowerEdge R450, PowerEdge R650XS, PowerEdge R750XS, PowerEdge T550, PowerEdge XR11, PowerEdge XR12, PowerEdge XR4510c, PowerEdge XR4520c, PowerEdge T150, PowerEdge T350, PowerEdge R250, PowerEdge R350, PowerEdge R6515, PowerEdge R6525, PowerEdge R7515, PowerEdge R7525, PowerEdge C6525, PowerEdge XE8545, Dell XC Core XC660, Dell XC Core XC760, Dell XC Core XC660xs, Dell XC Core XC760xa, Dell XC Core XC7625, Dell EMC XC Core XC450, Dell EMC XC Core XC650, Dell EMC XC Core XC750, Dell EMC XC Core XC750xa, Dell EMC XC Core XC6520, Dell EMC XC Core XC7525
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.dell.com/support/kbdoc/en-us/000323242/dsa-2025-169-security-update-for-dell-idrac-tools-vulnerabilities • https://www.dell.com/support/kbdoc/en-us/000331010/dsa-2025-232-security-update-for-dell-poweredge-server-for-a-trusted-platform-module-tpm-2-0-firmware-vulnerability

Affected Product	**Palo Alto Networks**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-4232, CVE-2025-4231, CVE-2025-4230, CVE-2025-4229, CVE-2025-4228, CVE-2025-4227)
Description	Palo Alto Networks has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to cause Code and Command Injection, Information Disclosure, Privilege Escalation and Traffic Interception. Palo Alto Networks advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	GlobalProtect App 6.3 versions prior to 6.3.3-h1 on macOS GlobalProtect App 6.3 versions prior to 6.3.2-566 on Windows GlobalProtect App 6.1 all versions on Windows, macOS GlobalProtect App 6.0 all versions on Windows, macOS PAN-OS 11.2 versions prior to 11.2.6 PAN-OS 11.1 versions prior to 11.1.10 PAN-OS 11.0 versions prior to 11.0.3 PAN-OS 10.2 versions prior to 10.2.17 PAN-OS 10.1 all versions Cortex XDR Broker VM versions prior to 27.0.26
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://security.paloaltonetworks.com/CVE-2025-4232 • https://security.paloaltonetworks.com/CVE-2025-4231 • https://security.paloaltonetworks.com/CVE-2025-4230 • https://security.paloaltonetworks.com/CVE-2025-4229 • https://security.paloaltonetworks.com/CVE-2025-4228 • https://security.paloaltonetworks.com/CVE-2025-4227

Affected Product	**IBM**
Severity	**Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2022-3510, CVE-2022-3509, CVE-2022-3171)
Description	IBM has released security updates addressing multiple vulnerabilities that exist in IBM Db2 Server. **CVE-2022-3510** - A parsing issue similar to CVE-2022-3171, but with Message-Type Extensions in protobuf-java core and lite versions prior to 3.21.7, 3.20.3, 3.19.6 and 3.16.3 can lead to a denial of service attack. Inputs containing multiple instances of non-repeated embedded messages with repeated or unknown fields causes objects to be converted back-n-forth between mutable and immutable forms, resulting in potentially long garbage collection pauses. We recommend updating to the versions mentioned above. **CVE-2022-3509** - A parsing issue similar to CVE-2022-3171, but with textformat in protobuf-java core and lite versions prior to 3.21.7, 3.20.3, 3.19.6 and 3.16.3 can lead to a denial of service attack. Inputs containing multiple instances of non-repeated embedded messages with repeated or unknown fields causes objects to be converted back-n-forth between mutable and immutable forms, resulting in potentially long garbage collection pauses. We recommend updating to the versions mentioned above. **CVE-2022-3171** - protobuf-java core and lite are vulnerable to a denial of service, caused by a flaw in the parsing procedure for binary and text format data. By sending non-repeated embedded messages with repeated or unknown fields, a remote authenticated attacker could exploit this vulnerability to cause long garbage collection pauses. IBM advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	IBM Db2 Server versions 11.1.0 - 11.1.4.7, 11.5.0 - 11.5.9 and 12.1.0 - 12.1.1
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/7234906

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.