Advisory Alert

Alert Number: AAA20250730 **Date:** July 30, 2025

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
IBM	**Critical**	Multiple Vulnerabilities
Dell	**High**	Multiple Vulnerabilities
IBM	**High**, Medium	Multiple Vulnerabilities
SolarWinds	Medium	XML External Entity Injection Vulnerability

Description

Affected Product	**IBM**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-45491, CVE-2024-45492, CVE-2025-30472)
Description	IBM has released security updates addressing multiple vulnerabilities that exist in IBM Db2. **CVE-2024-45491** - An issue was discovered in libexpat before 2.6.3. dtdCopy in xmlparse.c can have an integer overflow for nDefaultAtts on 32-bit platforms (where UINT_MAX equals SIZE_MAX). **CVE-2024-45492** - An issue was discovered in libexpat before 2.6.3. nextScaffoldPart in xmlparse.c can have an integer overflow for m_groupSize on 32-bit platforms (where UINT_MAX equals SIZE_MAX). **CVE-2025-30472** - Corosync through 3.1.9, if encryption is disabled or the attacker knows the encryption key, has a stack-based buffer overflow in orf_token_endian_convert in exec/totemsrp.c via a large UDP packet. IBM advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	IBM Db2 Server Versions - 10.5.0.0 - 10.5.0.11, 11.1.0 - 11.1.4.7, 11.5.0 - 11.5.9, 12.1.0 - 12.1.2
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.ibm.com/support/pages/node/7240946 • https://www.ibm.com/support/pages/node/7240977

Affected Product	**Dell**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2016-2183, CVE-2008-5161, CVE-2025-24813, CVE-2025-31651, CVE-2025-25193, CVE-2025-27789, CVE-2024-29409, CVE-2025-23083, CVE-2025-23084, CVE-2025-23085, CVE-2025-23166, CVE-2025-23165, CVE-2025-23167, CVE-2024-9681, CVE-2024-7264, CVE-2023-46218, CVE-2023-46219, CVE-2025-32414, CVE-2025-32415, CVE-2025-27113, CVE-2025-2588, CVE-2025-30204, CVE-2025-22869, CVE-2025-0736, CVE-2025-30691, CVE-2025-21587, CVE-2021-47671, CVE-2022-49741, CVE-2024-46784, CVE-2025-21726, CVE-2025-21785, CVE-2025-21791, CVE-2025-21812, CVE-2025-21886, CVE-2025-22004, CVE-2025-22020, CVE-2025-22029, CVE-2025-22045, CVE-2025-22055, CVE-2025-22097, CVE-2022-39377, CVE-2023-33204, CVE-2025-32728, CVE-2025-4207, CVE-2025-47273, CVE-2025-4802, CVE-2024-28956, CVE-2024-43420, CVE-2024-45332, CVE-2025-20012, CVE-2025-20054, CVE-2025-20103, CVE-2025-20623, CVE-2025-24495)
Description	Dell 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. Dell advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Dell EMC PowerMax eNAS - Versions prior to 8.1.15.24 Dell PowerProtect Data Manager - Versions prior to 19.20
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.dell.com/support/kbdoc/en-us/000180942/dsa-2020-222-dell-emc-powermax-embedded-nas-enas-security-update-for-multiple-third-party-component-vulnerabilities • https://www.dell.com/support/kbdoc/en-us/000349609/dsa-2025-304-security-update-for-dell-powerprotect-data-manager-multiple-security-vulnerabilities

Affected Product	**IBM**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-36071, CVE-2024-52894, CVE-2025-33092, CVE-2025-0755, CVE-2025-33114, CVE-2024-51473, CVE-2024-49828, CVE-2024-45490, CVE-2024-50602, CVE-2025-2533, CVE-2025-33143, CVE-2025-24970)
Description	IBM has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to cause denial of service Improper Input validation, buffer overflow and integer overflow. IBM advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	IBM Db2 Server Versions - 11.5.0 - 11.5.9, 12.1.0 - 12.1.2, 10.5.0.0 - 10.5.0.11, 11.1.0 - 11.1.4.7 IBM Db2 Client and Server Versions - 11.5.0 - 11.5.9, 12.1.0 - 12.1.2
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.ibm.com/support/pages/node/7240955 • https://www.ibm.com/support/pages/node/7240953 • https://www.ibm.com/support/pages/node/7240940 • https://www.ibm.com/support/pages/node/7240941 • https://www.ibm.com/support/pages/node/7240943 • https://www.ibm.com/support/pages/node/7240944 • https://www.ibm.com/support/pages/node/7240945 • https://www.ibm.com/support/pages/node/7240946 • https://www.ibm.com/support/pages/node/7240947 • https://www.ibm.com/support/pages/node/7240949 • https://www.ibm.com/support/pages/node/7240952

Affected Product	**SolarWinds**
Severity	**Medium**
Affected Vulnerability	XML External Entity Injection Vulnerability (CVE-2025-26400)
Description	SolarWinds has released security updates addressing an XML External Entity Injection Vulnerability that exists in their products. **CVE-2025-26400** - SolarWinds Web Help Desk was reported to be affected by an XML External Entity Injection (XXE) vulnerability that could lead to information disclosure. A valid, low-privilege access is required unless the attacker had access to the local server to modify configuration files. SolarWinds advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	SolarWinds Web Help Desk 12.8.6 and all previous versions
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.solarwinds.com/trust-center/security-advisories/cve-2025-26400

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.