Advisory Alert

Alert Number: AAA20260121 **Date:** January 21, 2026

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
IBM	**Critical**	Multiple Vulnerabilities
Oracle	**Critical**	Multiple Vulnerabilities
Dell	**High**	Integer Overflow Vulnerability
SUSE	**High**	Multiple Vulnerabilities
Hitachi	**High**, Medium	Multiple Vulnerabilities
IBM	**High**, Medium, Low	Multiple Vulnerabilities
Oracle	**High**, Medium, Low	Multiple Vulnerabilities
cPanel	**High**, Low	Multiple Vulnerabilities

Description

Affected Product	**IBM**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2016-6293, CVE-2017-14952)
Description	IBM has released a security update addressing multiple vulnerabilities that exist in IBM's Db2 Servers. **CVE-2016-6293**: The uloc_acceptLanguageFromHTTP function in common/uloc.cpp in International Components for Unicode (ICU) through 57.1 for C/C++ does not ensure that there is a '\0' character at the end of a certain temporary array, which allows remote attackers to cause a denial of service (out-of-bounds read) or possibly have unspecified other impact via a call with a long httpAcceptLanguage argument. **CVE-2017-14952**: Double free in i18n/zonemeta.cpp in International Components for Unicode (ICU) for C/C++ through 59.1 allows remote attackers to execute arbitrary code via a crafted string, aka a "redundant UVector entry clean up function call" issue. IBM advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	IBM Db2 Server Version 10.5.0.0 to 10.5.0.11 IBM Db2 Server Version 11.1.0 to 11.1.4.7 IBM Db2 Server Version 11.5.0 to 11.5.9
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/7241823

Affected Product	**Oracle**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-66516, CVE-2025-49844, CVE-2021-43113, CVE-2025-49796, CVE-2026-21962, CVE-2025-54988, CVE-2025-4949, CVE-2025-54874, CVE-2025-23048, CVE-2021-23926, CVE-2024-52046, CVE-2025-6965, CVE-2026-21969, CVE-2025-10230, CVE-2025-62168, CVE-2025-14321)
Description	Oracle 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. Oracle advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	Multiple Products
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.oracle.com/security-alerts/cpujan2026.html • https://www.oracle.com/security-alerts/bulletinjan2026.html

Affected Product	**Dell**
Severity	**High**
Affected Vulnerability	Integer Overflow Vulnerability (CVE-2023-5869)
Description	Dell has released a security update addressing an integer overflow vulnerability that exists in the third party component PostgreSQL which is present in PowerScale InsightIQ. **CVE-2023-5869**: A flaw was found in PostgreSQL that allows authenticated database users to execute arbitrary code through missing overflow checks during SQL array value modification. This issue exists due to an integer overflow during array modification where a remote user can trigger the overflow by providing specially crafted data. This enables the execution of arbitrary code on the target system, allowing users to write arbitrary bytes to memory and extensively read the server's memory. Dell advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	PowerScale InsightIQ Versions prior to 6.0.0
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.dell.com/support/kbdoc/en-us/000417416/dsa-2026-050-security-update-for-dell-powerscale-insightiq-postgresql-vulnerability

Affected Product	**SUSE**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2022-50327, CVE-2022-50409, CVE-2022-50490, CVE-2023-53676, CVE-2024-58239, CVE-2025-38476, CVE-2025-38572, CVE-2025-38608, CVE-2025-40204)
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	openSUSE Leap 15.4 openSUSE Leap 15.5 SUSE Linux Enterprise High Performance Computing 15 SP4 SUSE Linux Enterprise High Performance Computing 15 SP5 SUSE Linux Enterprise Live Patching 15-SP4 SUSE Linux Enterprise Live Patching 15-SP5 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 Server 15 SP4 SUSE Linux Enterprise Server 15 SP5 SUSE Linux Enterprise Server for SAP Applications 15 SP4 SUSE Linux Enterprise Server for SAP Applications 15 SP5
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.suse.com/support/update/announcement/2026/suse-su-20260180-1/ • https://www.suse.com/support/update/announcement/2026/suse-su-20260184-1/ • https://www.suse.com/support/update/announcement/2026/suse-su-20260185-1/ • https://www.suse.com/support/update/announcement/2026/suse-su-20260186-1/ • https://www.suse.com/support/update/announcement/2026/suse-su-20260187-1/ • https://www.suse.com/support/update/announcement/2026/suse-su-20260188-1/

Affected Product	**Hitachi**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-54100, CVE-2025-55233, CVE-2025-59516, CVE-2025-59517, CVE-2025-62221, CVE-2025-62454, CVE-2025-62455, CVE-2025-62457, CVE-2025-62458, CVE-2025-62461, CVE-2025-62462, CVE-2025-62463, CVE-2025-62464, CVE-2025-62466, CVE-2025-62467, CVE-2025-62470, CVE-2025-62472, CVE-2025-62473, CVE-2025-62474, CVE-2025-62549, CVE-2025-62565, CVE-2025-62567, CVE-2025-62571, CVE-2025-62573, CVE-2025-64658, CVE-2025-64661, CVE-2025-64670, CVE-2025-64673)
Description	Hitachi 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. Hitachi advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	Hitachi Virtual Storage Platform versions 5200, 5600, 5200H and 5600H Hitachi Virtual Storage Platform versions 5100, 5500, 5100H and 5500H
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.hitachi.com/products/it/storage-solutions/sec_info/2025/12.html

Affected Product	**IBM**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2017-15422, CVE-2017-7868, CVE-2011-4599, CVE-2014-7923, CVE-2017-7867, CVE-2017-15396, CVE-2020-21913, CVE-2020-10531, CVE-2016-7415, CVE-2017-17484)
Description	IBM has released a security update addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to conduct Denial of Service (DoS) and Arbitrary Code Execution. IBM advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	IBM Db2 Server Version 10.5.0.0 to 10.5.0.11 IBM Db2 Server Version 11.1.0 to 11.1.4.7 IBM Db2 Server Version 11.5.0 to 11.5.9
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/7241823

Affected Product	**Oracle**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities
Description	Oracle has released a monthly security update addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to compromise the affected system. Oracle advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	Multiple Products
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.oracle.com/security-alerts/cpujan2026.html • https://www.oracle.com/security-alerts/bulletinjan2026.html

Affected Product	**cPanel**
Severity	**High**, **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-55132, CVE-2025-59465)
Description	cPanel has released a security update addressing multiple vulnerabilities that exist in third party components utilized within their products. **CVE-2025-55132**: A flaw in Node.js's permission model allows a file's access and modification timestamps to be changed via `futimes()` even when the process has only read permissions. Unlike `utimes()`, `futimes()` does not apply the expected write-permission checks, which means file metadata can be modified in read-only directories. **CVE-2025-59465:** A malformed `HTTP/2 HEADERS` frame with oversized, invalid `HPACK` data can cause Node.js to crash by triggering an unhandled `TLSSocket` error `ECONNRESET`. Instead of safely closing the connection, the process crashes, enabling a remote denial of service. This primarily affects applications that do not attach explicit error handlers to secure sockets. cPanel advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	ea-nodejs20 versions 20.19.6 ea-nodejs22 versions 22.21.1
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://docs.cpanel.net/changelogs/easyapache-4-change-log-25/

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.