



# Advisory Alert

Alert Number: AAA20251022      Date: October 22, 2025

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
IBM	Critical	Improper Input Validation Vulnerability
Oracle	Critical	Multiple Vulnerabilities
Citrix	High	Multiple Vulnerabilities
IBM	High, Medium	Multiple Vulnerabilities
Oracle	High, Medium	Multiple Vulnerabilities
Ubuntu	Medium	Multiple Vulnerabilities
Dell	Medium	Security Update
Red Hat	Medium	Multiple Vulnerabilities
NetApp	Medium	Security Update

Description

Affected Product	IBM
Severity	Critical
Affected Vulnerability	Improper Input Validation Vulnerability (CVE-2024-47175)
Description	<p>IBM has released security updates addressing an Improper Input Validation Vulnerability that exists in IBM DB2 Data Management Console.</p> <p><b>CVE-2024-47175</b> - CUPS is a standards-based, open-source printing system, and `libppd` can be used for legacy PPD file support. The `libppd` function `ppdCreatePPDFromIPP2` does not sanitize IPP attributes when creating the PPD buffer. When used in combination with other functions such as `cfGetPrinterAttributes5`, can result in user controlled input and ultimately code execution via Foomatic.</p> <p>IBM advises to apply security fixes at your earliest to protect systems from potential threats.</p>
Affected Products	IBM DB2 Data Management Console version 3.1.12
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	<a href="https://www.ibm.com/support/pages/node/7248583">https://www.ibm.com/support/pages/node/7248583</a>

Affected Product	Oracle
Severity	Critical
Affected Vulnerability	Multiple Vulnerabilities
Description	<p>Oracle has released Critical Patch Update Advisory for October, addressing multiple vulnerabilities that exist in Oracle code and third party components included in Oracle products.</p> <p>Oracle advises to apply security fixes at your earliest to protect systems from potential threats.</p>
Affected Products	Multiple Products
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	<a href="https://www.oracle.com/security-alerts/cpuoct2025.html">https://www.oracle.com/security-alerts/cpuoct2025.html</a>

Affected Product	Citrix
Severity	High
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-58147, CVE-2025-58148)
Description	<p>Citrix has released security updates addressing multiple vulnerabilities that exist XenServer. Several issues have been identified in XenServer 8.4 that may allow privileged code in a guest VM to compromise or crash the host.</p> <p>Citrix advises to apply security fixes at your earliest to protect systems from potential threats.</p>
Affected Products	XenServer 8.4
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	<a href="https://support.citrix.com/support-home/kbsearch/article?articleNumber=CTX695405&amp;articleURL=XenServer_Security_Update_for_CVE_2025_58147_and_CVE_2025_58148">https://support.citrix.com/support-home/kbsearch/article?articleNumber=CTX695405&amp;articleURL=XenServer_Security_Update_for_CVE_2025_58147_and_CVE_2025_58148</a>

Affected Product	IBM
Severity	High, Medium
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-51775, CVE-2023-23916, CVE-2025-27363, CVE-2024-38819, CVE-2024-45801, CVE-2024-47176, CVE-2024-47076, CVE-2024-47177, CVE-2024-2985)
Description	<p>IBM has released security updates addressing multiple vulnerabilities that exist in IBM DB2 Data Management Console. These vulnerabilities could be exploited by malicious users to cause Denial of Service, Arbitrary Code Execution, Path Traversal, Cross-Site Scripting.</p> <p>IBM advises to apply security fixes at your earliest to protect systems from potential threats.</p>
Affected Products	IBM DB2 Data Management Console version 3.1.12
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	<a href="https://www.ibm.com/support/pages/node/7248583">https://www.ibm.com/support/pages/node/7248583</a>

Affected Product	Oracle
Severity	High, Medium
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-54874, CVE-2025-48989 , CVE-2025-7345, CVE-2025-57833, CVE-2025-52434, CVE-2025-52520 CVE-2025-53506)
Description	<p>Oracle has released security updates addressing multiple vulnerabilities that exist in Oracle Solaris Operating System. These vulnerabilities may be remotely exploitable without authentication, i.e., may be exploited over a network without the need for a username and password.</p> <p>Oracle advises to apply security fixes at your earliest to protect systems from potential threats.</p>
Affected Products	Oracle Solaris 11.4
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	<a href="https://www.oracle.com/security-alerts/bulletinoc2025.html">https://www.oracle.com/security-alerts/bulletinoc2025.html</a>

Affected Product	Ubuntu
Severity	Medium
Affected Vulnerability	Multiple Vulnerabilities
Description	<p>Ubuntu 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.</p> <p>Ubuntu advises to apply security fixes at your earliest to protect systems from potential threats.</p>
Affected Products	Ubuntu 25.04 Ubuntu 24.04
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	<a href="https://ubuntu.com/security/notices/USN-7833-1">https://ubuntu.com/security/notices/USN-7833-1</a>

Affected Product	Dell
Severity	Medium
Affected Vulnerability	Security Update (CVE-2025-33043)
Description	<p>Dell has released security updates addressing a vulnerability that exists in AMI BIOS which affects Dell products. This vulnerability could be exploited by malicious users to compromise the affected system.</p> <p>Dell advises to apply security fixes at your earliest to protect systems from potential threats.</p>
Affected Products	<p>Dell Precision 3431 Tower BIOS Versions prior to 1.36.0</p> <p>OptiPlex 3070 BIOS Versions prior to 1.35.0</p> <p>OptiPlex 5070 BIOS Versions prior to 1.35.0</p> <p>OptiPlex 7070 BIOS Versions prior to 1.35.0</p> <p>Optiplex 7071 BIOS Versions prior to 1.35.0</p> <p>OptiPlex XE3 BIOS Versions prior to 1.38.0</p>
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	<a href="https://www.dell.com/support/kbdoc/en-us/000331782/dsa-2025-237">https://www.dell.com/support/kbdoc/en-us/000331782/dsa-2025-237</a>

Affected Product	Red Hat
Severity	Medium
Affected Vulnerability	Multiple Vulnerabilities (CVE-2022-50228, CVE-2023-53125, CVE-2023-53305, CVE-2025-22026, CVE-2025-37797, CVE-2025-38461, CVE-2025-38556, CVE-2025-39730, CVE-2025-39751)
Description	<p>Red Hat 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.</p> <p>Red Hat advises to apply security fixes at your earliest to protect systems from potential threats.</p>
Affected Products	<p>Red Hat Enterprise Linux for x86_64 - Extended Update Support Extension 8.8 x86_64</p> <p>Red Hat Enterprise Linux Server - TUS 8.8 x86_64</p> <p>Red Hat Enterprise Linux Server for Power LE - Update Services for SAP Solutions 8.8 ppc64le</p> <p>Red Hat Enterprise Linux for x86_64 - Update Services for SAP Solutions 8.8 x86_64</p>
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	<a href="https://access.redhat.com/errata/RHSA-2025:18932">https://access.redhat.com/errata/RHSA-2025:18932</a>

Affected Product	NetApp
Severity	Medium
Affected Vulnerability	Security Update (CVE-2024-36905)
Description	<p>NetApp has released security updates addressing a vulnerability that exists in their products.</p> <p><b>CVE-2024-36905</b> - Multiple NetApp products incorporate Linux kernel. Certain versions of Linux kernel are susceptible to a vulnerability which when successfully exploited could lead to Denial of Service.</p> <p>NetApp advises to apply security fixes at your earliest to protect systems from potential threats.</p>
Affected Products	<p>Active IQ Unified Manager for VMware vSphere</p> <p>E-Series SANtricity OS Controller Software 11.x</p> <p>FAS/AFF Baseboard Management Controller (BMC) - 8300/8700/A400/C400</p> <p>ONTAP Select Deploy administration utility</p>
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	<a href="https://security.netapp.com/advisory/ntap-20240905-0005">https://security.netapp.com/advisory/ntap-20240905-0005</a>

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.