



Advisory Alert

Alert Number: AAA20250401 Date: April 1, 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
SUSE	High	Multiple Kernel Vulnerabilities
IBM	High, Medium	Multiple Vulnerabilities
Ubuntu	High, Medium	Multiple Kernel Vulnerabilities

Description

Affected Product	IBM
Severity	Critical
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-45337, CVE-2024-41110, CVE-2024-27281)
Description	IBM has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to cause execute arbitrary code, bypass authorization plugins, privilege escalation. IBM advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	IBM Db2 on Cloud Pak for Data and Db2 Warehouse on Cloud Pak for Data Versions - <ul style="list-style-type: none">v3.5 through refresh 10v4.0 through refresh 9v4.5 through refresh 3v4.6 through refresh 6v4.7 through refresh 4v4.8 through refresh 6v4.8 through refresh 8v5.0 through refresh 2v5.0 through refresh 3v5.1 through refresh 1
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/7229443

Affected Product	Dell
Severity	High
Affected Vulnerability	Multiple Vulnerabilities
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	Unisphere for PowerMax 9.2.4.15 Host Installation - Versions prior to 9.2.4.15 Unisphere for PowerMax 10.1.0.19 Host Installation - Versions prior to 10.1.0.19 Unisphere for PowerMax 10.2.0.9 Host Installation - Versions prior to 10.2.0.9 Unisphere for PowerMax Virtual Appliance 9.2.4.15 Virtual Appliance - Versions prior to 9.2.4.15 Unisphere 360 9.2.4.35 Host Installation - Versions prior to 9.2.4.35 Solutions Enabler Virtual Appliance 9.2.4.9 Virtual Appliance - Versions prior to 9.2.4.9 Dell PowerMax EEM 5978 Embedded Management 5978.714.714.10730 and prior Dell PowerMaxOS 5978 PowerMax OS 5978.714.714.10730and prior Dell PowerMax EEM 10.1.0.7 Embedded Management 10.1.0.7 and prior Dell PowerMax OS 10.1.0.7 PowerMax OS 10.1.0.7 and prior Dell PowerMax EEM 10.2.0.1 Embedded Management 10.2.0.1 and prior Dell PowerMax OS 10.2.0.1 PowerMax OS 10.2.0.1 and prior
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.dell.com/support/kbdoc/en-us/000302223/dsa-2025-111-dell-powermaxos-dell-powermax-eem-dell-unisphere-for-powermax-dell-unisphere-for-powermax-virtual-appliance-dell-unisphere-360-dell-solutions-enabler-and-dell-solutions-enabler-virtual-appliance-security-update-for-multiple-vulnerabilities

Affected Product	SUSE
Severity	High
Affected Vulnerability	Multiple Kernel Vulnerabilities (CVE-2024-41062, CVE-2024-57882)
Description	<p>SUSE has released security updates addressing multiple kernel vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to compromise the affected system.</p> <p>SUSE advises to apply security fixes at your earliest to protect systems from potential threats.</p>
Affected Products	OpenSUSE Leap 15.6 SUSE Linux Enterprise Live Patching 15-SP6 SUSE Linux Enterprise Real Time 15 SP6 SUSE Linux Enterprise Server 15 SP6 SUSE Linux Enterprise Server for SAP Applications 15 SP6
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	<ul style="list-style-type: none">https://www.suse.com/support/update/announcement/2025/suse-su-20251057-1https://www.suse.com/support/update/announcement/2025/suse-su-20251059-1https://www.suse.com/support/update/announcement/2025/suse-su-20251064-1https://www.suse.com/support/update/announcement/2025/suse-su-20251066-1https://www.suse.com/support/update/announcement/2025/suse-su-20251072-1https://www.suse.com/support/update/announcement/2025/suse-su-20251076-1

Affected Product	IBM
Severity	High, Medium
Affected Vulnerability	Multiple Vulnerabilities (CVE-2018-20225, CVE-2019-11253, CVE-2020-13844, CVE-2021-4204, CVE-2021-44906, CVE-2021-47495, CVE-2022-29153, CVE-2022-48706, CVE-2022-48890, CVE-2022-48921, CVE-2023-43804, CVE-2023-44487, CVE-2023-45142, CVE-2023-45857, CVE-2023-52455, CVE-2023-52467, CVE-2023-52605, CVE-2023-52832, CVE-2023-52885, CVE-2023-52898, CVE-2024-26740, CVE-2024-26776, CVE-2024-26843, CVE-2024-34997, CVE-2024-35176, CVE-2024-35790, CVE-2024-35946, CVE-2024-36620, CVE-2024-37071, CVE-2024-39494, CVE-2024-39908, CVE-2024-40679, CVE-2024-41123, CVE-2024-41761, CVE-2024-41762, CVE-2024-41946, CVE-2024-43398, CVE-2024-45338, CVE-2024-45663, CVE-2024-47764, CVE-2024-49761, CVE-2024-6119, CVE-2024-6232, CVE-2024-6484, CVE-2024-6485)
Description	<p>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, NULL pointer dereference, memory leak, and Cross-Site Request Forgery (CSRF).</p> <p>IBM advises to apply security fixes at your earliest to protect systems from potential threats.</p>
Affected Products	IBM Db2 on Cloud Pak for Data and Db2 Warehouse on Cloud Pak for Data Versions - <ul style="list-style-type: none">v3.5 through refresh 10v4.0 through refresh 9v4.5 through refresh 3v4.6 through refresh 6v4.7 through refresh 4v4.8 through refresh 6v4.8 through refresh 8v5.0 through refresh 2v5.0 through refresh 3v5.1 through refresh 1
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/7229443

Affected Product	Ubuntu
Severity	High, Medium
Affected Vulnerability	Multiple Kernel 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 cause use-after-free, denial of service and execute arbitrary code.</p> <p>Ubuntu advises to apply security fixes at your earliest to protect systems from potential threats.</p>
Affected Products	Ubuntu 20.04 Ubuntu 18.04
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://ubuntu.com/security/notices/USN-7391-1

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.