Advisory Alert

Alert Number: AAA20230630 **Date:** June 30, 2023

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Suse	**High**	Multiple Vulnerabilities
Ubuntu	**High**, Medium	Multiple Vulnerabilities
IBM	**High**, Medium, Low	Multiple Vulnerabilities

Description

Affected Product	**Suse**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2022-4744, CVE-2023-1390, CVE-2023-23455, CVE-2023-28466, CVE-2023-31436)
Description	Suse has released security updates addressing multiple vulnerabilities affecting their products. Exploitation of the vulnerabilities could lead to Denial of Service, Out-of-bounds write and use-after-free or NULL pointer dereference, Suse recommends to apply the necessary patch updates at your earliest to avoid issues.
Affected Products	SUSE Linux Enterprise High Performance Computing 12 SP4, 12 SP5, 15 SP1, 15 SP2, 15 SP3, 15 SP4 SUSE Linux Enterprise Live Patching 12-SP4, 12-SP5, 15-SP1, 15-SP2, 15-SP3, 15-SP4 SUSE Linux Enterprise Micro 5.1, 5.2, 5.3, 5.4 SUSE Linux Enterprise Real Time 15 SP4 SUSE Linux Enterprise Server 12 SP4, 12 SP5, 15 SP1, 15 SP2, 15 SP3, 15 SP4 SUSE Linux Enterprise Server for SAP Applications 12 SP4, 12 SP5, 15 SP1, 15 SP2, 15 SP3, 15 SP4
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.suse.com/support/update/announcement/2023/suse-su-20232701-1 https://www.suse.com/support/update/announcement/2023/suse-su-20232695-1 https://www.suse.com/support/update/announcement/2023/suse-su-20232697-1 https://www.suse.com/support/update/announcement/2023/suse-su-20232698-1 https://www.suse.com/support/update/announcement/2023/suse-su-20232700-1 https://www.suse.com/support/update/announcement/2023/suse-su-20232710-1/ https://www.suse.com/support/update/announcement/2023/suse-su-20232709-1/ https://www.suse.com/support/update/announcement/2023/suse-su-20232708-1/ https://www.suse.com/support/update/announcement/2023/suse-su-20232703-1/ https://www.suse.com/support/update/announcement/2023/suse-su-20232702-1/ https://www.suse.com/support/update/announcement/2023/suse-su-20232734-1/ https://www.suse.com/support/update/announcement/2023/suse-su-20232731-1/ https://www.suse.com/support/update/announcement/2023/suse-su-20232735-1/ https://www.suse.com/support/update/announcement/2023/suse-su-20232724-1/ https://www.suse.com/support/update/announcement/2023/suse-su-20232727-1/ https://www.suse.com/support/update/announcement/2023/suse-su-20232700-1/ https://www.suse.com/support/update/announcement/2023/suse-su-20232698-1/ https://www.suse.com/support/update/announcement/2023/suse-su-20232697-1/ https://www.suse.com/support/update/announcement/2023/suse-su-20232695-1/ https://www.suse.com/support/update/announcement/2023/suse-su-20232701-1/ https://www.suse.com/support/update/announcement/2023/suse-su-20232721-1/ https://www.suse.com/support/update/announcement/2023/suse-su-20232720-1/ https://www.suse.com/support/update/announcement/2023/suse-su-20232719-1/ https://www.suse.com/support/update/announcement/2023/suse-su-20232714-1/ https://www.suse.com/support/update/announcement/2023/suse-su-20232718-1/

Affected Product	**Ubuntu**
Severity	**High**, Medium
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-2176, CVE-2023-35788, CVE-2023-2430)
Description	Ubuntu has released security updates addressing multiple vulnerabilities in their products. If exploited theses vulnerabilities could lead to Denial of service, Sensitive information disclosure and Arbitrary code execution. Ubuntu recommends to apply the necessary patch updates at your earliest to avoid issues.
Affected Products	Ubuntu 16.04 Ubuntu 18.04 Ubuntu 20.04 Ubuntu 22.04 Ubuntu 22.10 Ubuntu 23.04
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://ubuntu.com/security/notices/USN-6194-1 https://ubuntu.com/security/notices/USN-6193-1 https://ubuntu.com/security/notices/USN-6192-1 https://ubuntu.com/security/notices/USN-6191-1

Affected Product	**IBM**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-35890, CVE-2023-24998, CVE-2022-41721, CVE-2022-46175, CVE-2022-43929, CVE-2022-43927, CVE-2014-3577, CVE-2022-43930, CVE-2023-29257, CVE-2023-29255, CVE-2023-27555, CVE-2023-26021, CVE-2023-25930, CVE-2023-26022, CVE-2023-27559, CVE-2023-25165, CVE-2019-10743, CVE-2022-1471, CVE-2022-41716, CVE-2023-24540, CVE-2023-29400, CVE-2023-24539, CVE-2021-3156, CVE-2019-19234, CVE-2019-19232, CVE-2019-18634, CVE-2022-41723, CVE-2022-41724, CVE-2022-41725, CVE-2023-24532, CVE-2023-24537, CVE-2022-41881, CVE-2022-41915, CVE-2022-42889, CVE-2022-33980, CVE-2022-25881, CVE-2020-8244, CVE-2022-42004, CVE-2022-42003, CVE-2022-38752, CVE-2022-38751, CVE-2022-38750, CVE-2022-38749, CVE-2022-41854, CVE-2022-25857, CVE-2023-23918, CVE-2023-23919, CVE-2023-23936, CVE-2023-24807, CVE-2023-23920, CVE-2022-37866, CVE-2022-37865, CVE-2022-43548)
Description	IBM has released security updates addressing multiple vulnerabilities in their products. Exploitation of the most severe vulnerabilities could lead to Denial of Service, Cross-site scripting, Heap-based buffer overflow and HTML injection IBM recommends to apply the necessary patch updates at your earliest to avoid issues.
Affected Products	IBM Cloud Pak for Applications 5.1 IBM Db2 on Cloud Pak for Data and Db2 Warehouse on Cloud Pak for Data v3.5 through refresh 10 IBM Db2 on Cloud Pak for Data and Db2 Warehouse on Cloud Pak for Data v4.0 through refresh 9 IBM Db2 on Cloud Pak for Data and Db2 Warehouse on Cloud Pak for Data v4.5 through refresh 3 IBM Db2 on Cloud Pak for Data and Db2 Warehouse on Cloud Pak for Data v4.6 through refresh 6 IBM Tivoli Application Dependency Discovery Manager 7.3.0.0 - 7.3.0.10 IBM WebSphere Application Server 9.0, 8.5 WebSphere Service Registry and Repository 8.5.x
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/7008345 https://www.ibm.com/support/pages/node/7008405 https://www.ibm.com/support/pages/node/7008449 https://www.ibm.com/support/pages/node/7008401

Disclaimer

The information provided herein is on "as is" basis, without warranty of any kind. FinCSIRT highly recommend to follow the company policies and procedures when applying the necessary patches with thorough testing and ensuring proper roll-back capabilities exists.