Advisory Alert

Alert Number: AAA20230720 **Date:** July 20, 2023

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Redhat	**High**	Use-after-free flaw Vulnerability
Suse	**High**	Multiple Vulnerabilities
IBM	**High**, Medium	Multiple Vulnerabilities
Cisco	Medium	Privilege Escalation Vulnerability

Description

Affected Product	**Redhat**
Severity	**High**
Affected Vulnerability	Use-after-free flaw Vulnerability (CVE-2022-3564)
Description	Redhat has released a patch update addressing a Use-after-free flaw vulnerability that exists in Linux kernel's L2CAP Bluetooth functionality. This flaw allows a local or Bluetooth connection user to crash the system or potentially escalate privileges. Redhat recommends to apply necessary fixes to avoid issues.
Affected Products	Red Hat Enterprise Linux Server 7 x86_64 Red Hat Enterprise Linux for Power, little endian 7 ppc64le
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://access.redhat.com/errata/RHSA-2023:4215

Affected Product	**Suse**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-1249, CVE-2023-1829, CVE-2023-2430, CVE-2023-28866, CVE-2023-3090, CVE-2023-3111, CVE-2023-3212, CVE-2023-3220, CVE-2023-3357, CVE-2023-3358, CVE-2023-3389, CVE-2023-35788, CVE-2023-35823, CVE-2023-35828, CVE-2023-35829)
Description	Suse has released a security update addressing multiple vulnerabilities affecting their products. Exploitation of these vulnerabilities could lead to Heap out-of-bounds write, Use-after-free flaw, NULL pointer dereference. Suse recommends to apply the necessary patch updates at your earliest to avoid issues.
Affected Products	openSUSE Leap 15.5 Public Cloud Module 15-SP5 SUSE Linux Enterprise High Performance Computing 15 SP5 SUSE Linux Enterprise Server 15 SP5 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/2023/suse-su-20232892-1/

Affected Product	**IBM**
Severity	**High ,Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2020-4682, CVE-2019-4055, CVE-2019-4762, CVE-2020-4310, CVE-2021-39034, CVE-2019-4227, CVE-2019-4261, CVE-2019-4378, CVE-2019-4614, CVE-2019-4656, CVE-2020-4320, CVE-2019-4049, CVE-2019-4619, CVE-2019-4719, CVE-2020-4338, CVE-2021-38949, CVE-2019-4655, CVE-2022-1471)
Description	IBM has released security updates addressing multiple vulnerabilities within their products. If exploited theses vulnerabilities could lead to Arbitrary code execution, Denial of Service and Sensitive information disclosure. IBM recommends to apply the necessary patch updates at your earliest to avoid issues.
Affected Products	IBM QRadar SIEM - All MQJMS versions before 7.4.0-QRADAR-PROTOCOL-MQJMS-7.4-20230327175451 IBM QRadar SIEM -All MQJMS versions before 7.5.0-QRADAR-PROTOCOL-MQJMS-7.5-20230327175444 IBM Db2 Web Query for i 2.3.0 IBM Db2 Web Query for i 2.4.0
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/7013143 https://www.ibm.com/support/pages/node/7013297

Affected Product	**Cisco**
Severity	**Medium**
Affected Vulnerability	Privilege Escalation Vulnerability (CVE-2023-20216)
Description	Cisco has released a security update addressing a Privilege Escalation vulnerability within privilege management functionality of all Cisco BroadWorks servers. This vulnerability is due to incorrect implementation of user role permissions. A successful exploit could allow an authenticated, local attacker to elevate privileges to root on an affected system. Cisco recommends to apply the necessary patch updates at your earliest to avoid issues.
Affected Products	BroadWorks Application Delivery Platform, Media Server, and Service Control Function Server Cisco BroadWorks Application Server 22.0 and earlier, 23.0, 24.0 BroadWorks Database Server, Execution Server, Network Database Server, and Network Function Manager 22.0 and earlier BroadWorks Database Troubleshooting Server 22.0 and earlier BroadWorks Network Server, Profile Server, and Xtended Services Platform 22.0 and earlier, 23.0
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-bw-priv-esc-qTgUZOsQ

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.