Advisory Alert

Alert Number: AAA20240521 **Date:** May 21, 2024

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Dell	**Critical**	Multiple Vulnerabilities
F5	**High**	Multiple Vulnerabilities
SUSE	**High**	Multiple Vulnerabilities
IBM	**High**, Medium	Multiple Vulnerabilities
MariaDB	**Medium**	Security Update

Description

Affected Product	**Dell**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-41993, CVE-2024-21085, CVE-2024-21011, CVE-2024-21068, CVE-2024-21094, CVE-2024-21012, CVE-2024-21003, CVE-2024-21005, CVE-2024-21002, CVE-2024-21004)
Description	Dell has issued security updates addressing multiple vulnerabilities that exist in Dell NetWorker Runtime Environment. 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	Dell NetWorker Runtime Environment (NRE) - Version 8.0.18
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.dell.com/support/kbdoc/en-us/000225215/dsa-2024-224-security-update-for-dell-networker-runtime-environment-nre-vulnerabilities

Affected Product	**F5**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2016-5636, CVE-2023-36632)
Description	F5 has released security updates addressing multiple vulnerabilities that exist in their products. **CVE-2016-5636 -** Integer overflow in the get_data function in zipimport.c in CPython (aka Python) before 2.7.12, 3.x before 3.4.5, and 3.5.x before 3.5.2 allows remote attackers to have unspecified impact via a negative data size value, which triggers a heap-based buffer overflow. **CVE-2023-36632 -** The legacy email.utils.parseaddr function in Python through 3.11.4 allows attackers to trigger "RecursionError: maximum recursion depth exceeded while calling a Python object" via a crafted argument. This argument is plausibly an untrusted value from an application's input data that was supposed to contain a name and an e-mail address. F5 advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Traffix SDC – Version 5.1.0
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://my.f5.com/manage/s/article/K000139698

Affected Product	**SUSE**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2022-48651, CVE-2023-52502, CVE-2023-6546, CVE-2024-26585 CVE-2024-26610, CVE-2024-26766, CVE-2023-6931, CVE-2023-1829)
Description	SUSE has released security updates addressing multiple vulnerabilities that exist in SUSE Linux Kernel. These vulnerabilities could be exploited by malicious users to cause Use After Free, Privilege Escalation, Memory Corruption, Heap Out-of-bounds Write. SUSE advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	OpenSUSE Leap 15.5, 15.3 SUSE Linux Enterprise High Performance Computing 15 SP5, 15 SP3, 12 SP5 SUSE Linux Enterprise Real Time 15 SP5 SUSE Linux Enterprise Server for SAP Applications 15 SP5 SUSE Linux Enterprise Live Patching 12-SP5, 15-SP3, 15-SP5 SUSE Linux Enterprise Server 12 SP5, 15 SP5 SUSE Linux Enterprise Server for SAP Applications 12 SP5 SUSE Linux Enterprise Micro 5.1, 5.2, 5.5 SUSE Linux Enterprise Server 15 SP3 SUSE Linux Enterprise Server for SAP Applications 15 SP3
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.suse.com/support/update/announcement/2024/suse-su-20241685-1 • https://www.suse.com/support/update/announcement/2024/suse-su-20241686-1 • https://www.suse.com/support/update/announcement/2024/suse-su-20241692-1 • https://www.suse.com/support/update/announcement/2024/suse-su-20241694-1 • https://www.suse.com/support/update/announcement/2024/suse-su-20241695-1 • https://www.suse.com/support/update/announcement/2024/suse-su-20241696-1

Affected Product	**IBM**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-45283, CVE-2023-45284, CVE-2023-45285, CVE-2023-39326 CVE-2021-35942, CVE-2021-3999, CVE-2020-1752, CVE-2020-1751, CVE-2020-10029 CVE-2019-19126, CVE-2023-48795, CVE-2022-2068, CVE-2021-3711, CVE-2022-1292 CVE-2022-0778, CVE-2021-3712, CVE-2021-4160, CVE-2022-2097)
Description	IBM has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to cause Buffer Overflow, Use After Free, Arbitrary Code Execution and Denial of Service. IBM advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	IBM Db2 Rest - Version(s) 1.0.0.121-amd64 to 1.0.0.301-amd64
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.ibm.com/support/pages/node/7154430 • https://www.ibm.com/support/pages/node/7154484

Affected Product	**MariaDB**
Severity	**Medium**
Affected Vulnerability	Security Update (CVE-2024-21096)
Description	MariaDB has released security updates addressing security vulnerabilities that exist in Maria database management system. These vulnerabilities could be exploited by malicious users to cause Denial of Service, Unauthorized Read Access and Unauthorized Update. MariaDB advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	MariaDB versions prior to : • MariaDB 11.2.4 • MariaDB 11.1.5 • MariaDB 11.0.6 • MariaDB 10.6.18 • MariaDB 10.5.25 • MariaDB 10.11.8
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://mariadb.com/kb/en/security/

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.