Advisory Alert

Alert Number: AAA20240828 **Date:** August 28, 2024

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
F5	**High**	Use-After-Free Vulnerability
Suse	**High**	Multiple Vulnerabilities
IBM	**High**, **Medium**	Multiple Vulnerabilities
Dell	**Medium**	Multiple Vulnerabilities

Affected Product	**F5**
Severity	**High**
Affected Vulnerability	Use-After-Free Vulnerability (CVE-2023-4921)
Description	F5 has released a mitigation procedure addressing a Use-After-Free Vulnerability that exists in Linux kernel's net/sched: sch_qfq component which affects F5 products. This vulnerability can be exploited to achieve local privilege escalation, when the plug qdisc is used as a class of the qfq qdisc, sending network packets triggers use-after-free in qfq_dequeue() due to the incorrect .peek handler of sch_plug and lack of error checking in agg_dequeue(). F5 advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Traffix SDC 5.2.0 and 5.1.0
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://my.f5.com/manage/s/article/K000140864

Affected Product	**SUSE**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-36921, CVE-2024-35950, CVE-2024-27398, CVE-2024-26930, CVE-2024-26923, CVE-2024-26852, CVE-2024-26828, CVE-2024-26610, CVE-2024-23307, CVE-2023-6546, CVE-2023-6531, CVE-2023-52772, CVE-2023-1829, CVE-2022-48651, CVE-2021-47402, CVE-2021-47402, CVE-2021-47383, CVE-2021-47378, CVE-2021-47378, CVE-2021-46955
Description	SUSE has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited to cause use-after-free conditions, integer overflow, memory corruption. SUSE advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	openSUSE Leap 15.3, 15.6 SUSE Linux Enterprise High Performance Computing 12 SP5, 15 SP2, 15 SP3 SUSE Linux Enterprise Live Patching 12 SP5, 15 SP2, 15 SP3, 15-SP6 SUSE Linux Enterprise Micro 5.1, 5.2 SUSE Linux Enterprise Real Time 15 SP6 SUSE Linux Enterprise Server 12 SP5, 15 SP2, 15 SP3, 15-SP6 SUSE Linux Enterprise Server for SAP Applications 12 SP5, 15 SP2, 15 SP3, 15-SP6
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.suse.com/support/update/announcement/2024/suse-su-20243039-1/ • https://www.suse.com/support/update/announcement/2024/suse-su-20243041-1/ • https://www.suse.com/support/update/announcement/2024/suse-su-20243048-1/ • https://www.suse.com/support/update/announcement/2024/suse-su-20243044-1/ • https://www.suse.com/support/update/announcement/2024/suse-su-20243043-1/ • https://www.suse.com/support/update/announcement/2024/suse-su-20243040-1/ • https://www.suse.com/support/update/announcement/2024/suse-su-20243037-1/ • https://www.suse.com/support/update/announcement/2024/suse-su-20243030-1/ • https://www.suse.com/support/update/announcement/2024/suse-su-20243034-1/ • https://www.suse.com/support/update/announcement/2024/suse-su-20243032-1/ • https://www.suse.com/support/update/announcement/2024/suse-su-20243027-1/ • https://www.suse.com/support/update/announcement/2024/suse-su-20243023-1/ • https://www.suse.com/support/update/announcement/2024/suse-su-20243021-1/ • https://www.suse.com/support/update/announcement/2024/suse-su-20243014-1/

Affected Product	**IBM**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-30171, CVE-2024-29857, CVE-2024-39249, CVE-2024-39338, CVE-2024-34064, CVE-2024-35118, CVE-2024-25026, CVE-2024-22329, CVE-2024-22354)
Description	IBM has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited to cause denial of service, sensitive information disclosure, cross-site scripting, server-side request forgery. IBM advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	IBM Storage Scale 5.1.0.0 - 5.1.9.4 IBM Storage Scale 5.2.0.0 IBM Storage Defender - Resiliency Service 2.0.0 - 2.0.6 Maas360 MDM for Android App 6.31 - 8.60
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.ibm.com/support/pages/node/7166617 • https://www.ibm.com/support/pages/node/7166616 • https://www.ibm.com/support/pages/node/7166286 • https://www.ibm.com/support/pages/node/7166750 • https://www.ibm.com/support/pages/node/7166619

Affected Product	**Dell**
Severity	**Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-37085, CVE-2024-37086, CVE-2024-37087, CVE-2023-22025, CVE-2023-22067, CVE-2023-22081)
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	PowerStore X 3.2.x firmware - ESXi versions prior to 7.0U3q of • PowerStore 1000X • PowerStore 1200X • PowerStore 3000X • PowerStore 3200X • PowerStore 5000X • PowerStore 5200X • PowerStore 7000X • PowerStore 7000X • PowerStore 7200X • PowerStore 7200X • PowerStore 9000X • PowerStore 9200X Dell OpenManage Server Administrator (OMSA) – AdoptOpenJDK Version 11.0.20
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.dell.com/support/kbdoc/en-us/000228074/dsa-2024-365-dell-powerstore-family-security-update-for-vmware-vulnerabilities • https://www.dell.com/support/kbdoc/en-us/000228093/dsa-2024-150-security-update-for-dell-openmanage-server-administrator-omsa-network-access-vulnerability

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.