Advisory Alert

Alert Number: AAA20241203 **Date:** December 3, 2024

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
SUSE	**High**	Multiple Vulnerabilities
F5	**High**, **Medium**	Multiple Vulnerabilities
FortiGuard	**Medium**	Multiple Vulnerabilities

Description

Affected Product	**SUSE**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities
Description	SUSE has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to cause Memory leakage, Denial of service, Integer Overflow, Use-after-free conditions SUSE advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	openSUSE Leap 15.3, 15.4, 15.5 SUSE Enterprise Storage 7.1 SUSE Linux Enterprise Desktop 15 SP4 LTSS SUSE Linux Enterprise High Availability Extension 15 SP3, 15 SP4 SUSE Linux Enterprise High Performance Computing 15 SP3, 15 SP4, 15 SP5 SUSE Linux Enterprise High Performance Computing ESPOS 15 SP4 SUSE Linux Enterprise High Performance Computing LTSS 15 SP3, 15 SP4 SUSE Linux Enterprise Live Patching 15 SP3, 15 SP4, 15 SP5, 15 SP6 SUSE Linux Enterprise Micro 5.1, 5.2, 5.3, 5.4, 5.5 SUSE Linux Enterprise Micro for Rancher 5.2, 5.3, 5.4 SUSE Linux Enterprise Real Time 15 SP4, 15 SP5, 15 SP6 SUSE Linux Enterprise Server 15 SP3, 15 SP4, 15 SP5, 15 SP6 SUSE Linux Enterprise Server 15 SP3 Business Critical Linux SUSE Linux Enterprise Server 15 SP3 LTSS SUSE Linux Enterprise Server 15 SP4 LTSS SUSE Linux Enterprise Server for SAP Applications 15 SP3, 15 SP4, 15 SP5, 15 SP6 SUSE Manager Proxy 4.2, 4.3 SUSE Manager Retail Branch Server 4.2, 4.3 SUSE Manager Server 4.2, 4.3
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.suse.com/support/update/announcement/2024/suse-su-20244141-1/ • https://www.suse.com/support/update/announcement/2024/suse-su-20244140-1/ • https://www.suse.com/support/update/announcement/2024/suse-su-20244139-1/ • https://www.suse.com/support/update/announcement/2024/suse-su-20244131-1/ • https://www.suse.com/support/update/announcement/2024/suse-su-20244129-1/ • https://www.suse.com/support/update/announcement/2024/suse-su-20244128-1/ • https://www.suse.com/support/update/announcement/2024/suse-su-20244127-1/ • https://www.suse.com/support/update/announcement/2024/suse-su-20244125-1/ • https://www.suse.com/support/update/announcement/2024/suse-su-20244120-1/ • https://www.suse.com/support/update/announcement/2024/suse-su-20244122-1/ • https://www.suse.com/support/update/announcement/2024/suse-su-20244123-1/

Affected Product	**F5**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-38197, CVE-2023-37369, CVE-2023-32763, CVE-2023-32762)
Description	F5 has released security updates addressing multiple vulnerabilities that exist in their products. **CVE-2023-38197** - An issue was discovered in Qt before 5.15.15, 6.x before 6.2.10, and 6.3.x through 6.5.x before 6.5.3. There are infinite loops in recursive entity expansion. **CVE-2023-37369** - In Qt before 5.15.15, 6.x before 6.2.9, and 6.3.x through 6.5.x before 6.5.2, there can be an application crash in QXmlStreamReader via a crafted XML string that triggers a situation in which a prefix is greater than a length. **CVE-2023-32763** - An issue was discovered in Qt before 5.15.15, 6.x before 6.2.9, and 6.3.x through 6.5.x before 6.5.1. When a SVG file with an image inside it is rendered, a QTextLayout buffer overflow can be triggered. **CVE-2023-32762** - An issue was discovered in Qt before 5.15.14, 6.x before 6.2.9, and 6.3.x through 6.5.x before 6.5.1. Qt Network incorrectly parses the strict-transport-security (HSTS) header, allowing unencrypted connections to be established, even when explicitly prohibited by the server. This happens if the case used for this header does not exactly match. F5 advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	BIG-IP 17.x 17.1.0 - 17.1.1 BIG-IP 16.x 16.1.0 - 16.1.5 BIG-IP 15.x 15.1.0 - 15.1.10 Traffix SDC 5.x 5.2.0 APM Clients 7.x 7.2.3 - 7.2.5
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://my.f5.com/manage/s/article/K000148809 • https://my.f5.com/manage/s/article/K000148689

Affected Product	**FortiGuard**
Severity	**Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-46720, CVE-2023-48784)
Description	FortiGuard has released security updates addressing multiple vulnerabilities that exist in their products. **CVE-2023-46720** - Multiple stack-based buffer overflow vulnerabilities [CWE-121] in FortiOS may allow an authenticated attacker to achieve arbitrary code execution via specially crafted CLI commands. **CVE-2023-48784** - A use of externally-controlled format string vulnerability [CWE-134] in FortiOS command line interface may allow a local privileged attacker with CLI access to execute arbitrary code or commands via specially crafted requests. FortiGuard advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	FortiOS 7.4 versions 7.4.0 through 7.4.3 FortiOS 7.2 versions 7.2.0 through 7.2.7 FortiOS 7.0 versions 7.0.0 through 7.0.15
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.fortiguard.com/psirt/FG-IR-23-356 • https://www.fortiguard.com/psirt/FG-IR-23-413

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.