Advisory Alert

Alert Number: AAA20260123 **Date:** January 23, 2026

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

Description

Affected Product	**SUSE**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2022-50327, CVE-2022-50409, CVE-2022-50490, CVE-2023-53676, CVE-2024-57849, CVE-2024-58239, CVE-2025-38476, CVE-2025-38572, CVE-2025-38608, CVE-2025-40204)
Description	SUSE has released a security update addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to compromise the affected system. SUSE advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	openSUSE Leap 15.5 SUSE Linux Enterprise High Performance Computing 15 SP5 SUSE Linux Enterprise Live Patching 15-SP5 SUSE Linux Enterprise Live Patching 15-SP7 SUSE Linux Enterprise Micro 5.5 SUSE Linux Enterprise Real Time 15 SP5 SUSE Linux Enterprise Real Time 15 SP7 SUSE Linux Enterprise Server 15 SP5 SUSE Linux Enterprise Server 15 SP7 SUSE Linux Enterprise Server for SAP Applications 15 SP5 SUSE Linux Enterprise Server for SAP Applications 15 SP7
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.suse.com/support/update/announcement/2026/suse-su-20260247-1/ • https://www.suse.com/support/update/announcement/2026/suse-su-20260246-1/

Affected Product	**F5**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-11082, CVE-2025-11083, CVE-2025-12816)
Description	F5 has released a security update addressing multiple vulnerabilities that exist in their products. **CVE-2025-11082:** A flaw has been found in GNU Binutils 2.45. Impacted is the function _bfd_elf_parse_eh_frame of the file bfd/elf-eh-frame.c of the component Linker. Executing manipulation can lead to heap-based buffer overflow. The attack is restricted to local execution. **CVE-2025-11083:** A vulnerability has been found in GNU Binutils 2.45. The affected element is the function elf_swap_shdr in the library bfd/elfcode.h of the component Linker. The manipulation leads to heap-based buffer overflow. The attack must be carried out locally**.** **CVE-2025-12816:** An interpretation-conflict vulnerability in node-forge versions 1.3.1 and earlier enables unauthenticated attackers to craft ASN.1 structures to desynchronize schema validations, yielding a semantic divergence that may bypass downstream cryptographic verifications and security decisions. F5 advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	F5OS-A versions 1.8.0 to 1.8.3 and 1.5.1 to 1.5.4 F5OS-C versions 1.8.0 to 1.8.3 and 1.6.0 to 1.6.4 BIG-IQ Centralized Management versions 8.3.0 to 8.4.0
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://my.f5.com/manage/s/article/K000159667 • https://my.f5.com/manage/s/article/K000159607

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.