Advisory Alert

Alert Number: AAA20250430 **Date:** April 30, 2025

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Cisco	**Critical**	Security Update
Red Hat	**High**	Memory Corruption Vulnerability
SUSE	**High**	Multiple Vulnerabilities

Description

Affected Product	**Cisco**
Severity	**Critical**
Affected Vulnerability	Security Update (CVE-2025-32433)
Description	Cisco has released security updates addressing a vulnerability that exists in third-party product which affects Cisco products. **CVE-2025-32433 -** A critical flaw in the Erlang/OTP SSH server allows unauthenticated remote attackers to execute code by exploiting improper SSH message handling during authentication. Cisco advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Cisco ConfD, ConfD Basic • 7.7.19.1 • 8.1.16.2 Cisco Network Services Orchestrator (NSO) • 5.7.19.1 • 6.1.16.2 • 6.2.11.1 • 6.4.1.1 • 6.4.4.1
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-erlang-otp-ssh-xyZZy

Affected Product	**Red Hat**
Severity	**High**
Affected Vulnerability	Memory Corruption Vulnerability (CVE-2025-21927)
Description	Red Hat has released security update addressing a Memory Corruption Vulnerability that exists in their products. **CVE-2025-21927 -** A vulnerability in the Linux kernel's nvme_tcp_recv_pdu() allowed memory corruption when processing packets with invalid header lengths, potentially leading to out-of-bounds memory access. This has been fixed by validating header lengths and rejecting malformed packets. Red Hat advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Red Hat Enterprise Linux for x86_64 - Update Services for SAP Solutions 9.2 x86_64
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://access.redhat.com/errata/RHSA-2025:4340

Affected Product	**SUSE**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-56650, CVE-2024-8805)
Description	SUSE has released security updates addressing multiple vulnerabilities that exist in Linux Kernel (Live Patch) System. These vulnerabilities could be exploited by malicious users to compromise the affected system. SUSE advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	SUSE Linux Enterprise High Performance Computing 12 SP5 SUSE Linux Enterprise Live Patching 12-SP5 SUSE Linux Enterprise Server 12 SP5 SUSE Linux Enterprise Server for SAP Applications 12 SP5
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.suse.com/support/update/announcement/2025/suse-su-20251402-1/

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.