Advisory Alert

Alert Number: AAA20250923 **Date:** September 23, 2025

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
SUSE	**High**	Multiple Vulnerabilities
Cisco	**Medium**	Packet Filtering Bypass Vulnerability

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 compromise the affected system. SUSE advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Basesystem Module 15-SP7 Development Tools Module 15-SP7 Legacy Module 15-SP7 SUSE Linux Enterprise Desktop 15 SP7 SUSE Linux Enterprise High Availability Extension 15 SP7 SUSE Linux Enterprise Live Patching 15-SP7 SUSE Linux Enterprise Real Time 15 SP7 SUSE Linux Enterprise Server 15 SP7 SUSE Linux Enterprise Server for SAP Applications 15 SP7 SUSE Linux Enterprise Workstation Extension 15 SP7
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.suse.com/support/update/announcement/2025/suse-su-202503290-1/

Affected Product	**Cisco**
Severity	**Medium**
Affected Vulnerability	Packet Filtering Bypass Vulnerability (CVE-2025-20221)
Description	Cisco has released security updates addressing a Packet Filtering Bypass Vulnerability that exists in IOS XE SD-WAN Software. **CVE-2025-20221** - Due to improper traffic filtering conditions on an affected device, an attacker could exploit this by sending a crafted packet to the affected device. A successful exploit could allow the attacker to bypass the Layer 3 and Layer 4 traffic filters and inject a crafted packet into the network. Cisco advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Following standalone Cisco IOS XE SD-WAN Software releases: • 16.9.1 through 16.9.4 • 16.10.1 through 16.10.5 • 16.11.1a • 16.12.2r through 16.12.4
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-snmp-bypass-HHUVujdn

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.