Advisory Alert

Alert Number: AAA20250929 **Date:** September 29, 2025

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
SUSE	**High**	Multiple Vulnerabilities
Cisco	**Medium**	Security Update
Red Hat	**Medium**	Security Update

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	OpenSUSE Leap 15.3, 15.4 SUSE Real Time Module 15-SP7 SUSE Linux Enterprise High Performance Computing 12 SP5, 15 SP3, 15 SP4 SUSE Linux Enterprise Live Patching 12-SP5, 15-SP3, 15-SP4, 15-SP7 SUSE Linux Enterprise Micro 5.1, 5.2, 5.3, 5.4 SUSE Linux Enterprise Micro for Rancher 5.2, 5.3, 5.4 SUSE Linux Enterprise Real Time 15 SP4, 15 SP7 SUSE Linux Enterprise Server 12 SP5, 15 SP3, 15 SP4, 15 SP7 SUSE Linux Enterprise Server for SAP Applications 12 SP5, 15 SP3, 15 SP4, 15 SP7
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.suse.com/support/update/announcement/2025/suse-su-202503363-1/ • https://www.suse.com/support/update/announcement/2025/suse-su-202503362-1/ • https://www.suse.com/support/update/announcement/2025/suse-su-202503370-1/ • https://www.suse.com/support/update/announcement/2025/suse-su-202503374-1/ • https://www.suse.com/support/update/announcement/2025/suse-su-202503375-1/ • https://www.suse.com/support/update/announcement/2025/suse-su-202503379-1/ • https://www.suse.com/support/update/announcement/2025/suse-su-202503382-1/ • https://www.suse.com/support/update/announcement/2025/suse-su-202503383-1/ • https://www.suse.com/support/update/announcement/2025/suse-su-202503384-1/ • https://www.suse.com/support/update/announcement/2025/suse-su-202503381-1/

Affected Product	**Cisco**
Severity	**Medium**
Affected Vulnerability	Security Update (CVE-2025-20365)
Description	Cisco has released security updates addressing a Vulnerability that exists in their products. **CVE-2025-20365 -** This vulnerability is due to a logic error in the processing of IPv6 RA packets that are received from wireless clients. An attacker could exploit this vulnerability by associating to a wireless network and sending a series of crafted IPv6 RA packets. A successful exploit could allow the attacker to temporarily change the IPv6 gateway of an affected device. This could also lead to intermittent packet loss for any wireless clients that are associated with the affected device. Cisco advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Following products which are running on Cisco WLC IOS XE Software versions 17.15 and prior. • 6300 Series Embedded Services Access Points (APs) • Aironet 1540 Series APs • Aironet 1560 Series APs • Aironet 1800 Series APs • Aironet 2800 Series APs • Aironet 3800 Series APs • Aironet 4800 APs • Catalyst 9100 APs • Catalyst IW6300 Heavy Duty Series APs • Integrated APs on1100 Integrated Services Routers (ISRs)
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ap-ipv6-gw-tUAzpn9O

Affected Product	**Red Hat**
Severity	**Medium**
Affected Vulnerability	Security Update (CVE-2025-38472, CVE-2025-38527, CVE-2025-38718, CVE-2025-39682, CVE-2025-39698)
Description	Red Hat 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. 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 9 x86_64 Red Hat Enterprise Linux for x86_64 - Extended Update Support 9.6 x86_64 Red Hat Enterprise Linux Server - AUS 9.6 x86_64 Red Hat Enterprise Linux for IBM z Systems 9 s390x Red Hat Enterprise Linux for IBM z Systems - Extended Update Support 9.6 s390x Red Hat Enterprise Linux for Power, little endian 9 ppc64le Red Hat Enterprise Linux for Power, little endian - Extended Update Support 9.6 ppc64le Red Hat Enterprise Linux for ARM 64 9 aarch64 Red Hat Enterprise Linux for ARM 64 - Extended Update Support 9.6 aarch64 Red Hat Enterprise Linux Server for Power LE - Update Services for SAP Solutions 9.6 ppc64le Red Hat Enterprise Linux for x86_64 - Update Services for SAP Solutions 9.6 x86_64 Red Hat CodeReady Linux Builder for x86_64 9 x86_64 Red Hat CodeReady Linux Builder for Power, little endian 9 ppc64le Red Hat CodeReady Linux Builder for ARM 64 9 aarch64 Red Hat CodeReady Linux Builder for IBM z Systems 9 s390x Red Hat CodeReady Linux Builder for x86_64 - Extended Update Support 9.6 x86_64 Red Hat CodeReady Linux Builder for Power, little endian - Extended Update Support 9.6 ppc64le Red Hat CodeReady Linux Builder for IBM z Systems - Extended Update Support 9.6 s390x Red Hat CodeReady Linux Builder for ARM 64 - Extended Update Support 9.6 aarch64 Red Hat Enterprise Linux for ARM 64 - 4 years of updates 9.6 aarch64 Red Hat Enterprise Linux for IBM z Systems - 4 years of updates 9.6 s390x
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://access.redhat.com/errata/RHSA-2025:16880

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.