Advisory Alert

Alert Number: AAA20251126 **Date:** November 26, 2025

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
ASUS	**Critical**	Authentication Bypass Vulnerability
SUSE	**High**	Multiple Vulnerabilities
ASUS	**High**, Medium	Multiple Vulnerabilities
Oracle	**High**, Medium, Low	Multiple Vulnerabilities
Ubuntu	**Medium**	Multiple Vulnerabilities

Description

Affected Product	**ASUS**
Severity	**Critical**
Affected Vulnerability	Authentication Bypass Vulnerability (CVE-2025-59366)
Description	ASUS has released a security update addressing an Authentication Bypass Vulnerability that exists in AiCloud which affects ASUS Router Firmware. **CVE-2025-59366 -** A critical, unauthenticated bypass vulnerability in the AiCloud feature that can be exploited remotely to execute functions and gain high-level control over the router. ASUS advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	ASUS Router Firmware Series 3.0.0.4_386 / 3.0.0.4_388 / 3.0.0.6_102
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.asus.com/security-advisory

Affected Product	**SUSE**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-53673, CVE-2024-53141, CVE-2025-23145)
Description	SUSE has released security updates addressing multiple vulnerabilities that exist in in their products. **CVE-2023-53673** - Use-After-Free (UAF) vulnerability in the Linux kernel's Bluetooth implementation that allows a local user to cause system instability or potentially escalate privileges. **CVE-2024-53141** - vulnerability in the Linux netfilter ipset module that lacks a necessary range check, allowing a local user to cause memory corruption and potentially escalate privileges. **CVE-2025-23145** - Denial of Service (DoS) vulnerability in the Multipath TCP (MPTCP) implementation, where an unauthenticated remote attacker can trigger a NULL pointer dereference and crash the kernel. SUSE advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	openSUSE Leap 15.4 SUSE Linux Enterprise High Performance Computing 15 SP4 SUSE Linux Enterprise Live Patching 15-SP4 SUSE Linux Enterprise Micro 5.3 SUSE Linux Enterprise Micro 5.4 SUSE Linux Enterprise Real Time 15 SP4 SUSE Linux Enterprise Server 15 SP4 SUSE Linux Enterprise Server for SAP Applications 15 SP4
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.suse.com/support/update/announcement/2025/suse-su-20254237-1/ • https://www.suse.com/support/update/announcement/2025/suse-su-20254239-1/ • https://www.suse.com/support/update/announcement/2025/suse-su-20254233-1/

Affected Product	**ASUS**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-12003, CVE-2025-59370, CVE-2025-59371, CVE-2025-59365, CVE-2025-59372, CVE-2025-59368, CVE-2025-59369)
Description	ASUS has released security updates addressing multiple vulnerabilities that exist in their Router firmware. These vulnerabilities could be exploited by malicious users to compromise device integrity via file writing, execute arbitrary commands or network wide Denial of Service (DoS). ASUS advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	ASUS Router Firmware Series 3.0.0.4_386 / 3.0.0.4_388 / 3.0.0.6_102
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.asus.com/security-advisory

Affected Product	**Oracle**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2011-2964, CVE-2024-23337, CVE-2024-43374, CVE-2025-0624, CVE-2025-2361, CVE-2025-4476, CVE-2025-5399, CVE-2025-5914, CVE-2025-5992, CVE-2025-6069, CVE-2025-7039, CVE-2025-7462, CVE-2025-8194, CVE-2025-9179, CVE-2025-9230, CVE-2025-9232, CVE-2025-10527, CVE-2025-11001, CVE-2025-32989, CVE-2025-40778, CVE-2025-43023, CVE-2025-47183, CVE-2025-47806, CVE-2025-47910, CVE-2025-48060, CVE-2025-48379, CVE-2025-49014, CVE-2025-50181, CVE-2025-50420, CVE-2025-50422, CVE-2025-52886, CVE-2025-52891, CVE-2025-53014, CVE-2025-53066, CVE-2025-53537, CVE-2025-54571, CVE-2025-55005, CVE-2025-55188, CVE-2025-6141)
Description	Oracle has released security patches addressing multiple vulnerabilities that exist in their third party components that are included in Oracle Solaris. These vulnerabilities could be exploited by malicious users to compromise the affected system and even escalate into Remote Denial of Service (DoS) attacks. Oracle advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Oracle Solaris version 11.4 / 11.3 / 10
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.oracle.com/security-alerts/bulletinoct2025.html

Affected Product	**Ubuntu**
Severity	**Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-38678, CVE-2025-38616, CVE-2025-38227, CVE-2025-21729)
Description	Ubuntu has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to cause denial of service and privilege escalation. Ubuntu advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Ubuntu 24.04 and 22.04
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://ubuntu.com/security/notices/USN-7889-1

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.