Advisory Alert

Alert Number: AAA20250926 **Date:** September 26, 2025

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Cisco	**Critical**	Multiple Improper Input Validation Vulnerabilities
SUSE	**High**	Multiple Vulnerabilities
Cisco	**Medium**	Improper Input Validation Vulnerability
Ubuntu	**Medium**	Multiple Vulnerabilities

Description

Affected Product	**Cisco**
Severity	**Critical**
Affected Vulnerability	Multiple Improper Input Validation Vulnerabilities (CVE-2025-20333, CVE-2025-20363)
Description	Cisco has released security updates addressing multiple improper input validation vulnerabilities vulnerabilities that exist in their products. **CVE-2025-20333 -** A vulnerability in the VPN web server of Cisco Secure Firewall Adaptive Security Appliance (ASA) Software and Cisco Secure Firewall Threat Defense (FTD) Software could allow an authenticated, remote attacker to execute arbitrary code on an affected device. **CVE-2025-20363 -** A vulnerability in the web services of Cisco Secure Firewall Adaptive Security Appliance (ASA) Software, Cisco Secure Firewall Threat Defense (FTD) Software, Cisco IOS Software, Cisco IOS XE Software, and Cisco IOS XR Software could allow an unauthenticated, remote attacker (Cisco ASA and FTD Software) or authenticated, remote attacker (Cisco IOS, IOS XE, and IOS XR Software) with low user privileges to execute arbitrary code on an affected device. Cisco advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Cisco devices if they are running a release of Cisco Secure Firewall ASA Software or Cisco Secure FTD Software with vulnerable configurations. • SSL VPN • AnyConnect SSL VPN • Mobile User Security (MUS) • AnyConnect IKEv2 Remote Access (with client services) For information about which Cisco software releases are vulnerable configurations, see the possible vulnerable configuration sections of these advisories.
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-webvpn-z5xP8EUB • https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-http-code-exec-WmfP3h3O

Affected Product	**SUSE**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-38177, CVE-2025-38181, CVE-2025-38498)
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 SUSE Linux Enterprise High Performance Computing 15 SP3 SUSE Linux Enterprise Live Patching 15-SP3 SUSE Linux Enterprise Micro 5.1 SUSE Linux Enterprise Micro 5.2 SUSE Linux Enterprise Server 15 SP3 SUSE Linux Enterprise Server for SAP Applications 15 SP3
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.suse.com/support/update/announcement/2025/suse-su-202503359-1/

Affected Product	**Cisco**
Severity	**Medium**
Affected Vulnerability	Improper Input Validation Vulnerability (CVE-2025-20362)
Description	Cisco has released security updates addressing an input improper input validation vulnerability that exists in their products. **CVE-2025-20362 -** A vulnerability in the VPN web server of Cisco Secure Firewall Adaptive Security Appliance (ASA) Software and Cisco Secure Firewall Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to access restricted URL endpoints without authentication that should otherwise be inaccessible without authentication. Cisco advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Cisco devices if they are running a release of Cisco Secure Firewall ASA Software or Cisco Secure FTD Software with vulnerable configurations. • SSL VPN • AnyConnect SSL VPN • Mobile User Security (MUS) • AnyConnect IKEv2 Remote Access (with client services) For information about which Cisco software releases are vulnerable configurations, see the possible vulnerable configuration sections of these advisories.
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-webvpn-YROOTUW

Affected Product	**Ubuntu**
Severity	**Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-38542, CVE-2025-38540, CVE-2025-38516, CVE-2025-38515, CVE-2025-38514, CVE-2025-38513, CVE-2025-38498, CVE-2025-38467, CVE-2025-38466, CVE-2025-38465)
Description	Ubuntu 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. Ubuntu advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Ubuntu 20.04 Ubuntu 22.04
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://ubuntu.com/security/notices/USN-7774-1

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.