TLP: WHITE

Advisory Alert

Alert Number: AAA20250619 **Date:** June 19, 2025

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Broadcom VMware	**Critical**	Multiple Vulnerabilities
SUSE	**High**	Multiple Linux Kernel Vulnerabilities
Broadcom VMware	**High**	Multiple Vulnerabilities
Cisco	**High**, Medium	Multiple Vulnerabilities
Cpanel	**Medium**	Multiple Vulnerabilities

Description

Affected Product	**Broadcom VMware**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-1094, CVE-2024-10979, CVE-2024-7348, CVE-2023-2455, CVE-2023-5870, CVE-2024-10976, CVE-2024-10978, CVE-2022-41862, CVE-2024-10977, CVE-2024-3596, CVE-2023-37920, CVE-2022-42967, CVE-2025-22871)
Description	Broadcom 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. Broadcom advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	VMware Tanzu Greenplum Versions - Prior to 7.5.0
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/35843

Affected Product	**SUSE**
Severity	**High**
Affected Vulnerability	Multiple Linux Kernel Vulnerabilities
Description	SUSE has released security updates addressing multiple linux kernel 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-SP6 Development Tools Module 15-SP6 Legacy Module 15-SP6 OpenSUSE Leap 15.6 SUSE Linux Enterprise Desktop 15 SP6 SUSE Linux Enterprise High Availability Extension 15 SP6 SUSE Linux Enterprise Live Patching 15-SP6 SUSE Linux Enterprise Micro 5.1 SUSE Linux Enterprise Micro 5.2 SUSE Linux Enterprise Micro for Rancher 5.2 SUSE Linux Enterprise Real Time 15 SP6 SUSE Linux Enterprise Server 15 SP6 SUSE Linux Enterprise Server for SAP Applications 15 SP6 SUSE Linux Enterprise Workstation Extension 15 SP6
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.suse.com/support/update/announcement/2025/suse-su-202501995-1/ • https://www.suse.com/support/update/announcement/2025/suse-su-202502000-1/

Affected Product	**Broadcom VMware**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-49203, CVE-2025-22235, CVE-2025-31650, CVE-2025-22233, CVE-2025-31651, CVE-2025-46701)
Description	Broadcom 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. Broadcom advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	VMware Tanzu Data Lake Versions - Prior to 1.1.0
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/35849

Affected Product	**Cisco**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-20234, CVE-2025-20271)
Description	Cisco has released security updates addressing Multiple Vulnerabilities that exist in their products. **CVE-2025-20234** - A vulnerability in Universal Disk Format (UDF) processing of ClamAV could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. **CVE-2025-20271** - A vulnerability in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series Teleworker Gateway devices could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition in the Cisco AnyConnect service on an affected device. Cisco advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Secure Endpoint Connector for Linux Versions Prior to - 1.26.1 Secure Endpoint Connector for Mac Versions Prior to - 1.26.1 Secure Endpoint Connector for Windows Versions Prior to - 7.5.21, 8.4.5 Secure Endpoint Private Cloud Versions - 4.2.2 or Prior Versions Cisco Meraki MX Firmware Release Versions Prior to - 18.107.13, 18.211.6, 19.1.8
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-clamav-udf-hmwd9nDy • https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-sM5GCfm7

Affected Product	**Cpanel**
Severity	**Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-48976, CVE-2025-48988, CVE-2025-49125, CVE-2025-49124)
Description	Cpanel has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to cause authentication bypass, denial-of-service, untrusted search path, allocation of resources without limits or throttling. Cpanel advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	All versions of Tomcat through 10.1.41.
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://news.cpanel.com/easyapache4-v25-20-maintenance-and-security-release/

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.