Advisory Alert

Alert Number: AAA20260515 **Date:** May 15, 2026

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Cisco	**Critical**	Multiple Vulnerabilities
SUSE	**High**	Security Update
Broadcom	**High**	Privilege Escalation Vulnerability
PostgreSQL	**High**, **Medium**, **Low**	Multiple Vulnerabilities
HPE	**Medium**	Multiple Vulnerabilities

Description

Affected Product	**Cisco**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-20182, CVE-2026-20209, CVE-2026-20210, CVE-2026-20224)
Description	Cisco has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to compromise the affected systems. Cisco advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Cisco Catalyst SD-WAN Manager (All deployment types) Cisco Catalyst SD-WAN Controller (All deployment types)
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-rpa2-v69WY2SW • https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-mltvnps2-JxpWm7R

Affected Product	**SUSE**
Severity	**High**
Affected Vulnerability	Security Update (CVE-2026-43284)
Description	SUSE has released security updates addressing a vulnerability that exists in their products. **CVE-2026-43284**: In the Linux kernel, the following vulnerability has been resolved: xfrm: esp: avoid in-place decrypt on shared skb frags MSG_SPLICE_PAGES can attach pages from a pipe directly to an skb. TCP marks such skbs with SKBFL_SHARED_FRAG after skb_splice_from_iter(), so later paths that may modify packet data can first make a private copy. SUSE advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	openSUSE Leap 15.4 SUSE Linux Enterprise High Availability Extension 15 SP4 SUSE Linux Enterprise High Performance Computing 15 SP4 SUSE Linux Enterprise High Performance Computing ESPOS 15 SP4 SUSE Linux Enterprise High Performance Computing LTSS 15 SP4 SUSE Linux Enterprise Live Patching 15-SP4 SUSE Linux Enterprise Micro 5.3 and 5.4 SUSE Linux Enterprise Micro for Rancher 5.3 and 5.4 SUSE Linux Enterprise Real Time 15 SP4 SUSE Linux Enterprise Server 15 SP4 and 15 SP4 LTSS SUSE Linux Enterprise Server for SAP Applications 15 SP4 SUSE Manager Proxy 4.3 SUSE Manager Retail Branch Server 4.3 SUSE Manager Server 4.3
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.suse.com/support/update/announcement/2026/suse-su-20261857-1/

Affected Product	**Broadcom**
Severity	**High**
Affected Vulnerability	Privilege Escalation Vulnerability (CVE-2026-41702)
Description	Broadcom has released a security update addressing a vulnerability that exists in their products. **CVE-2026-41702**: VMware Fusion contains a TOCTOU (Time-of-check Time-of-use) vulnerability that occurs during an operation performed by a SETUID binary. A malicious actor with local non-administrative user privileges may exploit this vulnerability to escalate privileges to root on the system where Fusion is installed. Broadcom advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	VMware Fusion
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/37454

Affected Product	**PostgreSQL**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-6472, CVE-2026-6473, CVE-2026-6474, CVE-2026-6475, CVE-2026-6476, CVE-2026-6477, CVE-2026-6478, CVE-2026-6479, CVE-2026-6575, CVE-2026-6637, CVE-2026-6638)
Description	PostgreSQL has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to compromise the affected systems. PostgreSQL advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	PostgreSQL versions prior to: • 18.4 • 17.10 • 16.14 • 15.18 • 14.23
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.postgresql.org/about/news/postgresql-184-1710-1614-1518-and-1423-released-3297/

Affected Product	**HPE**
Severity	**Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-54510, CVE-2025-54502)
Description	HPE has released security updates addressing multiple vulnerabilities that exist in their products. **CVE-2025-54510**: A potential security vulnerability has been identified in certain HPE SimpliVity servers using certain AMD EPYC processors. This vulnerability could be locally exploited to allow compromise of system integrity. For more information on this vulnerability, please see AMD Security Bulletin AMD-SB-3034 – SEV-SNP Routing Misconfiguration. **CVE-2025-54502**: A potential security vulnerability has been identified in certain HPE SimpliVity servers using certain AMD EPYC processors. This vulnerability could be locally exploited to allow arbitrary code execution. For more information on this vulnerability, please see AMD Security Bulletin AMD-SB-7054 – Incorrect use of LocateProtocol Service of the EFI_BOOT_Services table in SMI Handler. HPE advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	HPE SimpliVity 325 Gen10 Plus - Prior to SimpliVity Gen10 Support Pack 2026-0417 HPE SimpliVity 325 Gen10 - Prior to SimpliVity Gen 10 Support Pack 2026-0417
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbhf05042en_us&docLocale=en_US • https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbhf05041en_us&docLocale=en_US

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.