Advisory Alert

Alert Number: AAA20250717 **Date:** July 17, 2025

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Broadcom VMware	**Critical**	Multiple Vulnerabilities
Dell	**Critical**	Multiple Vulnerabilities
Cisco	**Critical**	Multiple Unauthenticated Remote Code Execution Vulnerabilities
Zyxel	**Critical**	Buffer Overflow Vulnerability
cPanel	**High**	Multiple Vulnerabilities
SUSE	**High**	Multiple Vulnerabilities
IBM	**High**	Stack-based Overflow Vulnerability
Red Hat	**High**, Medium	Multiple Vulnerabilities
Cisco	**High**, Medium	Multiple Vulnerabilities
Dell	**High**, Medium, Low	Multiple Vulnerabilities
Drupal	**Medium**	Multiple Vulnerabilities
F5	**Medium**	Arbitrary Code Execution Vulnerability

Description

Affected Product	**Broadcom VMware**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-41236, CVE-2025-41237, CVE-2025-41238, CVE-2025-41239)
Description	Broadcom has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to cause Remote Code Execution, Information disclosure. Broadcom advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	VMware Cloud Foundation - 4.5.x, 5.x, VMware vSphere Foundation ESX - 9.0.0.0 VMware ESXi - 7.0, 8.0 VMware Workstation - 17.x VMware Fusion - 13.x VMware Tools [1] - 12.x.x, 11.x.x, 13.x.x VMware Telco Cloud Platform - 3.x, 2.x VMware Telco Cloud Infrastructure - 3.x, 2.x
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/35877

Affected Product	**Dell**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-24813, CVE-2024-38286)
Description	Dell has released a security update addressing multiple vulnerabilities that exist in their product. These vulnerabilities could be exploited by malicious users to cause Remote Code Execution and/or Information disclosure, OutOfMemoryError by abusing the TLS handshake process. Dell advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Dell Data Protection Central - Version prior to 19.12.0-2
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.dell.com/support/kbdoc/en-us/000345812/dsa-2025-286-security-update-for-dell-data-protection-central-multiple-third-party-component-vulnerabilities

Affected Product	**Cisco**
Severity	**Critical**
Affected Vulnerability	Multiple Unauthenticated Remote Code Execution Vulnerabilities (CVE-2025-20281, CVE-2025-20282, CVE-2025-20337)
Description	Cisco has released security updates addressing multiple unauthenticated remote code execution vulnerabilities that exist in their products. **CVE-2025-20281, CVE-2025-20337** - These vulnerabilities in a specific API of Cisco ISE and Cisco ISE-PIC could allow an unauthenticated, remote attacker to execute arbitrary code on the underlying operating system with root privileges. The attacker does not require valid credentials to exploit these vulnerabilities. **CVE-2025-20282** - This vulnerability is due a lack of file validation checks that would prevent uploaded files from being placed in privileged directories on an affected system. An attacker could exploit this vulnerability by uploading a crafted file to the affected device. A successful exploit could allow the attacker to store malicious files on the affected system and then execute arbitrary code or obtain root privileges on the system. Cisco advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Cisco ISE and ISE-PIC releases 3.3 and 3.4
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ise-unauth-rce-ZAd2GnJ6

Affected Product	**Zyxel**
Severity	**Critical**
Affected Vulnerability	Buffer Overflow Vulnerability (CVE-2025-7673)
Description	Zyxel has released a security update addressing a buffer overflow vulnerability that exists in their products. **CVE-2025-7673** - The buffer overflow vulnerability in the URL parser of the zhttpd web server on certain CPE models could allow an unauthenticated attacker to cause DoS conditions and potentially execute arbitrary code by sending a specially crafted HTTP request. Zyxel advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	EMG3525-T50B EMG5523-T50B EMG5723-T50K EMG6726-B10A EX3510-B0 EX5510-B0 VMG1312-T20B VMG3625-T50B VMG3925-B10B / B10C VMG3927-B50A / B60A VMG3927-B50B VMG3927-T50K VMG4005-B50B VMG4927-B50A VMG8623-T50B VMG8825-B50A / B60A VMG8825-Bx0B VMG8825-T50K VMG8924-B10D XMG3927-B50A XMG8825-B50A
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-remote-code-execution-and-denial-of-service-vulnerabilities-of-cpe-07-16-2025

Affected Product	**cPanel**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-32023, CVE-2025-48367)
Description	cPanel has released security updates addressing multiple vulnerabilities that exist in their products. **CVE-2025-32023** - An authenticated user may use a specially crafted string to trigger a stack/heap out of bounds write on hyperloglog operations, potentially leading to remote code execution. **CVE-2025-48367** – An in-memory database that persists on disk. An unauthenticated connection can cause repeated IP protocol errors, leading to client starvation and, ultimately, a denial of service. cPanel advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	All versions of Redis through 6.2.18
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://news.cpanel.com/easyapache4-v25-23-maintenance-and-security-release/

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 affected systems. SUSE advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	openSUSE Leap 15.6 SUSE Linux Enterprise Live Patching 15-SP6 SUSE Linux Enterprise Real Time 15 SP6 SUSE Linux Enterprise Server 15 SP6 SUSE Linux Enterprise Server for SAP Applications 15 SP6 SUSE Real Time Module 15-SP6 SUSE Linux Enterprise High Performance Computing 12 SP5 SUSE Linux Enterprise Live Patching 12-SP5 SUSE Linux Enterprise Server 12 SP5 SUSE Linux Enterprise Server 12 SP5 LTSS SUSE Linux Enterprise Server 12 SP5 LTSS Extended Security SUSE Linux Enterprise Server for SAP Applications 12 SP5 SUSE Linux Enterprise Live Patching 15-SP7 SUSE Linux Enterprise Real Time 15 SP7 SUSE Linux Enterprise Server 15 SP7 SUSE Linux Enterprise Server for SAP Applications 15 SP7 SUSE Real Time Module 15-SP7
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.suse.com/support/update/announcement/2025/suse-su-202502335-1/ • https://www.suse.com/support/update/announcement/2025/suse-su-202502334-1/ • https://www.suse.com/support/update/announcement/2025/suse-su-202502333-1/

Affected Product	**IBM**
Severity	**High**
Affected Vulnerability	Stack-based Overflow Vulnerability (CVE-2025-36097)
Description	IBM has released a security update to address a stack-based overflow vulnerability that exists in their products. IBM WebSphere Application Server and WebSphere Application Server Liberty are vulnerable to a denial of service, caused by a stack-based overflow. An attacker can send a specially crafted request that cause the server to consume excessive memory resources. IBM advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	IBM WebSphere Application Server Liberty - 17.0.0.3-25.0.0.7 IBM WebSphere Application Server - 9.0
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/7239856

Affected Product	**Red Hat**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-22004, CVE-2022-50066, CVE-2022-49058, CVE-2024-58002, CVE-2024-57980, CVE-2025-21991, CVE-2025-23150, CVE-2025-37738, CVE-2022-49788)
Description	Red Hat has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to compromise affected systems. 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 8 x86_64 Red Hat Enterprise Linux for IBM z Systems 8 s390x Red Hat Enterprise Linux for Power, little endian 8 ppc64le Red Hat Enterprise Linux for ARM 64 8 aarch64 Red Hat CodeReady Linux Builder for x86_64 8 x86_64 Red Hat CodeReady Linux Builder for Power, little endian 8 ppc64le Red Hat CodeReady Linux Builder for ARM 64 8 aarch64 Red Hat Enterprise Linux Server - Extended Life Cycle Support 7 x86_64 Red Hat Enterprise Linux Server - Extended Life Cycle Support (for IBM z Systems) 7 s390x Red Hat Enterprise Linux Server - Extended Life Cycle Support for IBM Power, big endian 7 ppc64 Red Hat Enterprise Linux Server - Extended Life Cycle Support for IBM Power, little endian 7 ppc64le
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://access.redhat.com/errata/RHSA-2025:11358 • https://access.redhat.com/errata/RHSA-2025:11298

Affected Product	**Cisco**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-20274, CVE-2025-20272, CVE-2025-20283, CVE-2025-20284, CVE-2025-20285, CVE-2025-20288)
Description	Cisco has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to cause remote code execution, blind SQL injection, and server-side request forgery. Cisco advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Cisco Unified Intelligence Center - 12.5, 12.6 Cisco Unified CCX - 12.5(1)SU3 and earlier Cisco EPNM - 7.1 and earlier, 8,0, 8.1 Cisco Prime Infrastructure - 3.9 and earlier, 3.10 Cisco ISE or ISE-PIC - 3.3, 3.4, 3.2 and earlier
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cuis-file-upload-UhNEtStm • https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-piepnm-bsi-25JJqsbb • https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ise-multi-3VpsXOxO • https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cuis-ssrf-JSuDjeV

Affected Product	**Dell**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities
Description	Dell has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to compromise affected systems. Dell advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	PowerEdge T40 - Versions prior to 1.20.0 Data Protection Central - Versions 19.8. through 19.12.1 PowerEdge R6615 – BIOS versions prior to 1.11.2 PowerEdge R7615 – BIOS versions prior to 1.11.2 PowerEdge R6625 – BIOS versions prior to 1.11.2 PowerEdge R7625 – BIOS versions prior to 1.11.2 PowerEdge C6615 – BIOS versions prior to 1.6.2 PowerEdge R6515 – BIOS versions prior to 2.19.0 PowerEdge R6525 – BIOS versions prior to 2.19.0 PowerEdge R7515 – BIOS versions prior to 2.19.0 PowerEdge R7525 – BIOS versions prior to 2.19.0 Connectrix B-Series – SANnav - Versions prior to 2.4.0 Connectrix B-Series – FOS - Versions 9.1.0 through 9.2.2
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.dell.com/support/kbdoc/en-us/000345850/dsa-2025-289-security-update-for-dell-poweredge-t40-mini-tower-server-for-multiple-ami-bios-vulnerabilities • https://www.dell.com/support/kbdoc/en-us/000345824/dsa-2025-288-security-update-for-dell-data-protection-central-multiple-third-party-component-vulnerabilities • https://www.dell.com/support/kbdoc/en-us/000345844/dsa-2025-181-security-update-for-dell-amd-based-poweredge-server-vulnerabilities • https://www.dell.com/support/kbdoc/en-us/000345805/dsa-2025-282-security-update-for-dell-connectrix-b-series-sannav-and-fos-brocade-vulnerabilities

Affected Product	**Drupal**
Severity	**Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-7716, CVE-2025-7715)
Description	Drupal has released security updates addressing multiple vulnerabilities that exist in their products. **CVE-2025-7392** - A stored XSS vulnerability in the Real-time SEO module allows users with permissions to edit content to inject malicious JavaScript via SEO fields. This code then runs when other users or administrators view these fields, potentially compromising account access or session data. **CVE-2025-7715** - The module does not sufficiently validate the provided attributes, which makes it possible to insert JavaScript event attributes such as onmouseover, onkeyup, etc. These attributes can execute JavaScript code when the page is rendered, leading to cross-site scripting (XSS) vulnerabilities. Drupal advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Block Attributes - prior to 1.1.0, or versions from 2.0.0 Real-time SEO for Drupal - Versions prior to 2.2.0
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.drupal.org/sa-contrib-2025-091 • https://www.drupal.org/sa-contrib-2025-090

Affected Product	**F5**
Severity	**Medium**
Affected Vulnerability	Arbitrary Code Execution Vulnerability (CVE-2023-39323)
Description	F5 has released a security update addressing an arbitrary code execution vulnerability that exists in their products. **CVE-2023-39323** - Line directives ("//line") can be used to bypass the restrictions on "//go:cgo_" directives, allowing blocked linker and compiler flags to be passed during compilation. This can result in unexpected execution of arbitrary code when running "go build". The line directive requires the absolute path of the file in which the directive lives, which makes exploiting this issue significantly more complex. F5 advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	BIG-IP Next SPK - 1.7.0 - 1.9.2, 2.0.0 - 2.0.1 BIG-IP Next CNF - 1.1.0 - 1.4.1, 2.0.0 - 2.0.1 BIG-IP Next for Kubernetes - 2.0.0
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://my.f5.com/manage/s/article/K000152607

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.