Advisory Alert

Alert Number: AAA20260604 **Date:** June 4, 2026

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Red Hat	**Critical**	Multiple Vulnerabilities
cPanel	**Critical**	Remote Denial-of-Service Vulnerability
Cisco	**Critical**	Server-Side Request Forgery Vulnerability
Red Hat	**High**	Multiple Vulnerabilities
SUSE	**High**	Multiple Vulnerabilities
NetApp	**Medium**	Multiple Vulnerabilities
IBM	**Medium**	Denial of Service Vulnerability
Cisco	**Medium**	Multiple Vulnerabilities

Description

Affected Product	**Red Hat**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-1933, CVE-2026-2340, CVE-2026-3012, CVE-2026-4480, CVE-2026-40170, CVE-2026-4408)
Description	Red Hat has released a security update addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to compromise the affected systems. Red Hat advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	• Red Hat Enterprise Linux for x86_64 10 x86_64 • Red Hat Enterprise Linux for x86_64 - Extended Update Support 10.2 x86_64 • Red Hat Enterprise Linux for IBM z Systems 10 s390x • Red Hat Enterprise Linux for IBM z Systems - Extended Update Support 10.2 s390x • Red Hat Enterprise Linux for Power, little endian 10 ppc64le • Red Hat Enterprise Linux for Power, little endian - Extended Update Support 10.2 ppc64le • Red Hat Enterprise Linux for ARM 64 10 aarch64 • Red Hat Enterprise Linux for ARM 64 - Extended Update Support 10.2 aarch64 • Red Hat CodeReady Linux Builder for x86_64 10 x86_64 • Red Hat CodeReady Linux Builder for Power, little endian 10 ppc64le • Red Hat CodeReady Linux Builder for ARM 64 10 aarch64 • Red Hat CodeReady Linux Builder for IBM z Systems 10 s390x • Red Hat CodeReady Linux Builder for x86_64 - Extended Update Support 10.2 x86_64 • Red Hat CodeReady Linux Builder for Power, little endian - Extended Update Support 10.2 ppc64le • Red Hat CodeReady Linux Builder for IBM z Systems - Extended Update Support 10.2 s390x • Red Hat CodeReady Linux Builder for ARM 64 - Extended Update Support 10.2 aarch64 • Red Hat Enterprise Linux for ARM 64 - 4 years of updates 10.2 aarch64 • Red Hat Enterprise Linux for IBM z Systems - 4 years of updates 10.2 s390x • Red Hat Enterprise Linux for Power, little endian - 4 years of support 10.2 ppc64le • Red Hat Enterprise Linux for x86_64 - 4 years of updates 10.2 x86_64 • Red Hat Enterprise Linux for x86_64 - Extended Life Cycle 10.2 x86_64 • Red Hat Enterprise Linux for ARM 64 - Extended Life Cycle 10.2 aarch64 • Red Hat Enterprise Linux for Power, little endian - Extended Life Cycle 10.2 ppc64le • Red Hat Enterprise Linux for IBM z Systems - Extended Life Cycle 10.2 s390x
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://access.redhat.com/errata/RHSA-2026:22963

Affected Product	**cPanel**
Severity	**Critical**
Affected Vulnerability	Remote Denial-of-Service Vulnerability (CVE-2026-49975)
Description	cPanel has released a security update addressing a vulnerability that exists in their products. **CVE-2026-49975**: HTTP/2 Bomb, is a remote denial-of-service exploit against most major web servers, including: nginx, Apache httpd, Microsoft IIS, Envoy, Cloudflare Pingor. The vulnerable behavior exists in each server's default HTTP/2 configuration. cPanel advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	EasyApache 25.64 • ea-apache24 version 2.4.67-2
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://docs.cpanel.net/changelogs/easyapache-4-change-log-25/

Affected Product	**Cisco**
Severity	**Critical**
Affected Vulnerability	Server-Side Request Forgery Vulnerability (CVE-2026-20230)
Description	Cisco has released a security update addressing a vulnerability that exists in their products. **CVE-2026-20230**: A vulnerability in Cisco Unified Communications Manager (Unified CM) and Cisco Unified Communications Manager Session Management Edition (Unified CM SME) could allow an unauthenticated, remote attacker to conduct server-side request forgery (SSRF) attacks through an affected device. Cisco advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	If WebDialer Service is enabled: • Cisco Unified CM • Unified CM SME
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cucm-ssrf-cXPnHcW

Affected Product	**Red Hat**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-39766, CVE-2026-23270, CVE-2026-31419, CVE-2026-43037, CVE-2026-43038, CVE-2026-31709, CVE-2026-43163)
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 the affected systems. Red Hat advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	• Red Hat Enterprise Linux Server - AUS 9.2 x86_64 • Red Hat Enterprise Linux Server for Power LE - Update Services for SAP Solutions 9.2 ppc64le • Red Hat Enterprise Linux for x86_64 - Update Services for SAP Solutions 9.2 x86_64 • Red Hat Enterprise Linux for ARM 64 - 4 years of updates 9.2 aarch64 • Red Hat Enterprise Linux for IBM z Systems - 4 years of updates 9.2 s390x • Red Hat Enterprise Linux for x86_64 - Extended Life Cycle 9.2 x86_64 • Red Hat Enterprise Linux for ARM 64 - Extended Life Cycle 9.2 aarch64 • Red Hat Enterprise Linux for Power, little endian - Extended Life Cycle 9.2 ppc64le • Red Hat Enterprise Linux for IBM z Systems - Extended Life Cycle 9.2 s390x
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://access.redhat.com/errata/RHSA-2026:22940

Affected Product	**SUSE**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-20585, CVE-2025-40219, CVE-2025-54518, CVE-2025-68310, CVE-2025-71183, CVE-2025-71238, CVE-2026-23168, CVE-2026-23209, CVE-2026-23236, CVE-2026-23237, CVE-2026-23239, CVE-2026-23240, CVE-2026-23245, CVE-2026-23246, CVE-2026-23253, CVE-2026-23260, CVE-2026-23261, CVE-2026-23262, CVE-2026-23264, CVE-2026-23266, CVE-2026-23268, CVE-2026-23269, CVE-2026-23271, CVE-2026-23273, CVE-2026-23276, CVE-2026-23279, CVE-2026-23290, CVE-2026-23291, CVE-2026-23298, CVE-2026-23300, CVE-2026-23304, CVE-2026-23306, CVE-2026-23307, CVE-2026-23308, CVE-2026-23312, CVE-2026-23313, CVE-2026-23315, CVE-2026-23318, CVE-2026-23321, CVE-2026-23324, CVE-2026-23325, CVE-2026-23335, CVE-2026-23336, CVE-2026-23339, CVE-2026-23340, CVE-2026-23343, CVE-2026-23346, CVE-2026-23351, CVE-2026-23354, CVE-2026-23357, CVE-2026-23362, CVE-2026-23363, CVE-2026-23365, CVE-2026-23367, CVE-2026-23368, CVE-2026-23370, CVE-2026-23372, CVE-2026-23373, CVE-2026-23374, CVE-2026-23378, CVE-2026-23382, CVE-2026-23383, CVE-2026-23391, CVE-2026-23392, CVE-2026-23393, CVE-2026-23395, CVE-2026-23396, CVE-2026-23397, CVE-2026-23399, CVE-2026-23403, CVE-2026-23404, CVE-2026-23405, CVE-2026-23406, CVE-2026-23407, CVE-2026-23408, CVE-2026-23409, CVE-2026-23410, CVE-2026-23411, CVE-2026-23412, CVE-2026-23418, CVE-2026-23419, CVE-2026-23420, CVE-2026-23426, CVE-2026-23434, CVE-2026-23440, CVE-2026-23441, CVE-2026-23442, CVE-2026-23443, CVE-2026-23445, CVE-2026-23446, CVE-2026-23447, CVE-2026-23448, CVE-2026-23449, CVE-2026-23450, CVE-2026-23452, CVE-2026-23454, CVE-2026-23455, CVE-2026-23456, CVE-2026-23457, CVE-2026-23458, CVE-2026-23460, CVE-2026-23461, CVE-2026-23462, CVE-2026-23463, CVE-2026-23465, CVE-2026-23466, CVE-2026-23468, CVE-2026-23470, CVE-2026-23472, CVE-2026-23473, CVE-2026-23474, CVE-2026-23475, CVE-2026-31389, CVE-2026-31392, CVE-2026-31393, CVE-2026-31394, CVE-2026-31395, CVE-2026-31400, CVE-2026-31402, CVE-2026-31403, CVE-2026-31404, CVE-2026-31405, CVE-2026-31407, CVE-2026-31408, CVE-2026-31411, CVE-2026-31412, CVE-2026-31415, CVE-2026-31416, CVE-2026-31417, CVE-2026-31420, CVE-2026-31421, CVE-2026-31422, CVE-2026-31423, CVE-2026-31424, CVE-2026-31425, CVE-2026-31426, CVE-2026-31427, CVE-2026-31428, CVE-2026-31436, CVE-2026-31449, CVE-2026-31470, CVE-2026-31488, CVE-2026-31494, CVE-2026-31496, CVE-2026-31504, CVE-2026-31505, CVE-2026-31507, CVE-2026-31512, CVE-2026-31515, CVE-2026-31519, CVE-2026-31525, CVE-2026-31528, CVE-2026-31533, CVE-2026-31547, CVE-2026-31550, CVE-2026-31565, CVE-2026-31570, CVE-2026-31586, CVE-2026-31588, CVE-2026-31602, CVE-2026-31607, CVE-2026-31622, CVE-2026-31649, CVE-2026-31656, CVE-2026-31662, CVE-2026-31668, CVE-2026-31669, CVE-2026-31675, CVE-2026-31679, CVE-2026-31681, CVE-2026-31682, CVE-2026-31684, CVE-2026-31685, CVE-2026-31694, CVE-2026-31700, CVE-2026-31738, CVE-2026-31787, CVE-2026-43009, CVE-2026-43025, CVE-2026-43027, CVE-2026-43037, CVE-2026-43038, CVE-2026-43044, CVE-2026-43050, CVE-2026-43060, CVE-2026-43088, CVE-2026-43110, CVE-2026-43120, CVE-2026-43126, CVE-2026-43190, CVE-2026-43214, CVE-2026-43265, CVE-2026-43329, CVE-2026-43330, CVE-2026-43334, CVE-2026-43365, CVE-2026-43366, CVE-2026-43419, CVE-2026-43437, CVE-2026-43441, CVE-2026-43494, CVE-2026-43503, CVE-2026-46300)
Description	SUSE has released a security update addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to compromise the affected systems. SUSE advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	Basesystem Module 15-SP7 Development Tools Module 15-SP7 Legacy Module 15-SP7 Public Cloud Module 15-SP7 SUSE Linux Enterprise Desktop 15 SP7 SUSE Linux Enterprise High Availability Extension 15 SP7 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 Linux Enterprise Workstation Extension 15 SP7
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.suse.com/support/update/announcement/2026/suse-su-20262238-1/

Affected Product	**NetApp**
Severity	**Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-22054, CVE-2026-22055)
Description	NetApp has released security updates addressing multiple vulnerabilities that exist in their products. **CVE-2026-22054**: Active IQ Config Advisor version 6.7.3 contains hard-coded credentials that could allow an authenticated attacker with low privileges to perform unauthorized AutoSupport operations. **CVE-2026-22055**: Active IQ OneCollect version 2.7.3 contains hard-coded credentials that could allow an authenticated attacker with low privileges to perform unauthorized AutoSupport operations. NetApp advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	Active IQ OneCollect Active IQ Config Advisor
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://security.netapp.com/advisory/ntap-20260603-0001 https://security.netapp.com/advisory/ntap-20260603-0002

Affected Product	**IBM**
Severity	**Medium**
Affected Vulnerability	Denial of Service Vulnerability (CVE-2025-13867)
Description	IBM has released a security update addressing a vulnerability that exists in their products. **CVE-2025-13867**: IBM Db2 for Linux, UNIX and Windows (includes Db2 Connect Server) 11.5.0 through 11.5.9 and 12.1.0 through 12.1.3 could allow an authenticated user to cause a denial of service due to improper neutralization of special elements in data query logic IBM advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	IBM Db2 Server Edition Versions 11.5.0 to 11.5.9 and 12.1.0 to 12.1.4
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/7259963

Affected Product	**Cisco**
Severity	**Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-20233, CVE-2026-20175)
Description	Cisco has released security updates addressing multiple vulnerabilities that exist in their products. **CVE-2026-20233**: A vulnerability in the web-based user interface of Cisco Webex Meetings could have allowed an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack. **CVE-2026-20175**: A vulnerability in Cisco Finesse could allow an unauthenticated, remote attacker to load arbitrary files from remote locations into an active user session on an affected device, possibly leading to browser-based attacks. Cisco advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	Cisco Webex Meetings (Cloud-based) Cisco Finesse
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webex-xss-jw3NeQzS • https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-finesse-rfi-gwpkdc89

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.