Advisory Alert

Alert Number: **AAA20250821** **Date:** **August 21, 2025**

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
SUSE	**High**	Multiple Vulnerabilities
cPanel	**High, Medium**	Multiple Vulnerabilities
IBM	**High, Medium**	Multiple Vulnerabilities
Red Hat	**High, Medium, Low**	Multiple Vulnerabilities
Cisco	**Medium**	Multiple Vulnerabilities
F5	**Medium, Low**	Multiple Vulnerabilities

Description

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 the affected systems. SUSE advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Multiple Products
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.suse.com/support/update/announcement/2025/suse-su-202502932-1/ • https://www.suse.com/support/update/announcement/2025/suse-su-202502930-1/ • https://www.suse.com/support/update/announcement/2025/suse-su-202502926-1/ • https://www.suse.com/support/update/announcement/2025/suse-su-202502923-1/

Affected Product	**cPanel**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-27210, CVE-2025-54571)
Description	cPanel has released a security update addressing multiple vulnerabilities that exist in their products. **CVE-2025-27210** - An incomplete fix has been identified for CVE-2025-23084 in Node.js, specifically affecting Windows device names like CON, PRN, and AUX. This vulnerability affects Windows users of `path.join` API. **CVE-2025-54571** – ModSecurity is an open source, cross platform web application firewall (WAF) engine for Apache, IIS and Nginx. In versions 2.9.11 and below, an attacker can override the HTTP response's Content-Type, which could lead to several issues depending on the HTTP scenario. For example, we have demonstrated the potential for XSS and arbitrary script source code disclosure in the latest version of mod_security2. cPanel advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	EasyApache 4 – versions prior to 25.26
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://news.cpanel.com/easyapache4-v25-26-maintenance-and-security-release/

Affected Product	**IBM**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-27516, CVE-2024-47081, CVE-2025-50181, CVE-2025-50182, CVE-2025-47273, CVE-2025-36114, CVE-2025-48976)
Description	IBM has released security updates addressing multiple vulnerabilities in their products. If exploited, these vulnerabilities could lead to path traversal, security restriction bypass, denial of service attacks. IBM advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	IBM SOAR QRadar Plugin App - 1.0.0 - 5.6.0 IBM WebSphere Application Server - 8.5, 9.0 IBM WebSphere Application Server Liberty - 17.0.0.3 - 25.0.0.8
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.ibm.com/support/pages/node/7242665 • https://www.ibm.com/support/pages/node/7242666 • https://www.ibm.com/support/pages/node/7242664 • https://www.ibm.com/support/pages/node/7242088

Affected Product	**Red Hat**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-52425, CVE-2024-5535, CVE-2024-24795, CVE-2024-36387, CVE-2024-45490, CVE-2024-56171, CVE-2025-24928, CVE-2021-47670, CVE-2022-49788, CVE-2022-50020, CVE-2024-57980, CVE-2025-21928, CVE-2025-38086)
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 JBoss Core Services Text-Only Advisories x86_64 Red Hat Enterprise Linux Server - AUS 8.2 x86_64 Red Hat JBoss Core Services 1 for RHEL 8 x86_64 Red Hat JBoss Core Services 1 for RHEL 7 x86_64
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://access.redhat.com/errata/RHSA-2025:3453 • https://access.redhat.com/errata/RHSA-2025:14136 • https://access.redhat.com/errata/RHSA-2025:3452

Affected Product	**Cisco**
Severity	**Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-20269, CVE-2025-20345)
Description	Cisco has released security updates addressing multiple vulnerabilities that exist in their products. **CVE-2025-20269** - This vulnerability is due to insufficient input validation for specific HTTP requests. An attacker could exploit this vulnerability by sending crafted HTTP requests to the web-based management interface on an affected device. A successful exploit could allow the attacker to access sensitive files from the affected device. **CVE-2025-20345** - This vulnerability is due to insufficient masking of sensitive information before it is written to system log files. An attacker could exploit this vulnerability by accessing logs on an affected system. A successful exploit could allow the attacker to view sensitive information that should be restricted. Cisco advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Cisco EPNM - 7.1 and earlier, 8.0, 8.1 Cisco Prime Infrastructure - 3.9 and earlier, 3.10 Cisco Duo Authentication Proxy - 5.8.2 and earlier, 6.5.1 and earlier
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-pi-epnm-TET4GxBX • https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-authproxlog-SxczXQ63

Affected Product	**F5**
Severity	**Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2016-4448, CVE-2014-7822, CVE-2023-0662)
Description	F5 has released security updates addressing multiple vulnerabilities that exist in their products. **CVE-2016-4448** - Format string vulnerability in libxml2 before 2.9.4 allows attackers to have unspecified impact via format string specifiers in unknown vectors. **CVE-2014-7822** - An authenticated attacker may be able to cause a denial-of-service (DoS) attack, or other attack with an unspecified impact. This vulnerability is considered local, because it is exploitable only by an authenticated user that accesses the system by using the command line. **CVE-2023-0662** - This vulnerability allows authenticated attackers to consume a large amount of CPU time and trigger excessive logging, which can lead to a degradation of service or a denial-of-service (DoS) on the BIG-IP system. It impacts mostly the control plane, as PHP is used in the Configuration utility for POST uploads such as upgrading iApps, uploading iRules, and uploading UCS archives. F5 advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Multiple Products
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://my.f5.com/manage/s/article/K41103561 • https://my.f5.com/manage/s/article/K17237 • https://my.f5.com/manage/s/article/K000133753

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.