TLP: WHITE

Advisory Alert

Alert Number: AAA20250117 **Date:** January 17, 2025

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
cPanel	**High**	Multiple Vulnerabilities
Red Hat	**High**, **Medium**	Multiple Vulnerabilities

Description

Affected Product	**cPanel**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-46981, CVE-2024-51741)
Description	cPanel has released security updates addressing multiple vulnerabilities that exist in their products. **CVE-2024-46981 –** An authenticated user may use a specially crafted Lua script to manipulate the garbage collector and potentially lead to remote code execution. The problem is fixed in 7.4.2, 7.2.7, and 6.2.17. An additional workaround to mitigate the problem without patching the redis-server executable is to prevent users from executing Lua scripts. This can be done using ACL to restrict EVAL and EVALSHA commands. **CVE-2024-51741 –** Vulnerability in Redis, In-memory database that persists on disk. An Authenticated malicious user with sufficient privileges may create a malformed ACL selector which, when accessed, triggers a server panic and subsequent denial of service. cPanel advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	EasyApache 4 - All versions of Valkey through 7.2.7
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://news.cpanel.com/easyapache4-v25-2-maintenance-and-security-release/

Affected Product	**Red Hat**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-50379, CVE-2024-51127)
Description	Red Hat has released security updates addressing multiple vulnerabilities in their products. If exploited, these vulnerabilities could lead to remote code execution, arbitrary file overwriting, or unauthorized access to sensitive information. Red Hat advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	JBoss Enterprise Application Platform 8.0 for RHEL 8 x86_64 JBoss Enterprise Application Platform 8.0 for RHEL 9 x86_64 JBoss Enterprise Application Platform Text-Only Advisories x86_64 JBoss Enterprise Web Server 5 for RHEL 7 x86_64 JBoss Enterprise Web Server 5 for RHEL 8 x86_64 JBoss Enterprise Web Server 5 for RHEL 9 x86_64 JBoss Enterprise Web Server Text-Only Advisories x86_64
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://access.redhat.com/errata/RHSA-2025:0362 • https://access.redhat.com/errata/RHSA-2025:0361 • https://access.redhat.com/errata/RHSA-2025:0372 • https://access.redhat.com/errata/RHSA-2025:0371

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.