Advisory Alert

Alert Number: AAA20251223 **Date:** December 23, 2025

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
MongoDB	**High**	Improper Handling of Length Parameter Vulnerability
Red Hat	**Medium**	Multiple Vulnerabilities
Check Point	**Medium**	Multiple Information Disclosure Vulnerabilities

Description

Affected Product	**MongoDB**
Severity	**High**
Affected Vulnerability	Improper Handling of Length Parameter Vulnerability (CVE-2025-14847)
Description	MongoDB has released a security update addressing a vulnerability that exists in their products. **CVE-2025-14847:** A client-side exploit of the Server's zlib implementation can return uninitialized heap memory without authenticating to the server. MongoDB advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	MongoDB 8.2.0 through 8.2.3 MongoDB 8.0.0 through 8.0.16 MongoDB 7.0.0 through 7.0.26 MongoDB 6.0.0 through 6.0.26 MongoDB 5.0.0 through 5.0.31 MongoDB 4.4.0 through 4.4.29 All MongoDB Server v4.2 versions All MongoDB Server v4.0 versions All MongoDB Server v3.6 versions
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://jira.mongodb.org/browse/SERVER-115508

Affected Product	**Red Hat**
Severity	**Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-38729, CVE-2025-39757, CVE-2023-53178, CVE-2023-53297, CVE-2023-53322, CVE-2022-50367, CVE-2022-50356, CVE-2022-50403, CVE-2022-50410, CVE-2022-50406, CVE-2025-39955)
Description	Red Hat has released a security update addressing multiple vulnerabilities that are present 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 - 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-2025:23947

Affected Product	**Check Point**
Severity	**Medium**
Affected Vulnerability	Multiple Information Disclosure Vulnerabilities (CVE-2025-8304, CVE-2025-8305)
Description	Check Point has released a security update addressing multiple information disclosure vulnerabilities that exist in the Identity Awareness product. **CVE-2025-8304**: An authenticated local user can obtain information that allows claiming security policy rules of another user due to sensitive information being accessible in the Windows Registry keys for Check Point Identity Agent running on a Terminal Server. **CVE-2025-8305:** An authenticated local user can obtain information that allows claiming security policy rules of another user due to sensitive information being printed in plaintext in Identity Agent for Terminal Services debug files. Check Point advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	Identity Awareness versions: • R81.10 • R81.20 • R82 • R82.10
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://support.checkpoint.com/results/sk/sk184263 • https://support.checkpoint.com/results/sk/sk184264

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.