



Advisory Alert

Alert Number: AAA20241127

Date: November 27, 2024

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
IBM	High	Insufficient Verification of Data Authenticity Vulnerability
Oracle	High, Medium, Low	Multiple Vulnerabilities
Red Hat	Medium	Sensitive Information Disclosure Vulnerability

Description

Affected Product	IBM
Severity	High
Affected Vulnerability	Insufficient Verification of Data Authenticity Vulnerability (CVE-2023-37920)
Description	<p>IBM has released security updates addressing an Insufficient Verification of Data Authenticity Vulnerability that exists in IBM Storage Defender.</p> <p>CVE-2023-37920 - An unspecified error with the removal of e-Tugra root certificate in Certifi has an unknown impact and attack vector.</p> <p>IBM advises to apply security fixes at your earliest to protect systems from potential threats.</p>
Affected Products	IBM Storage Defender - Resiliency Service versions 2.0.0 - 2.0.8
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/7177222

Affected Product	Oracle
Severity	High, Medium, Low
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-41671, CVE-2024-24246, CVE-2024-38535, CVE-2024-6239, CVE-2024-9392, CVE-2024-9680, CVE-2024-36472, CVE-2024-6655, CVE-2024-40897, CVE-2020-35357, CVE-2024-7006, CVE-2024-0914, CVE-2024-6119, CVE-2023-52722, CVE-2024-38428, CVE-2024-37371, CVE-2023-52169, CVE-2024-41965, CVE-2024-5535, CVE-2024-35235, CVE-2023-48232, CVE-2024-37535, CVE-2024-43167, CVE-2024-31744, CVE-2024-45230, CVE-2024-8381, CVE-2024-42353)
Description	<p>Oracle has released security updates addressing multiple vulnerabilities that exist in Oracle Solaris. These vulnerabilities could be exploited by malicious users to compromise the affected system.</p> <p>Oracle advises to apply security fixes at your earliest to protect systems from potential threats.</p>
Affected Products	Oracle Solaris 11.4
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.oracle.com/security-alerts/bulletinOct2024.html

Affected Product	Red Hat
Severity	Medium
Affected Vulnerability	Sensitive Information Disclosure Vulnerability (CVE-2024-8883)
Description	<p>Red Hat has released security updates addressing a Sensitive Information Disclosure Vulnerability that exists in JBoss Enterprise Application Platform.</p> <p>CVE-2024-8883 - A misconfiguration flaw was found in Keycloak. This issue can allow an attacker to redirect users to an arbitrary URL if a 'Valid Redirect URI' is set to http://localhost or http://127.0.0.1, enabling sensitive information such as authorization codes to be exposed to the attacker, potentially leading to session hijacking.</p> <p>Red Hat advises to apply security fixes at your earliest to protect systems from potential threats.</p>
Affected Products	JBoss Enterprise Application Platform Text-Only Advisories x86_64 JBoss Enterprise Application Platform 8.0 for RHEL 9 x86_64 JBoss Enterprise Application Platform 8.0 for RHEL 8 x86_64
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	<ul style="list-style-type: none"> https://access.redhat.com/errata/RHSA-2024:10385 https://access.redhat.com/errata/RHSA-2024:10386

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.