Advisory Alert

Alert Number: AAA20230601 **Date:** June 1, 2023

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Drupal	**High**	Multiple Vulnerabilities
RedHat	**High**	Multiple Vulnerabilities
IBM	**High**, Medium	Multiple Vulnerabilities

Description

Affected Product	**Drupal**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities
Description	Drupal has released security patch updates addressing multiple vulnerabilities in Drupal Modules. These vulnerabilities, identified as Cross-Site Scripting (XSS), Access Bypass. Exploiting these vulnerabilities could lead to unauthorized access, data breaches, and potential compromise of the entire website. Drupal recommends to apply the necessary patch updates at your earliest to avoid issues.
Affected Products	AddToAny Share Buttons module for Drupal 9.4+ or 10 AddToAny Share Buttons module for Drupal versions before 9.4 Consent Popup before 1.0.3 Iubenda Integration module for Drupal 7 Iubenda Integration module for Drupal 9+
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.drupal.org/sa-contrib-2023-019 https://www.drupal.org/sa-contrib-2023-018 https://www.drupal.org/sa-contrib-2023-017 https://www.drupal.org/sa-contrib-2023-016

Affected Product	**RedHat**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2022-2414, CVE-2022-2393)
Description	Redhat has released security updates addressing multiple vulnerabilities that exists in The Public Key Infrastructure (PKI) Core is an essential component of Red Hat Certificate System. **CVE-2022-2414** - The pki-core module is vulnerable to XML External Entity (XXE) attacks, which could allow an attacker to access external entities during XML parsing. **CVE-2022-2393** - In the caServerKeygen_DirUserCert profile, a user can obtain certificates for other User IDs (UIDs) by entering their name in the Subject field. Redhat recommends to apply the necessary patch updates at your earliest to avoid issues.
Affected Products	Red Hat Enterprise Linux for x86_64 - Extended Update Support 8.6 x86_64 Red Hat Enterprise Linux Server - AUS 8.6 x86_64 Red Hat Enterprise Linux for IBM z Systems - Extended Update Support 8.6 s390x Red Hat Enterprise Linux for Power, little endian - Extended Update Support 8.6 ppc64le Red Hat Enterprise Linux Server - TUS 8.6 x86_64 Red Hat Enterprise Linux for ARM 64 - Extended Update Support 8.6 aarch64 Red Hat Enterprise Linux Server for Power LE - Update Services for SAP Solutions 8.6 ppc64le Red Hat Enterprise Linux for x86_64 - Update Services for SAP Solutions 8.6 x86_64
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://access.redhat.com/errata/RHSA-2023:3394

Affected Product	**IBM**
Severity	**High**, Medium
Affected Vulnerability	Multiple vulnerabilities (CVE-2023-25690, CVE-2022-25881, CVE-2022-25901, CVE-2022-43441)
Description	IBM has released security updates addressing multiple vulnerabilities that exist in the QRadar SIEM. The vulnerabilities could be exploited by remote attackers to bypass access controls, perform cache poisoning, and cause denial of service conditions **CVE-2023-25690** - Apache HTTP Server, as utilized by IBM QRadar SIEM, is susceptible to HTTP request splitting attacks. Exploitation of this flaw could allow a remote attacker to bypass access controls in the proxy server, proxy unintended URLs to existing origin servers, and potentially perform cache poisoning. **CVE-2022-25881, CVE-2022-25901, CVE-2022-43441** - Denial of service conditions in the QRadar Pulse application add-on, integrated with IBM QRadar SIEM it could be exploited by remote attackers. IBM recommends to apply the necessary patch updates at your earliest to avoid issues.
Affected Products	IBM QRadar SIEM versions 7.5.0 - 7.5.0 UP5 IBM QRadar Pulse App versions 1.0.0 - 2.2.9
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/6999241 https://www.ibm.com/support/pages/node/6999287

Disclaimer

The information provided herein is on "as is" basis, without warranty of any kind. FinCSIRT highly recommend to follow the company policies and procedures when applying the necessary patches with thorough testing and ensuring proper roll-back capabilities exists.