Advisory Alert

Alert Number: AAA20210916 **Date:** September 16, 2021

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Drupal core	**Critical**	**Multiple Vulnerabilities**
Apache	**High**	**Denial of Service**
Redhat	**Medium**	**Multiple Vulnerabilities**

Description

Affected Product	**Drupal core**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2020-13673, CVE-2020-13674, CVE-2020-13675, CVE-2020-13676, CVE-2020-13677)
Description	CVE-2020-13677 - The Drupal core JSON API module doesn't restrict access as expected to certain substance, which might bring about accidental access bypass. CVE-2020-13676 - The QuickEdit module doesn't check access to fields as expected in certain conditions, which can prompt accidental disclosure of field data. CVE-2020-13675 - Drupal's JSON API and REST/File modules allow file uploads through their HTTP APIs. CVE-2020-13674 - The QuickEdit module doesn't validate access to routes as expected, this scenario could allow cross site request forgery under certain conditions and lead to potential data integrity issues. CVE-2020-13673- Drupal core Media allow embedding content fields in internal and external media. In specific conditions, the filter could allow an unprivileged user to inject HTML into a page when it is accessed by an accessible in users with authorization to embed media.
Affected Products	Drupal 9.2 Drupal 9.1 Drupal 8.2 Drupal 8.9
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.drupal.org/sa-core-2021-010 https://www.drupal.org/sa-core-2021-009 https://www.drupal.org/sa-core-2021-008 https://www.drupal.org/sa-core-2021-007 https://www.drupal.org/sa-core-2021-006

Affected Product	**Apache**
Severity	**High**
Affected Vulnerability	Denial of Service (CVE-2021-41079)
Description	Tomcat was configured to utilize NIO+OpenSSL or NIO2+OpenSSL for TLS, a specially created parcel could be utilized to trigger an infinite loop. as a result this could be a denial of service.
Affected Products	Apache Tomcat 10.0.0-M1 to 10.0.2 Apache Tomcat 9.0.0-M1 to 9.0.43 Apache Tomcat 8.5.0 to 8.5.6
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://tomcat.apache.org/security-10.html https://tomcat.apache.org/security-9.html https://tomcat.apache.org/security-8.html

Affected Product	**Redhat**
Severity	**Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2021-3653)
Description	A flaw was found in the KVM's AMD code for supporting SVM nested virtualization. This flaw could allow a malicious L1 guest to enable Advanced Virtual Interrupt Controller support (AVIC) for the L2 guest. Thus, the L2 guest would be permitted to read/write actual pages of the host, resulting in a crash of the entire system, leak of sensitive data or potential guest-to-host escape.
Affected Products	Multiple Products
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://access.redhat.com/errata/RHSA-2021:3548 https://access.redhat.com/security/cve/CVE-2021-3653

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.