Advisory Alert

Alert Number: AAA20220721 **Date:** July 21, 2022

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Cisco	**Critical**	Unauthorized Access Vulnerability
Cisco	**High**, **Medium**	Multiple vulnerabilities
Drupal	**High**, **Medium**	Multiple vulnerabilities
IBM	**Medium**	Information Disclosure Vulnerability

Description

Affected Product	**Cisco**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2022-20857, CVE-2022-20858, CVE-2022-20861)
Description	Cisco has released a security update addressing Multiple Vulnerabilities that exist in their Cisco Nexus Dashboard product. If exploited these vulnerabilities could cause an unauthenticated attacker to execute arbitrary commands, read or upload container image files, and perform a cross-site request forgery attack. Cisco highly recommends applying necessary security fixes at earliest to avoid issues
Affected Products	Cisco Nexus Dashboard 1.11 Cisco Nexus Dashboard 2.0 Cisco Nexus Dashboard 2.1 Cisco Nexus Dashboard 2.2
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ndb-mhcvuln-vpsBPJ9y

Affected Product	**Cisco**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple vulnerabilities (CVE-2022-20860, CVE-2022-20873, CVE-2022-20874, CVE-2022-20875, CVE-2022-20906, CVE-2022-20907, CVE-2022-20908, CVE-2022-20913, CVE-2022-20916)
Description	Cisco has released security updates addressing Multiple Vulnerabilities that exist in their products. Successful exploitation of these vulnerabilities could cause sensitive information disclosure, arbitrary code execution, execute denial of service attacks, execute cross site scripting and privilege escalation. Cisco highly recommends to apply necessary security fixes at earliest to avoid issues
Affected Products	Cisco Nexus Dashboard 1.1 Cisco Nexus Dashboard 2.0 Cisco Nexus Dashboard 2.1 Cisco Nexus Dashboard 2.2 RV110W Wireless-N VPN Firewall RV130 VPN Router RV130W Wireless-N Multifunction VPN Router RV215W Wireless-N VPN Router Cisco IoT Control Center, which is cloud based
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nd-tlsvld-TbAQLp3N https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv-rce-overflow-ygHByAK https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ndb-mprvesc-EMhDgXe5 https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ndb-afw-2MT9tb99 https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iotcc-xss-WQrCLRVd#vp

Affected Product	**Drupal**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2022-25277, CVE-2022-25276, CVE-2022-25278, CVE-2022-25275)
Description	Drupal has released security updates addressing multiple vulnerabilities that affect their products. **CVE-2022-25277** - Due a flaw in the Drupal Core if the files are uploaded with htaccess extension they would not be properly sanitized. This could allow bypassing the protections provided by Drupal core's default remote code execution on Apache web servers leading to arbitrary PHP remote code execution. **CVE-2022-25276**- Due to improper validations in iframe domain setting of Media oEmbed iframe, it allows embeds to be displayed in the context of the primary domain. Under certain circumstances, this could lead to cross-site scripting, leaked cookies, or other vulnerabilities. **CVE-2022-25278**- Drupal core form API evaluates form element access incorrectly under certain circumstances. This may lead to a user being able to alter data they should not have access to.No forms provided by Drupal core are known to be vulnerable. However, forms added through contributed or custom modules or themes may be affected. **CVE-2022-25275** -When creating derivative images using the image styles system, the Image module sometimes fails to properly check access to image files that are not kept in the standard public files directory. Drupal strongly advises to apply security fixes at earliest to avoid problems.
Affected Products	Drupal 9.4 Drupal 9.3 Drupal 7
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.drupal.org/sa-core-2022-014 https://www.drupal.org/sa-core-2022-015 https://www.drupal.org/sa-core-2022-013 https://www.drupal.org/sa-core-2022-012

Affected Product	**IBM**
Severity	**Medium**
Affected Vulnerability	Information Disclosure Vulnerability (CVE-2021-38936)
Description	IBM has issued a Security Update addressing an information disclosure vulnerability that exist IBM QRadar SIEM product. Using this vulnerability an attacker with system privileges can reveal highly sensitive information. IBM strongly advises to apply security fixes at earliest to avoid problems.
Affected Products	IBM QRadar SIEM 7.3 IBM QRadar SIEM 7.4 IBM QRadar SIEM 7.5
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/6605429

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.