Advisory Alert

Alert Number: AAA20210120 **Date:** January 20, 2022

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Drupal	**Critical**	Cross Site Scripting Vulnerabilities
Cisco	**Critical**	Multiple Vulnerabilities
Red Hat	**Medium**	Multiple Vulnerabilities

Description

Affected Product	**Drupal**
Severity	**Critical**
Affected Vulnerability	Cross Site Scripting Vulnerabilities (CVE-2021-41182, CVE-2021-41183, CVE-2016-7103, CVE-2010-5312)
Description	Drupal has released a security update addressing multiple vulnerabilities. The disclosed vulnerabilities allow a remote attacker to perform cross-site scripting (XSS) attacks. • **CVE-2021-41182**: XSS in the altField option of the Datepicker widget • **CVE-2021-41183**: XSS in *Text options of the Datepicker widget • **CVE-2016-7103**: XSS in closeText option of Dialog • **CVE-2010-5312**: XSS in the title option of Dialog (applicable only to the jQuery UI version included in D7 core) Drupal users are encouraged to upgrade to the latest versions.
Affected Products	Drupal 7, update to Drupal 7.86 Drupal 9.3, update to Drupal 9.3.3. Drupal 9.2, update to Drupal 9.2.11 Drupal 7, update to Drupal 7.86
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.drupal.org/sa-core-2022-001 https://www.drupal.org/sa-core-2022-002

Affected Product	**Cisco**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2022-20648, CVE-2022-20649, CVE-2022-20685, CVE-2022-20655)
Description	Cisco has released Security Updates addressing multiple vulnerabilities that exist with various cisco products such as Remote Code Execution Vulnerability, Information Disclosure Vulnerability, Denial of Service Vulnerability, and CLI Command Injection Vulnerability. It is highly recommended to apply necessary fixes at earliest to the cisco products to avoid issues
Affected Products	Cisco RCM for Cisco StarOS Software Cybervision Software Firepower Threat Defense (FTD) Software - All platforms Meraki MX Series Software 1000 Series Integrated Services Routers (ISRs) 4000 Series Integrated Services Routers (ISRs) Catalyst 8000V Edge Software Catalyst 8200 Series Edge Platforms Catalyst 8300 Series Edge Platforms Catalyst 8500 Series Edge Platforms Catalyst 8500L Series Edge Platforms Cloud Services Routers 1000V Integrated Services Virtual Routers (ISRv) ConfD Cisco Ultra Gateway Platform Cisco Enterprise NFV Infrastructure Software (NFVIS) Cisco Network Services Orchestrator (NSO) Cisco Virtual Topology System (VTS) Cisco Carrier Packet Transport Cisco SD-WAN vBond Software Cisco SD-WAN vEdge Routers Cisco SD-WAN vManage Software Cisco SD-WAN vSmart Software Cisco IOS XE SD-WAN Cisco IOS XR (64-Bit) Software
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rcm-vuls-7cS3Nuq https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-snort-dos-9D3hJLuj https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-confdcli-cmdinj-wybQDSSh https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cli-cmdinj-4MttWZPB

Affected Product	**Red Hat**
Severity	**Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2022-21248, CVE-2022-21277, CVE-2022-21282, CVE-2022-21283, CVE-2022-21291, CVE-2022-21293, CVE-2022-21294, CVE-2022-21296, CVE-2022-21299, CVE-2022-21305, CVE-2022-21340, CVE-2022-21341, CVE-2022-21360, CVE-2022-21365, CVE-2022-21366)
Description	Red Hat has released security updates for java-17-openjdk to address several vulnerabilities. It is highly recommended to apply necessary fixes provided on the official Red Hat website at the earliest to avoid these security issues, and all Red Hat users are encouraged to upgrade to the latest versions.
Affected Products	Red Hat Enterprise Linux for x86_64 8 x86_64 Red Hat Enterprise Linux for IBM z Systems 8 s390x Red Hat Enterprise Linux for Power, little endian 8 ppc64le Red Hat Enterprise Linux for ARM 64 8 aarch64 Red Hat CodeReady Linux Builder for x86_64 8 x86_64 Red Hat CodeReady Linux Builder for Power, little endian 8 ppc64le Red Hat CodeReady Linux Builder for ARM 64 8 aarch64 Red Hat CodeReady Linux Builder for IBM z Systems 8 s390x
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://access.redhat.com/errata/RHSA-2022:0161

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.