Advisory Alert

Alert Number : AAA20210422 **Date :** April 22, 2021

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Drupal	**Critical**	**Cross-site scripting**
IBM	**High**	**Prototype Pollution**
Cisco	**Medium**	**Multiple Vulnerabilities**
HP	**Medium**	**Denial of service**

Description

Affected Product	**Drupal**
Severity	**Critical**
Affected Vulnerability	Cross-site scripting
Description	Drupal core's sanitization API fails to properly filter cross-site scripting under difference situations. Proper configuration changes to prevent the exploit might be impractical and will vary between sites.Drupal recommend all sites are update to latest versions.
Affected Products	If you are using Drupal 9.1, update to Drupal 9.1.7. If you are using Drupal 9.0, update to Drupal 9.0.12. If you are using Drupal 8.9, update to Drupal 8.9.14. If you are using Drupal 7, update to Drupal 7.80.
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.drupal.org/sa-core-2021-002

Affected Product	**IBM**
Severity	**High**
Affected Vulnerability	Prototype Pollution (CVE-2020-5258)
Description	An affected versions of dojo (NPM package) the deepCopy method is vulnerable to Prototype Pollution. Prototype Pollution refers to the ability to inject properties into existing JavaScript language construct prototypes such as objects. An attacker manipulates these attributes to overwrite or pollute a JavaScript application object prototype of the base object by injecting other values.
Affected Products	WebSphere Application Server 7.0 WebSphere Application Server 8.0 WebSphere Application Server 8.5 WebSphere Application Server 9.0
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/6443101

Affected Product	**Cisco**
Severity	**Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2021-1491, CVE-2021-1481, CVE-2021-1483, CVE-2021-1484, CVE-2021-1482)
Description	Cisco has released security patch update addressing vulnerabilities that exist in Cisco SD-WAN vManage Software product such as Authorization Bypass, Command Injection, XML External Entity, Query Language Injection and Information Disclosure Vulnerability. Cisco recommends installing necessary patch updates at earliest to avoid issues.
Affected Products	Cisco SD-WAN vManage Software releases earlier than Release 20.5.1.
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-vmanage-info-disclos-gGvm9Mfu https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-vmanage-cql-inject-c7z9QqyB https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-vman-xml-ext-entity-q6Z7uVUg https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-vman-cmdinj-nRHKgfHX https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-vman-auth-by-pass-Z3Zze5XC

Affected Product	**HP**
Severity	**Medium**
Affected Vulnerability	Denial of service (CVE-2020-24495, CVE-2020-24505)
Description	HPE has been identified security vulnerabilities in HPE Ethernet Adapters that are based on Intel Ethernet 700 series controllers. Insufficient access control (**CVE-2020-24495)** and insufficient input validation (**CVE-2020-24505)** may lead to local denial of service.
Affected Products	HPE Ethernet 10Gb 2-port FLR-SFP+ X710-DA2 Adapter - Prior to Version 10.54.7 HPE Ethernet 10Gb 2-port SFP+ X710-DA2 Adapter - Prior to Version 10.54.7 Intel X710-DA2 Ethernet 10Gb 2-port SFP+ OCP3 Adapter for HPE - Prior to Version 1.2829 Intel X710-DA2 Ethernet 10Gb 2-port SFP+ Adapter for HPE - Prior to Version 1.2829
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbhf04091en_us

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.