Advisory Alert

Alert Number: AAA20210121 **Date:** January 21, 2021

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Drupal	**Critical**	Directory Traversal
Juniper	**High**	Denial of Service
Oracle	**High**	Multiple Vulnerabilities
Cisco	**High**	Multiple Vulnerabilities
IBM® Db2	**High**	Denial of Service
Cpanel	**High**	Information Disclosure
Redhat	**Medium**	DNS Cache Poisoning

Description

Affected Product	Drupal
Severity	**Critical**
Affected Vulnerability	Directory Traversal (CVE-2020-36193)
Description	Drupal has released security patch updates addressing Directory Traversal that exists in the Drupal core.This vulnerability allows writing pear Archive_Tar library to operations due to inadequate checking of symbolic links.
Affected Products	Drupal 9.1, update to Drupal 9.1.3. Drupal 9.0, update to Drupal 9.0.11. Drupal 8.9, update to Drupal 8.9.13. Drupal 7, update to Drupal 7.78.
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.drupal.org/sa-core-2021-001

Affected Product	Juniper
Severity	**High**
Affected Vulnerability	Denial of Service (CVE-2021-0222, CVE-2021-0221)
Description	These vulnerabilities in Juniper Networks Junos OS allows an attacker to cause a Denial of Service (DoS) to the device by sending certain crafted protocol packets from an adjacent device with invalid payloads to the device. These crafted packets, which should be discarded, are instead replicated and sent to the RE. Over time, a Denial of Service (DoS) occurs. Continued receipt of these crafted protocol packets will cause an extended Denial of Service (DoS) condition.
Affected Products	Junos OS 14.1X53, 15.1, 16.1, 17.1, 17.2, 17.3, 17.4, 18.1, 18.2, 18.3, 18.4, 19.1, 19.2, 19.3. Affected platforms: EX2300, EX3400, EX4300, EX4600, EX4650, QFX3500, QFX5100, QFX5110, QFX5120, QFX5200, QFX5210, QFX10K Series
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://kb.juniper.net/InfoCenter/index?page=content&id=JSA11094&cat=SIRT_1&actp=LIST https://kb.juniper.net/InfoCenter/index?page=content&id=JSA11111&cat=SIRT_1&actp=LIST

Affected Product	Oracle
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities
Description	Oracle has released its January 2021 Security Updates which address multiple Vulnerabilities across several of products, which an attacker could use to gain control of an affected system. Oracle highly recommends to apply relevant patches at earliest to avoid issues.
Affected Products	Multiple Products
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.oracle.com/security-alerts/cpujan2021.html

Affected Product	Cisco
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2021-1129, CVE-2021-1271, CVE-2021-1260, CVE-2021-1261, CVE-2021-1262, CVE-2021-1300, CVE-2021-1301, CVE-2021-1241, CVE-2021-1273, CVE-2021-1274, CVE-2021-1302,CVE-2021-1304 ,CVE-2021-1305, CVE-2021-1349, CVE-2021-1225, CVE-2021-1259, CVE-2021-1235, CVE-2021-1233, CVE-2021-1280)
Description	Cisco has released security patch updates addressing multiple vulnerabilities that exists in multiple Cisco products. An attacker could use these vulnerabilities to gain access to systems and perform Information Disclosure, Cross-Site Scripting, Denial of Service, SQL Injection, Path Traversal, DLL Hijacking various malicious activities. Most of the vulnerabilities are found in the Cisco Web Security Appliance, Cisco SD-WAN, and Cisco Advanced Malware Protection.
Affected Products	Multiple products
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	**Cisco Web Security Appliance** https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-esa-wsa-sma-info-RHp44vAC https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-wsa-xss-RuB5WGqL **Cisco SD-WAN** https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-cmdinjm-9QMSmgcn https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-bufovulns-B5NrSHbj https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-dosmulti-48jJuEUP https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-abyp-TnGFHrS https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-vmanage-cql-inject-72EhnUc https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-vman-sqlinjm-xV8dsjq5 https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-vman-pathtrav-Z5mCVsjf https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-vinfdis-MC8L58dj https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-infodis-2-UPO232DG **Cisco Advanced Malware Protection** https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-amp-imm-dll-5PAZ3hRV

Affected Product	IBM® Db2
Severity	**High**
Affected Vulnerability	Denial of Service (CVE-2020-4642)
Description	IBM DB2 has released a security patch update. IBM DB2 for Linux, UNIX, and Windows could allow a local attacker to cause a denial of service inside the DB2 Management Service.
Affected Products	All fix pack levels of IBM Db2 V9.7, V10.1, V10.5, V11.1, and V11.5 on Windows are affected.
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/6391652

Affected Product	Cpanel
Severity	**High**
Affected Vulnerability	Information Disclosure
Description	Cpanel has released its Security Updates which address Information Disclosure Vulnerability of a product. These updates provide targeted changes to address security concerns.
Affected Products	Previous versions of Cpanel 11.92.0.9 Previous versions of Cpanel 11.86.0.36
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://news.cpanel.com/cpanel-tsr-2021-0001-full-disclosure/

Affected Product	Redhat
Severity	**Medium**
Affected Vulnerability	DNS Cache Poisoning (CVE-2020-25684, CVE-2020-25685, CVE-2020-25686)
Description	Redhat has released security patch updates addressing DNS Cache Poisoning that exists in Redhat products. These issues are in the Domain Name System (DNS) service provided by dnsmasq could be used by a remote attacker, poison the DNS cache, and redirect victim users to incorrect sites or execute code on the machine which is using dnsmasq.
Affected Products	Red Hat Enterprise Linux Server 7 x86_64 Red Hat Enterprise Linux Workstation 7 x86_64 Red Hat Enterprise Linux Desktop 7 x86_64 Red Hat Enterprise Linux for IBM z Systems 7 s390x Red Hat Enterprise Linux for Power, big endian 7 ppc64 Red Hat Enterprise Linux for Scientific Computing 7 x86_64 Red Hat Enterprise Linux for Power, little endian 7 ppc64le
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://access.redhat.com/security/cve/CVE-2020-25684 https://access.redhat.com/security/cve/CVE-2020-25685 https://access.redhat.com/security/cve/CVE-2020-25686

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.