TLP: WHITE

Advisory Alert

Alert Number : AAA20200805 **Date :** August 5, 2020

Document Classification Level : Public Circulation Permitted

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Red Hat	**High**	Multiple Vulnerabilities
CISCO	**High**	Multiple Vulnerabilities

Description

Affected Product	Red Hat
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2020-10713, CVE-2020-14308, CVE-2020-14309, CVE-2020-14310, CVE-2020-14311, CVE-2020-15705, CVE-2020-15706, CVE-2020-15707), (CVE-2020-13692)
Description	Redhat has released patch updates addressing multiple vulnerabilities that exists in grub2 which is highly configurable/ customizable boot loader with modular architecture and for shim package which is a first stage UEFI boot loader that handles chaining to a trusted full boot loader under secure boot environments. CVE-2020-13692 PostgreSQL contains a vulnerability in postgresql-jdbc which includes .jar files required for Java programs to access database. This flaw allows an attacker to cause an XML external entity attack using PgSQLXML.
Affected Products	Red Hat Enterprise Linux Server - TUS 7.3 x86_64 Red Hat Enterprise Linux Server (for IBM Power LE) - Update Services for SAP Solutions 8.0 ppc64le Red Hat Enterprise Linux Server - Update Services for SAP Solutions 8.0 x86_64
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://access.redhat.com/errata/RHSA-2020:3276 https://access.redhat.com/errata/RHSA-2020:3283

Affected Product	CISCO
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2020-3461), (CVE-2020-3374), (CVE-2020-3375), (CVE-2020-3274, CVE-2020-3275, CVE-2020-3276, CVE-2020-3277, CVE-2020-3278, CVE-2020-3279)
Description	Cisco has released security patches addressing vulnerabilities that exists in web-based management interfaces of multiple products and SD-WAN solution software. There are no workarounds available for these vulnerabilities and it is recommended to apply the fixes at earliest.
Affected Products	Cisco DCNM software releases earlier than Release 11.4(1) Cisco SD-WAN vManage Software Cisco SD-WAN Solution Software Cisco Small Business router firmware releases of RV320,RV325, RV016, RV042,RV082
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-dcnm-info-disclosure-tFX3KerC https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-uabvman-SYGzt8Bv https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdbufof-h5f5VSeL https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-routers-Rj5JRfF8

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.