Advisory Alert

Alert Number: AAA20210415 **Date:** April 15, 2021

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Redhat	High	Multiple Vulnerabilities
IBM	High	Multiple Vulnerabilities
Juniper	High	Multiple Vulnerabilities
Cisco	Medium	Denial of service vulnerability
PaloAlto	Medium	Multiple Vulnerabilities
Joomla	Low	Multiple Vulnerabilities

Description

Affected Product	Redhat
Severity	High
Affected Vulnerability	Multiple Vulnerabilities (CVE-2019-20921, CVE-2020-25657, CVE-2020-28458, CVE-2020-28477, CVE-2021-3449, CVE-2021-3450)
Description	Redhat has released Security Updates addressing multiple vulnerabilities that exists with multiple Redhat virtualization products. Redhat highly recommends to apply necessary security fixes at earliest to avoid issues.
Affected Products	Red Hat Virtualization 4 for RHEL 8 x86_64 Red Hat Virtualization Host 4 for RHEL 8 x86_64 Red Hat Virtualization Manager 4.4 x86_64
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://access.redhat.com/security/cve/CVE-2019-20921 https://access.redhat.com/security/cve/CVE-2020-25657 https://access.redhat.com/security/cve/CVE-2020-28458 https://access.redhat.com/security/cve/CVE-2020-28477 https://access.redhat.com/security/cve/CVE-2021-3449 https://access.redhat.com/security/cve/CVE-2021-3450

Affected Product	IBM
Severity	High
Affected Vulnerability	Multiple Vulnerabilities (CVE-2020-5258,CVE-2021-20480,CVE-2020-14803,CVE-2020-27221,CVE-2021-3156,CVE-2018-11782,CVE-2019-19956,CVE-2019-20388,CVE-2020-7595,CVE-2019-5094,CVE-2019-5188,CVE-2017-12652,CVE-2019-11068,CVE-2019-18197,CVE-2020-4329)
Description	IBM has released security updates addressing multiple vulnerabilities that exists in QRadar, WebSphere application server, DB2 and InfoSphere information server. IBM highly recommends to apply necessary security fixes at earliest to avoid issues.
Affected Products	IBM QRadar Network Security 5.4.0 IBM QRadar Network Security 5.5.0 IBM QRadar 7.3.0 to 7.3.3 Patch 7 IBM QRadar 7.4.0 to 7.4.2 Patch 2 WebSphere Application Server 9.0, 8.5, 8.0, 7.0 WebSphere Application Server Liberty 17.0.0.3 - 21.0.0.3 DB2 Query Management Facility for z/OS 11.2.1 DB2 Query Management Facility for z/OS 12.1 DB2 Query Management Facility for z/OS 12.2 DB2 Query Management Facility for z/OS 11.2 DB2 Query Management Facility for z/OS 11.1 Query Management Facility Classic Edition 11.1 Query Management Facility Enterprise Edition 11.1 InfoSphere Information Server with a Microservices tier 11.7
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/6443101 https://www.ibm.com/support/pages/node/6441063 https://www.ibm.com/support/pages/node/6439991 https://www.ibm.com/support/pages/node/6442607 https://www.ibm.com/support/pages/node/6441625 https://www.ibm.com/support/pages/node/6436379

Affected Product	Juniper
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities
Description	Juniper has released Security Updates addressing multiple vulnerabilities that exists with multiple juniper products. Juniper highly recommends to apply necessary security fixes at earliest to avoid issues.
Affected Products	Multiple Products
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://kb.juniper.net/InfoCenter/index?page=content&channel=SECURITY_ADVISORIES&cat=SIRT_1&sort=datemodified&&actp=&dir=descending&max=1000&batch=15&rss=true

Affected Product	Cisco
Severity	**Medium**
Affected Vulnerability	Denial of service vulnerability (CVE-2021-1450)
Description	Cisco has released security updates addressing denial of service vulnerability that exists in their products. Due to insufficient validation of user supplied input, the IPC channel of Cisco AnyConnect secure mobile client could allow an authenticated local attacker to cause DOS attack on the affected device by sending crafted IPC messages to the AnyConnect process.
Affected Products	AnyConnect Secure Mobility Client for Windows AnyConnect Secure Mobility Client for MacOS AnyConnect Secure Mobility Client for Linux
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-anyconnect-dos-55AYyxYr

Affected Product	PaloAlto
Severity	**Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2021-3036, CVE-2021-3037)
Description	PaloAlto has released security updates addressing multiple vulnerabilities that exists in their products. CVE-2021-3036 – PAN-OS appliances that are configured to use the PAN-OS XML API contains a vulnerability that gets exploited when a client includes a duplicate API parameter in API requests leading to an information exposure. CVE-2021-3037 – PAN-OS software contains an information exposure through log file vulnerability which occurs where the connection details of scheduled configuration export are also logged in system logs.
Affected Products	PAN-OS 10.0 < 10.0.1 PAN-OS 9.1 < 9.1.6 PAN-OS 9.0 < 9.0.13 PAN-OS 8.1 < 8.1.19
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://security.paloaltonetworks.com/CVE-2021-3036 https://security.paloaltonetworks.com/CVE-2021-3037

Affected Product	Joomla
Severity	**Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2021-26031, CVE-2021-26030)
Description	Joomla has released security updates addressing multiple vulnerabilities that exists in their products. CVE-2021-26031 – Due to inadequate filters on module layout settings could cause local file inclusion vulnerability and may lead to information disclosure, remote code execution or XSS attack. CVE-2021-26030 – Due to inadequate escaping, an XSS can be caused using the logo parameter of the default templates on the error page.
Affected Products	Joomla! CMS versions 3.0.0 - 3.9.25
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://developer.joomla.org/security-centre/

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.