Advisory Alert

Alert Number: AAA20230406 **Date:** April 6, 2023

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
RedHat	**High**	Multiple Vulnerabilities
Cisco	**High**, Medium	Multiple Vulnerabilities
IBM	**High**, Medium	Multiple Vulnerabilities

Description

Affected Product	**RedHat**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-0266, CVE-2023-0386, CVE-2023-0461, CVE-2022-3564, CVE-2022-4269, CVE-2022-4378, CVE-2023-1476)
Description	RedHat has released security updates addressing multiple vulnerabilities that exist in their products. If exploited these vulnerabilities could cause kernel information leakage, privilege escalation, system crash, and Denial of service. RedHat recommends to apply the necessary patch updates at your earliest to avoid issues.
Affected Products	Red Hat Enterprise Linux for x86_64 - Extended Update Support 8.6 x86_64 Red Hat Enterprise Linux Server - AUS 8.6 x86_64 Red Hat Enterprise Linux for IBM z Systems - Extended Update Support 8.6 s390x Red Hat Enterprise Linux for Power, little endian - Extended Update Support 8.6 ppc64le Red Hat Virtualization Host 4 for RHEL 8 x86_64 Red Hat Enterprise Linux Server - TUS 8.6 x86_64 Red Hat Enterprise Linux for ARM 64 - Extended Update Support 8.6 aarch64 Red Hat Enterprise Linux Server for Power LE - Update Services for SAP Solutions 8.6 ppc64le Red Hat Enterprise Linux for x86_64 - Update Services for SAP Solutions 8.6 x86_64 Red Hat CodeReady Linux Builder for x86_64 - Extended Update Support 8.6 x86_64 Red Hat CodeReady Linux Builder for Power, little endian - Extended Update Support 8.6 ppc64le Red Hat CodeReady Linux Builder for ARM 64 - Extended Update Support 8.6 aarch64 Red Hat Enterprise Linux for Real Time - Telecommunications Update Service 8.4 x86_64 Red Hat Enterprise Linux for Real Time for NFV - Telecommunications Update Service 8.4 x86_64 Red Hat Enterprise Linux for x86_64 - Extended Update Support 8.4 x86_64 Red Hat Enterprise Linux Server - AUS 8.4 x86_64 Red Hat Enterprise Linux for IBM z Systems - Extended Update Support 8.4 s390x Red Hat Enterprise Linux for Power, little endian - Extended Update Support 8.4 ppc64le Red Hat Enterprise Linux Server - TUS 8.4 x86_64 Red Hat Enterprise Linux for ARM 64 - Extended Update Support 8.4 aarch64 Red Hat Enterprise Linux Server for Power LE - Update Services for SAP Solutions 8.4 ppc64le Red Hat Enterprise Linux for x86_64 - Update Services for SAP Solutions 8.4 x86_64 Red Hat CodeReady Linux Builder for x86_64 - Extended Update Support 8.4 x86_64 Red Hat CodeReady Linux Builder for Power, little endian - Extended Update Support 8.4 ppc64le Red Hat CodeReady Linux Builder for ARM 64 - Extended Update Support 8.4 aarch6 Red Hat Enterprise Linux Server - AUS 8.2 x86_64 Red Hat Enterprise Linux Server - TUS 8.2 x86_64 Red Hat Enterprise Linux Server for Power LE - Update Services for SAP Solutions 8.2 ppc64le Red Hat Enterprise Linux for x86_64 - Update Services for SAP Solutions 8.2 x86_64 Red Hat Enterprise Linux for Real Time 8 x86_64 Red Hat Enterprise Linux for Real Time for NFV 8 x86_64 Red Hat Enterprise Linux for x86_64 8 x86_64 Red Hat Enterprise Linux for Power, little endian 8 ppc64le
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://access.redhat.com/errata/RHSA-2023:1554 https://access.redhat.com/errata/RHSA-2023:1556 https://access.redhat.com/errata/RHSA-2023:1557 https://access.redhat.com/errata/RHSA-2023:1559 https://access.redhat.com/errata/RHSA-2023:1584 https://access.redhat.com/errata/RHSA-2023:1659 https://access.redhat.com/errata/RHSA-2023:1660 https://access.redhat.com/errata/RHSA-2023:1662 https://access.redhat.com/errata/RHSA-2023:1666

Affected Product	**Cisco**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-20123, CVE-2023-20152, CVE-2023-20153, CVE-2023-20127, CVE-2023-20129, CVE-2023-20130, CVE-2023-20131, CVE-2023-20137, CVE-2023-20138, CVE-2023-20139, CVE-2023-20140, CVE-2023-20141, CVE-2023-20142, CVE-2023-20143, CVE-2023-20144, CVE-2023-20145, CVE-2023-20146, CVE-2023-20147, CVE-2023-20148, CVE-2023-20149, CVE-2023-20150, CVE-2023-20151, CVE-2023-20103, CVE-2023-20096, CVE-2023-20132, CVE-2023-20134, CVE-2023-20124, CVE-2023-20121, CVE-2023-20122, CVE-2023-20117, CVE-2023-20128)
Description	Cisco has released security updates addressing multiple vulnerabilities that exist in their products. If exploited these vulnerabilities could cause unauthorized access, command injection, cross site scripting, cross site request forgery, and arbitrary code execution. CIsco recommends to apply the necessary patch updates at your earliest to avoid issues.
Affected Products	Cisco Duo for macOS Two-Factor Authentication Software 2.0 and earlier Cisco Duo Authentication for Windows Logon and RDP Software 4.2 and earlier Cisco ISE version 3.2 Cisco Prime Infrastructure Release 3.7 and earlier versions, 3.8, 3.9 and 3.10 Cisco EPNM 7.0, 6.1, 6.0, 5.1, 5.0 and earlier versions Cisco Secure Network Analytics versions earlier than 7.4.2 Cisco Unified CCX 12.5, 12.0 and earlier versions Cisco Webex Meetings (cloud based) RV016 Multi-WAN VPN Routers RV042 Dual WAN VPN Routers RV042G Dual Gigabit WAN VPN Routers RV082 Dual WAN VPN Routers RV320 Dual Gigabit WAN VPN Routers RV325 Dual Gigabit WAN VPN Routers RV160 VPN Routers RV160W Wireless-AC VPN Routers RV260 VPN Routers RV260P VPN Routers with PoE RV260W Wireless-AC VPN Routers RV340 Dual WAN Gigabit VPN Routers RV340W Dual WAN Gigabit Wireless-AC VPN Routers RV345 Dual WAN Gigabit VPN Routers RV345P Dual WAN Gigabit PoE VPN Routers
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-duo-replay-knuNKd https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ise-injection-2XbOg9Dg https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-pi-epnm-eRPWAXLe https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-stored-xss-vqz7gC8W https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-stealth-rce-BDwXFK9C https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-uccx-xss-GO9L9xxr https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-wbx-sxss-fupl-64uHbcm5 https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv01x_rv32x_rce-nzAGWWDD https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-adeos-MLAyEcvk https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv32x-cmdinject-cKQsZpxL https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-stealthsmc-rce-sfNBPjcS

Affected Product	**IBM**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2022-0235, CVE-2020-15168, CVE-2022-31129, CVE-2022-24785, CVE-2022-29244)
Description	IBM has released a security update addressing multiple vulnerabilities that exist in the components that used in IBM QRadar Data Synchronization App. If exploited these vulnerabilities could cause sensitive data exposure, denial of service, and directory traversal. IBM recommends to apply the necessary patch updates at your earliest to avoid issues.
Affected Products	IBM QRadar Data Synchronization App version 1.0 - 3.1.0
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/6980799

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.