TLP: WHITE

Advisory Alert

Alert Number: AAA20231009 **Date:** October 9, 2023

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Cisco	**Critical**	Multiple Vulnerabilities
IBM	**Critical**	Buffer Overflow Vulnerability
IBM	**High**, **Medium**	Multiple Vulnerabilities
Ubuntu	**High**, **Medium**, **Low**	Multiple Vulnerabilities
HPE	**Medium**	Information Disclosure Vulnerability
Redhat	**Medium**	Multiple Vulnerabilities
Qnap	**Medium**, **Low**	Multiple Vulnerabilities

Description

Affected Product	**Cisco**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-20034, CVE-2023-20252, CVE-2023-20253, CVE-2023-20254, CVE-2023-20262)
Description	Cisco has released security updates addressing multiple vulnerabilities that exist in Cisco Catalyst SD-WAN Manager. Successful exploitation of these vulnerabilities could allow an attacker to access an affected instance or cause a denial of service (DoS) condition on an affected system. Cisco highly recommends to apply the necessary security updates at earliest to avoid issues
Affected Products	Cisco Catalyst SD-WAN Manager versions 20.10.1, 20.11.1, 20.12.1, 20.3.4, 20.6.1, 20.6.2, 20.6.3.4, 20.7.1, 20.8.1, 20.9.1, 20.9.3, 20.9.41
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-vman-sc-LRLfu2z

Affected Product	**IBM**
Severity	**Critical**
Affected Vulnerability	Buffer Overflow Vulnerability (CVE-2023-39976)
Description	IBM has released security updates addressing a Buffer overflow vulnerability that exists in ClusterLabs libqb of Db2 servers. Caused by improper bounds checking by the qb_vsnprintf_serialize function in log_blackbox.c. By sending a specially crafted request, a remote attacker could overflow a buffer and execute arbitrary code on the system. IBM highly recommends to apply the necessary security updates at earliest to avoid issues
Affected Products	Db2 11.5.x Server
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/7047565

Affected Product	**IBM**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-40374, CVE-2023-38728, CVE-2023-33850, CVE-2023-38720, CVE-2023-30991, CVE-2023-38740, CVE-2023-21930, CVE-2023-21967, CVE-2023-21954, CVE-2023-21939, CVE-2023-21968, CVE-2023-21937, CVE-2023-21938, CVE-2023-2597, CVE-2023-38719, CVE-2023-30987, CVE-2023-40372, CVE-2023-40373, CVE-2022-40609)
Description	IBM has released security updates addressing multiple vulnerabilities that exist in their products. Exploitation of these vulnerabilities could lead to denial of service (DoS), Sensitive information disclosure, Buffer overflow, Arbitrary code execution. IBM recommends to apply the necessary security updates at earliest to avoid issues
Affected Products	IBM Db2 10.5.0.x Client and Server IBM Db2 11.1.4.x Client and Server IBM Db2 11.5.8 Server IBM Db2 11.5.x Client and Server
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/7047261 https://www.ibm.com/support/pages/node/7047478 https://www.ibm.com/support/pages/node/7047481 https://www.ibm.com/support/pages/node/7047489 https://www.ibm.com/support/pages/node/7047499 https://www.ibm.com/support/pages/node/7047554 https://www.ibm.com/support/pages/node/7047556 https://www.ibm.com/support/pages/node/7047558 https://www.ibm.com/support/pages/node/7047560 https://www.ibm.com/support/pages/node/7047561 https://www.ibm.com/support/pages/node/7047563 https://www.ibm.com/support/pages/node/7047724

Affected Product	**Ubuntu**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-4273, CVE-2023-1206, CVE-2023-3865, CVE-2023-3338, CVE-2023-4132, CVE-2023-4155, CVE-2023-3866, CVE-2023-44466, CVE-2023-20569, CVE-2023-3863, CVE-2023-38432, CVE-2023-4194, CVE-2023-2156)
Description	Ubuntu has released security updates addressing multiple vulnerabilities that exist in their products. Exploitation of these vulnerabilities could lead to Arbitrary code execution, Sensitive information disclosure, Denial of service. Ubuntu recommends to apply the necessary security updates at earliest to avoid issues
Affected Products	Ubuntu 20.04
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://ubuntu.com/security/notices/USN-6416-2

Affected Product	**HPE**
Severity	**Medium**
Affected Vulnerability	Information Disclosure Vulnerability (CVE-2022-40982)
Description	A security vulnerability in HPE Superdome Flex and Superdome Flex 280 servers using Skylake, Cascade Lake and CooperLake Intel processors could be locally exploited to allow disclosure of information. HPE recommends to apply the necessary security updates at earliest to avoid issues
Affected Products	HPE Superdome Flex Server - Prior to v3.80.24 HPE Superdome Flex 280 Server - Prior to v1.60.16
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbhf04534en_us

Affected Product	**Redhat**
Severity	**Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-1664, CVE-2023-2976, CVE-2023-33008)
Description	Redhat has released security updates addressing multiple vulnerabilities that exist in their products **CVE-2023-1664** - A flaw was found in Keycloak. This flaw depends on a non-default configuration "Revalidate Client Certificate" to be enabled and the reverse proxy is not validating the certificate before Keycloak. Using this method an attacker may choose the certificate which will be validated by the server. **CVE-2023-2976** - A flaw was found in Guava. The methodology for temporary directories and files can allow other local users or apps with accordant permissions to access the temp files, possibly leading to information exposure or tampering in the files created in the directory. **CVE-2023-33008** - A flaw was found in Apache Johnzon. This issue could allow an attacker to craft a specific JSON input that Johnzon will deserialize into a BigDecimal, which Johnzon may use to start converting large numbers, resulting in a denial of service. Redhat recommends to apply the necessary security updates at earliest to avoid issues
Affected Products	Red Hat JBoss Middleware Text-Only Advisories for MIDDLEWARE 1 x86_64
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://access.redhat.com/errata/RHSA-2023:5491

Affected Product	**Qnap**
Severity	**Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-20032, CVE-2023-20052, CVE-2023-32971, CVE-2023-32972, CVE-2023-23370, CVE-2023-23371)
Description	Qnap has released security updates addressing multiple vulnerabilities that exist in their products. Exploitation of these vulnerabilities could lead to Arbitrary code execution and Sensitive information disclosure. Qnap recommends to apply the necessary security updates at earliest to avoid issues
Affected Products	QTS 5.0.x, QuTS hero h5.0.x, QuTScloud c5.0.1 QTS 5.1.x, 5.0.x, 4.5.x; QuTS hero h5.1.x, h5.0.x, h4.5.x; QuTScloud c5.x QVPN Windows 2.1.x QVPN Windows 2.2.x
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.qnap.com/go/security-advisory/qsa-23-26 https://www.qnap.com/go/security-advisory/qsa-23-37 https://www.qnap.com/go/security-advisory/qsa-23-36 https://www.qnap.com/go/security-advisory/qsa-23-39

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.