Advisory Alert

Alert Number: AAA20230608 **Date:** June 8, 2023

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
VMware	**Critical**	Multiple Vulnerabilities
Cisco	**Critical**	Privilege Escalation Vulnerabilities
Cisco	**High**, Medium	Multiple Vulnerabilities
IBM	**High**, Medium	Multiple Vulnerabilities

Description

Affected Product	**VMware**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-20887, CVE-2023-20888, CVE-2023-20889)
Description	VMware has released a security update addressing multiple Critical vulnerabilities affecting VMware Aria Operations Networks. Successful exploitation could result in remote code execution and information disclosure. VMware highly recommends to apply the necessary patch updates at your earliest to avoid issues
Affected Products	VMware Aria Operations Networks 6.x
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.vmware.com/security/advisories/VMSA-2023-0012.html

Affected Product	**Cisco**
Severity	**Critical**
Affected Vulnerability	Privilege Escalation Vulnerabilities (CVE-2023-20105, CVE-2023-20192)
Description	Multiple critical vulnerabilities have been identified in Cisco Expressway Series and Cisco TelePresence Video Communication Server (VCS), which could allow an authenticated attacker with Administrator-level read-only credentials to escalate their privileges to Administrator with read-write credentials on the affected system. Cisco highly recommends to apply the necessary patch updates at your earliest to avoid issues
Affected Products	Cisco Expressway Series Earlier than 14.0 Cisco TelePresence VCS 14.0
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-expressway-priv-esc-Ls2B9t7b

Affected Product	**Cisco**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-20136, CVE-2023-20116, CVE-2023-20188, CVE-2023-20178, CVE-2023-20006, CVE-2023-20108)
Description	Cisco has released several security updates addressing multiple vulnerabilities in various Cisco products. These vulnerabilities could be exploited by malicious actors to execute arbitrary code, Cross-Site Scripting, cause a denial-of-service (DoS) condition, or Privilege Escalation Cisco recommends to apply the necessary patch updates at your earliest to avoid issues
Affected Products	Cisco Secure Workload with the default configuration Cisco Unified CM and Unified CM SME Small Business 200 Series Smart Switches Small Business 300 Series Managed Switches Small Business 500 Series Stackable Managed Switches Cisco AnyConnect Secure Mobility Client Software for Windows and Cisco Secure Client Software for Windows Cisco ASA Software and Cisco FTD Software if they are running on Cisco Firepower 2100 Series Cisco Unified CM IM&P
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-csw-auth-openapi-kTndjdNX https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cucm-dos-4Ag3yWbD https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-smb-sxss-OPYJZUmE https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ac-csc-privesc-wx4U4Kw https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-ssl-dos-uu7mV5p6 https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cucm-imp-dos-49GL7rzT

Affected Product	**IBM**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2022-3171, CVE-2022-41881, CVE-2022-40152, CVE-2022-31160, CVE-2017-7525, CVE-2022-25168, CVE-2022-3509, CVE-2022-41854, CVE-2022-38752, CVE-2022-1471, CVE-2021-37533, CVE-2022-42004, CVE-2022-42003)
Description	IBM has identified multiple vulnerabilities in IBM QRadar User Behavior Analytics, which could be exploited by attackers to cause denial-of-service (DoS) conditions, execute arbitrary code, or obtain sensitive information.. IBM recommends to apply the necessary patch updates at your earliest to avoid issues
Affected Products	IBM QRadar User Behavior Analytics versions 1.0.0 to 4.1.1
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/7001815

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.