Advisory Alert

Alert Number: **AAA20240328** **Date:** **March 28, 2024**

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
IBM	**Critical**	Denial of service Vulnerability
Dell	**High**	Improper Access Control Vulnerability
Zscaler	**High**	Multiple Vulnerabilities
Cisco	**High**, **Medium**	Multiple Vulnerabilities
IBM	**High**, **Medium**, **Low**	Multiple Vulnerabilities

Description

Affected Product	**IBM**
Severity	**Critical**
Affected Vulnerability	Denial of service Vulnerability (CVE-2020-36242)
Description	IBM has issued security updates addressing Denial of service Vulnerability that exists in IBM QRadar SIEM. **CVE-2020-36242**- Cryptography could allow a remote attacker to execute arbitrary code on the system, caused by an integer overflow and a buffer overflow. By using certain sequences of update calls to symmetrically encrypt multi-GB values, a remote attacker could exploit this vulnerability to execute arbitrary code on the system or cause a denial of service. IBM advises to apply security fixes at your earliest to protect your systems from potential threats.
Affected Products	IBM QRadar SIEM Version 7.5.0 - 7.5.0 UP7 IF06
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/7145367

Affected Product	**Dell**
Severity	**High**
Affected Vulnerability	Improper Access Control Vulnerability (CVE-2024-25962)
Description	Dell has released security updates addressing an Improper access control vulnerability that exists in Dell InsightIQ. **CVE-2024-25962** - An improper access control vulnerability exists in the Dell InsightIQ version 5.0. A remote low privileged attacker could potentially exploit this vulnerability, leading to unauthorized access to monitoring data. Dell advises to apply security fixes at your earliest to protect your systems from potential threats.
Affected Products	Dell InsightIQ Version 5.0.0
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.dell.com/support/kbdoc/en-us/000223551/dsa-2024-134-security-update-for-dell-insightiq-for-proprietary-code-vulnerability

Affected Product	**Zscaler**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-41969, CVE-2023-41972, CVE-2023-41973, CVE-2024-23482)
Description	Zscaler has released security updates addressing multiple vulnerabilities that exist in Zscaler Client Connector on Windows and macOS operating systems. If Exploited, these vulnerabilities could lead to Arbitrary File Deletion, Local Privilege Escalation. Zscaler advises to apply security fixes at your earliest to protect your systems from potential threats.
Affected Products	Zscaler Client Connector versions before 4.3.0.121 on Windows Zscaler Client Connector versions before 4.2.0.241 for macOS
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://trust.zscaler.com/zscaler.net/posts/18226

Affected Product	**Cisco**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-20259, CVE-2024-20265, CVE-2024-20271, CVE-2024-20276, CVE-2024-20278, CVE-2024-20303, CVE-2024-20306, CVE-2024-20307, CVE-2024-20308, CVE-2024-20309, CVE-2024-20311, CVE-2024-20312, CVE-2024-20313, CVE-2024-20314, CVE-2024-20316, CVE-2024-20324, CVE-2024-20333, CVE-2024-20354)
Description	Cisco has released security updates addressing multiple vulnerabilities that exist in their products. If exploited, these vulnerabilities could be lead to Denial of Service, Secure Boot Bypass, Privilege Escalation, Command Injection. Cisco recommends to apply security fixes at your earliest to protect your systems from potential threats.
Affected Products	Multiple Cisco Products
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-airo-ap-dos-PPPtcVW https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-aux-333WBz8f https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ccc-authz-bypass-5EKchJRb https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-dmi-acl-bypass-Xv8FO8Vz https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-priv-esc-seAx6NLX https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-utd-cmd-JbL8KvHT https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-wlc-privesc-RjSMrmPK https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ap-dos-h9TGGX6W https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ap-secureboot-bypass-zT5vJkSD https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-dhcp-dos-T3CXPO9z https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ikev1-NO2ccFWz https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dos-Hq4d3tZG https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-xe-sda-edge-dos-qZWuWXWG https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-ospf-dos-dR9Sfrxp https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-isis-sGjyOUHX https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-lisp-3gYXs3qP https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-wlc-mdns-dos-4hv6pBGf

Affected Product	**IBM**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-42503, CVE-2018-17196, CVE-2023-6129, CVE-2023-4806, CVE-2021-43818, CVE-2020-25659, CVE-2020-27783, CVE-2021-28957, CVE-2023-23931, CVE-2020-10683, CVE-2018-1000632, CVE-2023-7104, CVE-2022-40304, CVE-2022-40303, CVE-2023-3446, CVE-2023-27043, CVE-2023-36632, CVE-2022-25647, CVE-2020-28493, CVE-2020-10735, CVE-2023-3817, CVE-2022-4304, CVE-2023-0215, CVE-2023-0286, CVE-2022-48565, CVE-2022-48564, CVE-2023-42753, CVE-2023-4813, CVE-2023-5678, CVE-2022-36760, CVE-2023-3961, CVE-2023-4091, CVE-2023-42669, CVE-2022-2127, CVE-2023-34966, CVE-2023-34967, CVE-2023-34968, CVE-2020-1968, CVE-2019-1551, CVE-2019-1547, CVE-2019-1563, CVE-2023-3635, CVE-2024-22353)
Description	IBM has released security updates addressing multiple vulnerabilities that exist in their products. If exploited, these vulnerabilities could cause, Denial of Service, bypass security restrictions, cross-site scripting, execute arbitrary code. IBM recommends to apply security fixes at your earliest to protect your systems from potential threats.
Affected Products	IBM QRadar SIEM 7.5.0 - 7.5.0 UP7 IF06 All versions of APM WebSphere Application Server Agent, APM Tomcat Agent, APM SAP NetWeaver Java Stack Agent, APM WebLogic Agent and APM Data Collector for J2SE IBM WebSphere Application Server Liberty 17.0.0.3 - 24.0.0.3
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/7145367 https://www.ibm.com/support/pages/node/7051173 https://www.ibm.com/support/pages/node/7145365

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.