Advisory Alert

Alert Number: AAA20221020 **Date:** October 20, 2022

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

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

Description

Affected Product	**IBM**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2012-5783, CVE-2021-22569, CVE-2019-10202, CVE-2019-10172, CVE-2011-4969, CVE-2015-9251, CVE-2012-6708, CVE-2020-7656, CVE-2021-29425, CVE-2020-9492, CVE-2021-34538, CVE-2019-0205, CVE-2022-25647, CVE-2020-13936)
Description	IBM has released security updates addressing multiple critical vulnerabilities that exist in IBM QRadar User Behavior Analytics. Exploitation of the most severe vulnerabilities cause arbitrary code execution, privilege escalation, denial of service, Security restriction bypass and directory traversal. IBM highly recommends to apply the necessary security updates at earliest to avoid issues.
Affected Products	IBM Radar User Behavior Analytics 4.1.8
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/6830243

Affected Product	**Cisco**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2022-20933, CVE-2022-20822, CVE-2022-20776, CVE-2022-20811, CVE-2022-20953, CVE-2022-20954, CVE-2022-20955, CVE-2022-20959)
Description	Cisco has released security updates addressing multiple vulnerabilities that exist in their products. Attackers can exploit these vulnerabilities to cause denial of service (DoS), unauthorized file Access, path traversal attacks, view sensitive data, or write arbitrary files and cross-site scripting (XSS) Cisco highly recommends to apply the necessary security updates at earliest to avoid issues.
Affected Products	Cisco TelePresence CE Software Release 9, 10 Cisco ISE Software Release 2.4[1] and earlier, 2.6[2], 2.7[2], 3.0[2], 3.1, 3.2[2] with ERS enabled Cisco ISE Release 3.1[1], 3.2[1] Cisco Meraki products running a vulnerable release of Cisco Meraki MX firmware and have Cisco AnyConnect VPN enabled: • MX64,MX64W, MX65, MX65W, MX67, MX67CW, MX67W, MX68, MX68CW, MX68W, MX75, MX84, MX85, MX95, MX100, MX105, MX250, MX400, MX450, MX600, vMX, Z3C, Z3
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-vnESbgBf https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ise-path-trav-Dz5dpzyM https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-roomos-trav-beFvCcyu https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ise-xss-twLnpy3M

Affected Product	**IBM**
Severity	**Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2022-21496 , CVE-2022-21434 , CVE-2022-21443 , CVE-2021-35561 , CVE-2022-21299)
Description	IBM has released security updates addressing multiple vulnerabilities that exist in IBM WebSphere Application Server. Attackers can exploit these vulnerabilities to cause unauthorized update, insert or delete functions and partial denial of service. IBM highly recommends to apply the necessary security updates at earliest to avoid issues.
Affected Products	IBM Java SDK shipped with IBM WebSphere Application Server Patterns 1.0.0.0 through 1.0.0.7 and 2.2.0.0 through 2.3.3.5
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/blogs/psirt/security-bulletin-multiple-vulnerabilities-in-ibm-java-sdk-affects-ibm-websphere-application-server-april-2022-cpu-that-is-bundled-with-ibm-websphere-application-server-patterns/

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.