Advisory Alert

Alert Number: AAA20221018 **Date:** October 18, 2022

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
IBM	**Critical**	Multiple Vulnerabilities
IBM	**Medium**	SOAP Action spoofing Vulnerability
Juniper	**Medium**	Denial of Service Vulnerability

Description

Affected Product	**IBM**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2019-11358, CVE-2020-11022, CVE-2020-11023, CVE-2021-44907, CVE-2021-23337, CVE-2018-16487, CVE-2020-8203, CVE-2019-10744, CVE-2019-1010266, CVE-2018-3721, CVE-2018-25031, CVE-2021-32803, CVE-2021-37713, CVE-2021-32804, CVE-2021-37701, CVE-2021-37712, CVE-2021-44906, CVE-2020-7598, CVE-2021-3765, CVE-2020-28469, CVE-2021-3807, CVE-2021-22959, CVE-2021-22960, CVE-2021-3918, CVE-2021-33502, CVE-2020-7788)
Description	IBM has released security updates addressing multiple critical vulnerabilities that exist in IBM QRadar Pulse App. Exploitation of the most severs vulnerabilities cause arbitrary code execution, denial of service, cross site scripting and prototype pollution IBM highly recommends to apply the necessary security updates at earliest to avoid issues.
Affected Products	IBM QRadar Pulse App 1.0.0 – 2.2.8
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/6830017

Affected Product	**IBM**
Severity	**Medium**
Affected Vulnerability	SOAP Action spoofing Vulnerability (CVE-2022-38712)
Description	IBM has released security updates addressing a SOAP Action spoofing vulnerability that exist in IBM WebSphere Application Server. A man-in-the-middle attacker can conduct SOAP Action spoofing to execute unwanted or unauthorized operations. IBM highly recommends to apply the necessary patch updates at your earliest to avoid issues.
Affected Products	IBM WebSphere Application Server 9.0 IBM WebSphere Application Server 8.5 IBM WebSphere Application Server 8.0 IBM WebSphere Application Server 7.0
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/6829907

Affected Product	**Juniper**
Severity	**Medium**
Affected Vulnerability	Denial of Service Vulnerability (CVE-2022-22219)
Description	Juniper has released a security update addressing a denial vulnerability that exists due to improper handling of an unexpected data type in the processing of EVPN routes on Juniper Networks Junos OS and Junos OS Evolved products. Using this, an attacker who has direct control of the BGP client connected to a route reflector, or via a machine in the middle (MITM) attack,can send a specific EVPN route contained within a BGP Update, triggering a routing protocol daemon to (RPD) crash, leading to a Denial of Service (DoS) condition. Juniper highly recommends to apply the necessary patch updates at your earliest to avoid issues.
Affected Products	Junos OS 21.3, 21.4, 22.1, 22.2 Junos OS Evolved 21.3-EVO, 21.4-EVO, 22.1-EVO, 22.2-EVO
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://supportportal.juniper.net/s/article/2022-10-Security-Bulletin-Junos-OS-and-Junos-OS-Evolved-RPD-core-upon-receipt-of-a-specific-EVPN-route-by-a-BGP-route-reflector-in-an-EVPN-environment-CVE-2022-22199?language=en_US

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.