TLP: WHITE

Advisory Alert

Alert Number: AAA20201016 **Date:** October 16, 2020

Document Classification Level : Public Circulation Permitted

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Juniper	**High**	Multiple Vulnerabilities
IBM	**High**	Bypass Sanitation

Description

Affected Product	Juniper
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2020-1660, CVE-2020-1656, CVE-2020-1657, CVE-2020-1682, CVE-2020-1679, CVE-2020-1661, CVE-2019-15875, CVE-2019-5599, CVE-2019-11477, CVE-2019-11478, CVE-2019-11479)
Description	Juniper has released security patch updates addressing multiple vulnerabilities that exists in Junos OS which is a FreeBSD-based operating system used in Juniper Networks routers. Successful exploitation of the most severe of these vulnerabilities could result in the attacker gaining control of the affected system. The product owners are advised to apply necessary patches at earliest to avoid such issues.
Affected Products	Multiple Junos OS versions
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://kb.juniper.net/InfoCenter/index?page=content&id=JSA11053 https://kb.juniper.net/InfoCenter/index?page=content&id=JSA11054 https://kb.juniper.net/InfoCenter/index?page=content&id=JSA11049 https://kb.juniper.net/InfoCenter/index?page=content&id=JSA11050 https://kb.juniper.net/InfoCenter/index?page=content&id=JSA11079 https://kb.juniper.net/InfoCenter/index?page=content&id=JSA11076 https://kb.juniper.net/InfoCenter/index?page=content&id=JSA11056&actp=RSS https://kb.juniper.net/InfoCenter/index?page=content&id=JSA11046

Affected Product	IBM
Severity	**High**
Affected Vulnerability	Bypass Sanitation (CVE-2020-10693)
Description	IBM has released security patch updates addressing a vulnerability found in Hibernate Validator version 6.1.2 and it could allow a remote attacker to bypass security restrictions which is caused by a flaw in the message interpolation processor. An attacker could exploit this by sending a specially crafted request and bypass input sanitation (escaping, stripping) controls when handling user-controlled data in error messages. It is highly recommended to apply necessary security patches at earliest to avoid issues.
Affected Products	WebSphere Application Server Liberty17.0.0.3 - 20.0.0.10
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/6348216

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.