Advisory Alert

Alert Number: AAA20211116 **Date:** November 16, 2021

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
IBM	**Critical**	Multiple vulnerabilities
Ruby	**High**	Denial of service vulnerability

Description

Affected Product	IBM
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2021-3711, CVE-2021-28165)
Description	IBM has released security updates addressing multiple vulnerabilities that exists in their products. CVE-2021-3711 – Successful exploitation could lead a remote attacker to cause buffer overflow and execute arbitrary codes on the system /cause an application crash by sending specially crafted SM2 content CVE-2021-28165 - Due to improper input validation Eclipse Jetty is vulnerable to a denial of service. A remote attacker could exploit this vulnerability by sending a specially-crafted TLS frame and cause CPU resources to reach to 100% usage It is highly recommended by IBM to apply necessary security fixes at earliest to avoid issues.
Affected Products	WebSphere MQ V5.3 for HP NonStop Server (MIPS and Itanium) 5.3.1 IBM MQ 9.0, 9.1, 9.2 LTS IBM MQ 9.1, 9.2 CD
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/6516398 https://www.ibm.com/support/pages/node/6516422

Affected Product	Ruby
Severity	**High**
Affected Vulnerability	Denial of service vulnerability (CVE-2021-41817)
Description	Ruby has released security updates addressing regular expression denial of service vulnerability that exists in their products. The Date's parsing methods including Date.parse are using Regexps internally, some of which are vulnerable against regular expression denial of service. An attacker could cause DOS attack by exploiting this vulnerability. Ruby highly recommends to apply necessary security fixes at earliest to avoid issues.
Affected Products	date gem 2.0.0 or prior (which are bundled versions with Ruby 2.6 series) date gem 3.0.1 or prior (which are bundled versions with Ruby 2.7 series) date gem 3.1.1 or prior (which are bundled versions with Ruby 3.0 series) date gem 3.2.0 or prior
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ruby-lang.org/en/news/2021/11/15/date-parsing-method-regexp-dos-cve-2021-41817/

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.