



# Advisory Alert

Alert Number : AAA20210129

Date : January 29, 2021

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

## Overview

Product	Severity	Vulnerability
IBM QRadar SIEM	High	Multiple Vulnerabilities

## Description

Affected Product	IBM QRadar SIEM
Severity	High
Affected Vulnerabilities	Multiple Vulnerabilities ( CVE-2020-5421, CVE-2020-11979, CVE-2019-19126, CVE-2020-10754, CVE-2019-19956, CVE-2019-20388, CVE-2020-7595, CVE-2019-5482, CVE-2018-20843, CVE-2019-15903, CVE-2019-20386, CVE-2019-16935, CVE-2020-8492, CVE-2019-17498, CVE-2019-2974, CVE-2020-2752, CVE-2020-2780, CVE-2020-2812, CVE-2019-14907, CVE-2019-14866, CVE-2020-4787, CVE-2020-4789, CVE-2019-2974, CVE-2020-2574, CVE-2020-2752, CVE-2020-2780, CVE-2020-2812, CVE-2019-14973, CVE-2019-17546, CVE-2019-17498, CVE-2017-15715, CVE-2018-1283, CVE-2018-1303, CVE-2019-10098, CVE-2020-1927, CVE-2020-1934, CVE-2019-5094, CVE-2019-5188, CVE-2020-0034, CVE-2018-18074, CVE-2018-20060, CVE-2019-11236, CVE-2019-11324, CVE-2019-5094, CVE-2018-18074, CVE-2018-20060, CVE-2019-11236, CVE-2019-11324, CVE-2019-5094, CVE-2019-5188, CVE-2020-11008, CVE-2019-12450, CVE-2019-14822, CVE-2019-14973, CVE-2019-17546, CVE-2017-15715, CVE-2018-1283, CVE-2018-1303, CVE-2019-10098, CVE-2020-1927, CVE-2020-1934, CVE-2017-18551, CVE-2018-20836, CVE-2019-15217, CVE-2019-15807, CVE-2019-15917, CVE-2019-16231, CVE-2019-16233, CVE-2019-16994, CVE-2019-17053, CVE-2019-17055, CVE-2019-19046, CVE-2019-19062, CVE-2019-19063, CVE-2019-19332, CVE-2019-19447, CVE-2019-19524, CVE-2019-19530, CVE-2019-19534, CVE-2019-19537, CVE-2019-19767, CVE-2019-19807, CVE-2019-20054, CVE-2019-20636, CVE-2019-9454, CVE-2019-9458, CVE-2020-10690, CVE-2020-10732, CVE-2020-10742, CVE-2020-10751, CVE-2020-10942, CVE-2020-4888 )
Description	IBM has released security patch updates addressing multiple vulnerabilities that exists in QRadar SIEM products. An attacker could exploit these vulnerabilities to perform various malicious activities on an affected system. IBM highly recommends to apply relevant patches at earliest to avoid issues.
Affected Products	IBM QRadar SIEM 7.4.2 GA to 7.4.2 Patch 1 IBM QRadar SIEM 7.4.0 to 7.4.1 Patch 1 IBM QRadar SIEM 7.3.0 to 7.3.3 Patch 5
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	<a href="https://www.ibm.com/support/pages/node/6408868">https://www.ibm.com/support/pages/node/6408868</a> <a href="https://www.ibm.com/support/pages/node/6408860">https://www.ibm.com/support/pages/node/6408860</a> <a href="https://www.ibm.com/support/pages/node/6408848">https://www.ibm.com/support/pages/node/6408848</a> <a href="https://www.ibm.com/support/pages/node/6408864">https://www.ibm.com/support/pages/node/6408864</a> <a href="https://www.ibm.com/support/pages/node/6408862">https://www.ibm.com/support/pages/node/6408862</a> <a href="https://www.ibm.com/support/pages/node/6408858">https://www.ibm.com/support/pages/node/6408858</a> <a href="https://www.ibm.com/support/pages/node/6408856">https://www.ibm.com/support/pages/node/6408856</a> <a href="https://www.ibm.com/support/pages/node/6409306">https://www.ibm.com/support/pages/node/6409306</a> <a href="https://www.ibm.com/support/pages/node/6408860">https://www.ibm.com/support/pages/node/6408860</a>

## 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.