Advisory Alert

Alert Number: AAA20201222 **Date:** December 22, 2020

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
IBM QRadar SIEM	**Medium**	Information Disclosure

Description

Affected Product	IBM QRadar SIEM
Severity	**Medium**
Affected Vulnerability	Information Disclosure (CVE-2019-12415, CVE-2017-12626)
Description	IBM has released security patch updates for addressing the information disclosure vulnerability Apache Poi as used by IBM QRadar SIEM products. **CVE-2019-12415** - Apache POI could allow a remote attacker to obtain sensitive information caused by an XML external entity (XXE) error when processing XML data. By sending a specially crafted document, a remote attacker could exploit this vulnerability to obtain sensitive information. **CVE-2017-12626 -** Apache POI is vulnerable to a denial of service caused by an error while parsing malicious Windows Metafile and Enhanced MetaFile and macros and specially crafted Microsoft Office files. By Accepting a victim to open a specially crafted file attacker could exploit this vulnerability to cause the out of memory exception
Affected Products	IBM QRadar SIEM 7.3 IBM QRadar SIEM 7.4
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/6391000

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.