Advisory Alert

Alert Number: AAA20221124 **Date:** November 24, 2022

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
IBM	**Critical**	Arbitrary Code Execution

Affected Product	**IBM**
Severity	**Critical**
Affected Vulnerability	Arbitrary Code Execution (CVE-2022-42889)
Description	IBM has released a security patch update addressing an arbitrary code execution vulnerability that exist in IBM QRadar SIEM. This vulnerability exists due to an insecure variable interpolation when processing untrusted input. A remote attacker can send a specially crafted input and execute arbitrary code on the target system. IBM recommends to apply the necessary patch updates at your earliest to avoid issues
Affected Products	IBM QRadar SIEM 7.4.0 – 7.4.3 Fix Pack 7 IBM QRadar SIEM 7.5.0 – 7.5.0 Update Pack 3 Interim Fix
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/6841021

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.