



Advisory Alert

Alert Number: AAA20230313

Date: March 13, 2023

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
IBM QRadar	Medium	Server side request forgery Vulnerability

Description

Affected Product	IBM QRadar
Severity	Medium
Affected Vulnerability	Server side request forgery Vulnerability (CVE-2022-43879)
Description	<p>IBM has released a Security Update addressing Server side request forgery vulnerability that exist in the IBM QRadar.</p> <p>The vulnerability exists due to insufficient validation of user-supplied input. A remote user can send unauthorized requests from the system, potentially leading to network enumeration or facilitating other attacks.</p> <p>IBM recommends to apply necessary security fixes at earliest to avoid issues.</p>
Affected Products	QRadar WinCollect Agent 10.0 - 10.1.2
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/6962775

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.