Advisory Alert

Alert Number: AAA20230126 **Date:** January 26, 2023

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
IBM	**High**	Multiple Vulnerabilities

Description

Affected Product	**IBM**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2022-43552, CVE-2022-43551)
Description	IBM has released security updates addressing multiple vulnerabilities that exist in the IBM QRadar Wincollect standalone agent. **CVE-2022-43552 –** A vulnerability that exist due to a use-after-free flaw when using an HTTP proxy in the cURL libcurl that used in IBM QRadar Wincollect standalone agent. A remote attacker can exploit this vulnerability by sending a specially-crafted request resulting a denial of service condition. **CVE-2022-43551** - A vulnerability that exist due to a flaw when the host name in the given URL first uses IDN characters that get replaced to ASCII counterparts as part of the IDN conversion in the cURL libcurl that used in IBM QRadar Wincollect standalone agent. A remote attacker can exploit this vulnerability by sending a specially-crafted request resulting HSTS check bypass. IBM recommends to apply the necessary patch updates to at your earliest to avoid issues.
Affected Products	QRadar WinCollect Agent version 10.0 - 10.1.1
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/6857685

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.