



Advisory Alert

Alert Number: AAA20230609

Date: June 9, 2023

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
IBM	Critical	Authentication bypass vulnerabilities
IBM	High , Medium , Low	Multiple vulnerabilities

Description

Affected Product	IBM
Severity	Critical
Affected Vulnerability	Authentication bypass vulnerabilities (CVE-2023-27535, CVE-2023-27536)
Description	<p>IBM has released a security update addressing multiple Authentication bypass vulnerabilities that exist in their products.</p> <p>CVE-2023-27535 - A flaw in cURL libcurl could enable a remote attacker to bypass security restrictions. This vulnerability is caused by an FTP connection reuse flaw. An attacker can exploit this vulnerability by sending a specifically crafted request to reuse a previously established FTP connection.</p> <p>CVE-2023-27536 - A flaw in cURL libcurl could enable a remote attacker to bypass security restrictions. This vulnerability is caused by GSS delegation reuse flaw. An attacker can exploit this vulnerability by sending a specifically crafted request to reuse a previously established created connection even when the GSS delegation.</p> <p>IBM highly recommends to apply the necessary patch updates at your earliest to avoid issues.</p>
Affected Products	QRadar WinCollect Agent 10.0 - 10.1.3
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/7002501

Affected Product	IBM
Severity	High ,Medium ,Low
Affected Vulnerability	Multiple vulnerabilities (CVE-2023-21930, CVE-2023-21967, CVE-2023-21954, CVE-2023-21968, CVE-2023-21937, CVE-2023-21938, CVE-2023-27533, CVE-2023-27537, CVE-2023-27538, CVE-2023-27534)
Description	<p>IBM has released security updates addressing multiple vulnerabilities that exist in their products. Successful exploitation of these vulnerabilities could lead to denial of service, sensitive information disclosure, Authentication bypass.</p> <p>IBM recommends to apply the necessary patch updates at your earliest to avoid issues</p>
Affected Products	WebSphere Service Registry and Repository 8.5.x WebSphere Service Registry and Repository Studio 8.5.x QRadar WinCollect Agent 10.0 - 10.1.3
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/7002501 https://www.ibm.com/support/pages/node/7002387

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.