



Advisory Alert

Alert Number: AAA20221004

Date: October 4, 2022

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Dell	Critical	Multiple Vulnerabilities
IBM	High	Spoofing Vulnerability

Description

Affected Product	Dell
Severity	Critical
Affected Vulnerability	Multiple Vulnerabilities (CVE-2022-0778, CVE-2020-1971, CVE-2021-3711, CVE-2021-3712)
Description	<p>Dell has released a security update addressing multiple vulnerabilities that exist in the third party component named Openssl that is used in Dell EMC RecoverPoint products. The vulnerabilities could be exploited by malicious users to compromise the affected system.</p> <p>Dell highly recommends to apply necessary fixes at earliest to avoid issues</p>
Affected Products	RecoverPoint for Virtual machines 5.3 SP3 RecoverPoint for Virtual machines 5.3 SP2 P4 RecoverPoint for Virtual machines 5.3 SP2 P3 RecoverPoint for Virtual machines 5.3 SP2 P2 RecoverPoint for Virtual machines 5.3 SP2 P1 RecoverPoint for Virtual machines 5.3 SP1 P1 RecoverPoint for Virtual machines 5.3 SP2 RecoverPoint for Virtual machines 5.3 SP1 RecoverPoint for Virtual machines 5.3
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.dell.com/support/kbdoc/en-us/000203943/dsa-2022-275-dell-emc-recoverpoint-security-update-for-openssl-security-vulnerability

Affected Product	IBM
Severity	High
Affected Vulnerability	Spoofing Vulnerability (CVE-2019-11777)
Description	<p>IBM has released a security update addressing a spoofing vulnerability that exists in the Eclipse Paho library used by IBM WebSphere Application Server Liberty with the rtcomm-1.0 or rtcommGateway-1.0 feature enabled.</p> <p>An attacker could avoid security restrictions as a result of the Eclipse Paho Java client failing to check the result when connecting to an MQTT server using TLS and setting a host name verifier. An attacker could specially craft a request to allow one MQTT server to impersonate another and provide the client library with incorrect information.</p> <p>IBM recommends to apply necessary security fixes at your earliest to avoid issues.</p>
Affected Products	ICP - IBM Match 360 all versions
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/6825899

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.

Financial Sector Computer Security Incident Response Team (FinCSIRT)

LankaClear Pvt Ltd, Level 18, Bank of Ceylon Head Office, BOC Square, 01 Bank of Ceylon Mawatha, Colombo 00100, Sri Lanka
Hotline: + 94 112039777

Public Circulation Permitted | Public

Report incident to incident@fincsirt.lk

TLP: WHITE