Advisory Alert

Alert Number: AAA20220620 **Date:** June 20, 2022

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
IBM	**High**	Multiple Vulnerabilities
PaloAlto	**Medium**	Weak Cryptographic Algorithm

Description

Affected Product	**IBM**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2022-1434, CVE-2022-1343, CVE-2022-1292, CVE-2022-1473, CVE-2021-22947, CVE-2022-22576, CVE-2021-22945, CVE-2022-27774, CVE-2022-0778, CVE-2022-27776, CVE-2021-22946, CVE-2022-27775, CVE-2021-3712)
Description	IBM has released security updates addressing multiple vulnerabilities that exists in IBM QRadar that could cause man in the middle attack, bypass security restrictions, obtain sensitive information, execute arbitrary commands and denial of service in systems with affected versions. IBM highly recommends to apply necessary security fixes at earliest to avoid issue
Affected Products	QRadar WinCollect Agent 10.0 QRadar WinCollect Agent 10.0.1
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/6596085

Affected Product	**PaloAlto**
Severity	**Medium**
Affected Vulnerability	Weak Cryptographic Algorithm (CVE-2022-0022)
Description	PaloAlto has released security updates addressing Weak Cryptography flaw that exists in their products Due to this flaw in PaloAlto Network PAN-OS software where the password hashes of administrator and local user accounts are not created with a sufficient level of computational effort allowing to crack passwords on accounts in normal (non-FIPS-CC) operational mode.
Affected Products	PAN-OS 8.1 versions earlier than PAN-OS 8.1.21 All versions of PAN-OS 9.0 PAN-OS 9.1 versions earlier than PAN-OS 9.1.11; PAN-OS 10.0 versions earlier than PAN-OS 10.0.7c
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://security.paloaltonetworks.com/CVE-2022-0022

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.