Advisory Alert

Alert Number: AAA20220824 **Date:** August 24, 2022

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
IBM	**Critical**	Multiple Vulnerabilities
VMware	**High**	Local Privilege Escalation Vulnerability

Description

Affected Product	**IBM**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities(CVE-2021-43859, CVE-2022-24407, CVE-2021-22060, CVE-2021-3677,CVE-2022-22720, CVE-2021-28169, CVE-2021-34428, CVE-2021-28163, CVE-2021-28164, CVE-2021-34429, CVE-2021-28165, CVE-2021-45960, CVE-2021-46143, CVE-2022-22822, CVE-2022-22823, CVE-2022-22824, CVE-2022-22825, CVE-2022-22826, CVE-2022-22827, CVE-2022-23852, CVE-2022-25235, CVE-2022-25236, CVE-2022-25315, CVE-2021-4083)
Description	IBM has released a critical security update addressing multiple vulnerabilities that exist in the components that are used by the QRadar SIEM product. Successful exploitation of these vulnerabilities could cause denial of service, SQL injection, security restrictions bypass, sensitive information disclosure, HTTP request smuggling, Arbitrary code execution and privilege escalation. IBM highly recommends to apply the available patch updates at earliest to avoid issues.
Affected Products	IBM QRadar SIEM 7.3.0 - 7.3.3 Fix Pack 11 IBM QRadar SIEM 7.4.0 - 7.4.3 Fix Pack 5 IBM QRadar SIEM 7.5.0 - 7.5.0 Update Pack 1
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/blogs/psirt/security-bulletin-ibm-qradar-siem-includes-components-with-multiple-known-vulnerabilities/

Affected Product	**VMware**
Severity	**High**
Affected Vulnerability	Local Privilege Escalation Vulnerability (CVE-2022-31676)
Description	VMware has released security update addressing a local privilege escalation vulnerability that exist in VMware Tools. Using this vulnerability, a malicious actor with local non-administrative access to the guest OS can escalate privileges as a root in the virtual machine. VMware highly recommends to apply the available patch updates at earliest to avoid issues.
Affected Products	VMware tools on Windows version 11.x.y, 12.x.y VMware tools on Linux version 10.x.y , 11.x.y, 12.x.y
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.vmware.com/security/advisories/VMSA-2022-0024.html

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.