Advisory Alert

Alert Number: **AAA202306023** **Date:** **June 23, 2023**

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
VMware	**High**	Multiple Memory Corruption Vulnerabilities
IBM	**High**	Multiple Vulnerabilities

Description

Affected Product	**VMware**
Severity	**High**
Affected Vulnerability	Multiple Memory Corruption Vulnerabilities (CVE-2023-20892, CVE-2023-20893, CVE-2023-20894, CVE-2023-20895, CVE-2023-20896)
Description	VMware has released a security update addressing multiple memory corruption vulnerabilities affecting their products. Exploitation of the most severe vulnerabilities could lead to heap-overflow, Server use-after-free, out-of-bounds write, out-of-bounds read VMware recommends to apply the necessary patch updates at your earliest to avoid issues
Affected Products	vCenter Server 8.0 vCenter Server 7.0
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.vmware.com/security/advisories/VMSA-2023-0014.html

Affected Product	**IBM**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-26276, CVE-2023-26274, CVE-2023-26273, CVE-2020-35491, CVE-2018-7489, CVE-2020-35490, CVE-2020-36518, CVE-2020-11971, CVE-2020-13955, CVE-2022-39135, CVE-2022-34352)
Description	IBM has released security updates addressing multiple vulnerabilities that exist in IBM QRadar SIEM product. Successful exploitation of these vulnerabilities could lead to decryption of highly sensitive information, credentials disclosure, performance of unauthorized actions; read arbitrary files, denial of service, SSRF attack, Information disclosure IBM recommends to apply the necessary patch updates at your earliest to avoid issues
Affected Products	IBM QRadar SIEM 7.5.0 - 7.5.0 UP5
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/7006081 https://www.ibm.com/support/pages/node/7006085 https://www.ibm.com/support/pages/node/7006083 https://www.ibm.com/support/pages/node/7006069 https://www.ibm.com/support/pages/node/7006057

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.