TLP: WHITE

Advisory Alert

Alert Number: **AAA20230707** **Date:** **July 7, 2023**

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
IBM	**High**	Multiple Vulnerabilities
VMware	**Medium**	Authentication Bypass Vulnerability

Description

Affected Product	**IBM**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-24329, CVE-2023-1436, CVE-2023-0286, CVE-2019-9740, CVE-2021-3737, CVE-2022-0391, CVE-2022-45061, CVE-2021-23336, CVE-2018-20060, CVE-2021-28861, CVE-2019-18348, CVE-2020-26116, CVE-2021-3733, CVE-2015-20107, CVE-2023-20860, CVE-2019-8331, CVE-2016-10735, CVE-2022-40150, CVE-2022-45685, CVE-2022-40149, CVE-2022-45693, CVE-2023-28708, CVE-2023-24998, CVE-2022-43750, CVE-2022-40151, CVE-2023-1999, CVE-2022-34917, CVE-2023-25194, CVE-2021-43138, CVE-2022-4378, CVE-2022-42703, CVE-2023-0767, CVE-2015-0254, CVE-2022-38023, CVE-2022-37434, CVE-2022-23521, CVE-2022-41903, CVE-2023-20861, CVE-2023-20863)
Description	IBM has released a security update addressing multiple vulnerabilities that exist in IBM QRadar SIEM. These vulnerabilities could potentially be exploited by attackers to bypass security restrictions, execute arbitrary code, cause denial of service and sensitive 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/7010099

Affected Product	**VMware**
Severity	**Medium**
Affected Vulnerability	Authentication Bypass Vulnerability (CVE-2023-20899)
Description	VMware has a released security update addressing an Authentication bypass vulnerability that exists in VMware SD-WAN. This vulnerability allows an unauthenticated attacker to download the Diagnostic bundle of the application under VMware SD-WAN Management. VMware recommends to apply the necessary patch updates at your earliest to avoid issues
Affected Products	VMware SD-WAN (Edge) 5.0.x VMware SD-WAN (Edge) 4.5.x
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.vmware.com/security/advisories/VMSA-2023-0015.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.