Advisory Alert

Alert Number: AAA20230725 **Date:** July 25, 2023

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Ivanti	**Critical**	Remote Unauthenticated API Access Vulnerability
HPE	**High**	Denial Of Service Vulnerability
Citrix	**High**	Sensitive Information Disclosure Vulnerability
IBM	**Medium**, **Low**	Multiple Vulnerabilities

Description

Affected Product	**Ivanti**
Severity	**Critical**
Affected Vulnerability	Remote Unauthenticated API Access Vulnerability (CVE-2023-35078)
Description	Ivanti has released a security update addressing a Remote Unauthenticated API Access vulnerability within Ivanti Endpoint Manager Mobile (EPMM). If exploited, this vulnerability enables an unauthorized, remote (internet-facing) actor to potentially access users' personally identifiable information and make limited changes to the server. Ivanti highly recommends to apply the necessary patch updates at your earliest to avoid issues.
Affected Products	Ivanti Endpoint Manager Mobile (EPMM) 11.4 releases 11.10, 11.9, and 11.8 as well as older releases
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://forums.ivanti.com/s/article/CVE-2023-35078-Remote-unauthenticated-API-access-vulnerability?language=en_US

Affected Product	**HPE**
Severity	**High**
Affected Vulnerability	Denial Of Service Vulnerability (CVE-2023-24998)
Description	HPE has released a security update addressing a Denial of Service vulnerability within HPE IceWall Identity Manager running Apache Commons FileUpload. The vulnerability could be exploited remotely. HPE recommends to apply the necessary patch updates at your earliest to avoid issues.
Affected Products	IceWall Identity Manager 5.0 (RHEL and HP-UX) and 6.0 (RHEL and Windows) - using Apache Commons FileUpload
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbmu04496en_us

Affected Product	**Citrix**
Severity	**High**
Affected Vulnerability	Sensitive Information Disclosure Vulnerability (CVE-2023-20593)
Description	Citrix has released a security update addressing a sensitive information disclosure vulnerability within AMD Zen 2 CPUs running Citrix Hypervisor. Citrix recommends to apply the necessary patch updates at your earliest to avoid issues.
Affected Products	Citrix Hypervisor when running on AMD Zen 2 CPUs only
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.citrix.com/article/CTX566835/citrix-hypervisor-security-update-for-cve202320593

Affected Product	**IBM**
Severity	**Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-28319, CVE-2023-28320, CVE-2023-28321, CVE-2023-0466, CVE-2023-0465, CVE-2023-28322, CVE-2023-0464, CVE-2023-24534, CVE-2023-32342)
Description	IBM has released security updates addressing multiple vulnerabilities within their products. If exploited theses vulnerabilities could lead to Denial of Service, Sensitive information disclosure, Certification verification bypass, Policy checking bypass IBM recommends to apply the necessary patch updates at your earliest to avoid issues.
Affected Products	QRadar WinCollect Agent 10.0 - 10.1.5 IBM Storage Protect Server 8.1
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/7014253 https://www.ibm.com/support/pages/node/7014223 https://www.ibm.com/support/pages/node/7014225

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.