Advisory Alert

Alert Number: AAA20230822 **Date:** August 22, 2023

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Ivanti	**Critical**	API Authentication Vulnerabilities
Dell	**High**	Multiple Vulnerabilities
IBM	**High**	Path Traversal Vulnerability

Description

Affected Product	**Ivanti**
Severity	**Critical**
Affected Vulnerability	API Authentication vulnerabilities (CVE-2023-38035, CVE-2023-35078)
Description	Ivanti has released security updates addressing multiple API Authentication vulnerabilities that exists in their products. **CVE-2023-38035** - An API Authentication Bypass vulnerability in MICS Admin Portal in Ivanti MobileIron Sentry, may may allow an attacker to bypass authentication controls on the administrative interface due to an insufficiently restrictive Apache HTTPD configuration. **CVE-2023-35078** - An authentication bypass vulnerability in Ivanti EPMM allows unauthorized users to access restricted functionality or resources of the application without proper authentication. Ivanti recommends to apply the necessary security updates at earliest to avoid issues.
Affected Products	Ivanti Endpoint Manager Mobile (EPMM) Version 11.4 releases 11.10, 11.9 and 11.8. Older versions Ivanti MobileIron Sentry versions 9.18.0 and below
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://forums.ivanti.com/s/article/CVE-2023-38035-API-Authentication-Bypass-on-Sentry-Administrator-Interface?language=en_US https://forums.ivanti.com/s/article/CVE-2023-35078-Remote-unauthenticated-API-access-vulnerability?language=en_US

Affected Product	**Dell**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-0215, CVE-2022-4450, CVE-2023-0286, CVE-2022-4304)
Description	Dell has released security updates addressing multiple vulnerabilities that exists in third party components that in turn affect Dell products. Successful exploitation of the vulnerabilities could lead to denial of service attacks, reading of memory contents, sensitive data exposure and system crash. Dell recommends to apply necessary security fixes at earliest to avoid issues. We have already addressed these vulnerabilities of the third party components in the **AAA20230208** Advisory alert before.
Affected Products	PowerEdge T40 - BIOS Versions prior to 1.12.0
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.dell.com/support/kbdoc/en-us/000216897/dsa-2023-207-security-update-for-dell-poweredge-t40-mini-tower-server-openssl-vulnerabilities

Affected Product	**IBM**
Severity	**High**
Affected Vulnerability	Path Traversal Vulnerability (CVE-2022-31159)
Description	IBM has released security updates addressing a Path Traversal vulnerability affecting QRadar SIEM. Successful exploitation of the vulnerability may allow a remote authenticated attacker to traverse directories on the system, also the attacker could send a specially-crafted URL request containing "dot dot" sequences (/../) to write arbitrary files on the system. IBM recommends to apply necessary security fixes at earliest to avoid issues.
Affected Products	All AmazonWebServices versions before 7.5.0-QRADAR-PROTOCOL-AmazonWebServices-7.5-20230419193502.noarch.rpm All AmazonWebServices versions before 7.4.0-QRADAR-PROTOCOL-AmazonWebServices-7.4-20230419193457.noarch.rpm
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/7027598

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.