Advisory Alert

Alert Number: AAA20230814 **Date:** August 14, 2023

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Ivanti	**Critical**	Remote Unauthenticated API Access Vulnerability
PostgreSQL	**High**, Low	Multiple Vulnerabilities
Ubuntu	**High**, Medium, Low	Multiple Vulnerabilities

Description

Affected Product	**Ivanti**
Severity	**Critical**
Affected Vulnerability	Remote Unauthenticated API Access Vulnerability (CVE-2023-35082)
Description	Ivanti has released a security update addressing a Remote Unauthenticated API Access Vulnerability that exists in Ivanti Endpoint Manager Mobile (EPMM) due to an error when processing authentication requests within the API interface. A remote non-authenticated attacker can bypass authentication process and gain unauthorized access to the application. Ivanti highly recommends to apply the necessary patch updates at your earliest to avoid issues
Affected Products	Endpoint Manager Mobile (EPMM) 11.10, 11.9 and 11.8 and MobileIron Core 11.7 and below
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://forums.ivanti.com/s/article/CVE-2023-35082-Remote-Unauthenticated-API-Access-Vulnerability-in-MobileIron-Core-11-2-and-older?language=en_US

Affected Product	**PostgreSQL**
Severity	**High**, Low
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-39417, CVE-2023-39418)
Description	PostgreSQL has released security updates addressing multiple vulnerabilities that exist in their products. Successful exploitation of these vulnerabilities could lead to SQL injection and Privilege Escalation. **CVE-2023-39417-** SQL injection vulnerability exists due to insufficient sanitization of user-supplied data within the extension script @substitutions@, which uses @extowner@, @extschema@, or @extschema:...@ inside a quoting construct. A remote attacker can send a specially crafted request to the affected application and execute arbitrary SQL commands within the application database. **CVE-2023-39418-** Privilege Escalation vulnerability exists due to the MERGE command does not properly enforce UPDATE or SELECT row security policies. A remote user can read or update protected data. PostgreSQL recommends to apply the necessary security updates at earliest to avoid issues
Affected Products	PostgreSQL: 11.0 - 15.3
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.postgresql.org/support/security/CVE-2023-39417/ https://www.postgresql.org/support/security/CVE-2023-39418/

Affected Product	**Ubuntu**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2020-36691, CVE-2022-0168, CVE-2022-1184, CVE-2022-27672, CVE-2022-4269, CVE-2022-48502, CVE-2023-0590, CVE-2023-1611, CVE-2023-1855, CVE-2023-1990, CVE-2023-2002, CVE-2023-2124, CVE-2023-2194, CVE-2023-2269, CVE-2023-2640, CVE-2023-28466, CVE-2023-2898, CVE-2023-30772, CVE-2023-3111, CVE-2023-31248, CVE-2023-3141, CVE-2023-32248, CVE-2023-32254, CVE-2023-32629, CVE-2023-3268, CVE-2023-3312, CVE-2023-3317, CVE-2023-33203, CVE-2023-3390, CVE-2023-35001, CVE-2023-35823, CVE-2023-35824, CVE-2023-35826, CVE-2023-35828, CVE-2023-35829, CVE-2023-3609, CVE-2023-3610, CVE-2023-3611, CVE-2023-3776, CVE-2023-38430, CVE-2023-38432, CVE-2023-3863.)
Description	Ubuntu has released security updates addressing multiple vulnerabilities that exist in their products. Successful exploitation of these vulnerabilities could lead to Denial of service, sensitive information disclosure, Privilege Escalation. Ubuntu recommends to apply the necessary security updates at earliest to avoid issues
Affected Products	Ubuntu 23.04 Ubuntu 22.04 LTS Ubuntu 20.04 LTS Ubuntu 18.04 ESM
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://ubuntu.com/security/notices/USN-6285-1 https://ubuntu.com/security/notices/USN-6284-1 https://ubuntu.com/security/notices/USN-6283-1

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.