Advisory Alert

Alert Number: AAA20240319 **Date:** March 19, 2024

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Ivanti	**Critical**	SQL Injection Vulnerability
Red Hat	**High**, **Medium**	Multiple Vulnerabilities
Ubuntu	**High**, **Medium**, **Low**	Multiple Vulnerabilities

Description

Affected Product	**Ivanti**
Severity	**Critical**
Affected Vulnerability	SQL Injection vulnerability (CVE-2023-39336)
Description	Ivanti has issued a security update addressing a SQL Injection Vulnerability that exists in Ivanti Endpoint Manager. If exploited, an attacker with access to the internal network can leverage an unspecified SQL injection to execute arbitrary SQL queries and retrieve output without the need for authentication. This can then allow the attacker control over machines running the EPM agent. This applies to all instances of MSSQL. Additionally when the core server is configured to use Microsoft SQL Express, this might lead to RCE on the core server. Ivanti advises to apply security fixes at your earliest to protect your systems from potential threats.
Affected Products	All versions of EPM prior to 2022 SU5
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://forums.ivanti.com/s/article/SA-2023-12-19-CVE-2023-39336?language=en_US

Affected Product	**Red Hat**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-4921, CVE-2024-0646, CVE-2022-3545, CVE-2022-38096, CVE-2022-41858, CVE-2023-2166, CVE-2023-2176, CVE-2023-3611, CVE-2023-4459, CVE-2023-6817, CVE-2023-7192, CVE-2023-31436, CVE-2023-5678, CVE-2023-6710, CVE-2023-31122, CVE-2023-39615, CVE-2023-46218, CVE-2023-46219, CVE-2024-25062, CVE-2023-41080, CVE-2023-46589, CVE-2024-24549, CVE-2022-1471, CVE-2022-40151, CVE-2022-41966, CVE-2022-44729, CVE-2022-44730, CVE-2023-0482, CVE-2023-3635, CVE-2023-5072, CVE-2023-33201)
Description	Red Hat has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to cause Denial of Service, Use-after-free Condition, Information disclosure, Server-Side Request Forgery. Red Hat advises to apply security fixes at your earliest to protect your systems from potential threats.
Affected Products	Red Hat Enterprise Linux for x86_64 - Extended Update Support 8.8 x86_64 Red Hat Enterprise Linux for Power, little endian - Extended Update Support 8.8 ppc64le Red Hat Enterprise Linux Server - TUS 8.8 x86_64 Red Hat Enterprise Linux Server for Power LE - Update Services for SAP Solutions 8.8 ppc64le Red Hat Enterprise Linux for x86_64 - Update Services for SAP Solutions 8.8 x86_64 Red Hat Enterprise Linux Server - AUS 8.4 x86_64 Red Hat Enterprise Linux Server - TUS 8.4 x86_64 Red Hat Enterprise Linux Server for Power LE - Update Services for SAP Solutions 8.4 ppc64le Red Hat Enterprise Linux for x86_64 - Update Services for SAP Solutions 8.4 x86_64 Red Hat JBoss Core Services Text-Only Advisories x86_64 Red Hat JBoss Core Services 1 for RHEL 8 x86_64 Red Hat JBoss Core Services 1 for RHEL 7 x86_64 JBoss Enterprise Web Server Text-Only Advisories x86_64 JBoss Enterprise Web Server 5 for RHEL 9 x86_64 JBoss Enterprise Web Server 5 for RHEL 8 x86_64 JBoss Enterprise Web Server 5 for RHEL 7 x86_64 Red Hat JBoss Middleware Text-Only Advisories for MIDDLEWARE 1 x86_64
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://access.redhat.com/errata/RHSA-2024:1368 https://access.redhat.com/errata/RHSA-2024:1367 https://access.redhat.com/errata/RHSA-2024:1317 https://access.redhat.com/errata/RHSA-2024:1316 https://access.redhat.com/errata/RHSA-2024:1325 https://access.redhat.com/errata/RHSA-2024:1319 https://access.redhat.com/errata/RHSA-2024:1318 https://access.redhat.com/errata/RHSA-2024:1353

Affected Product	**Ubuntu**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-34256, CVE-2023-51781, CVE-2024-24855, CVE-2023-39197, CVE-2024-0775, CVE-2022-20567, CVE-2024-1086, CVE-2023-46838, CVE-2023-4132, CVE-2023-3006, CVE-2023-23000, CVE-2023-6121, CVE-2023-2002, CVE-2023-30456, CVE-2023-4921)
Description	Ubuntu has released security updates addressing multiple vulnerabilities that exist in Ubuntu Linux kernel. If exploited, these vulnerabilities could lead to Denial of Service, Arbitrary code execution and Sensitive information disclosure. Ubuntu advises to apply security fixes at your earliest to protect your systems from potential threats.
Affected Products	Ubuntu 14.04 Ubuntu 16.04 Ubuntu 18.04
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://ubuntu.com/security/notices/USN-6700-1 https://ubuntu.com/security/notices/USN-6701-1 https://ubuntu.com/security/notices/USN-6699-1

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.