Advisory Alert

Alert Number: **AAA20240105** **Date:** **January 5, 2024**

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Ivanti	**Critical**	SQL injection Vulnerability
IBM	**Critical**	Server-Side Request Forgery Vulnerability
IBM	**High ,** **Medium**	Denial of Service Vulnerability

Description

Affected Product	**Ivanti**
Severity	**Critical**
Affected Vulnerability	SQL injection Vulnerability (CVE-2023-39336)
Description	Ivanthi has released a security update addressing a SQL injection Vulnerability. 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. When the core server is configured to use SQL express, this might lead to RCE on the core server. Ivanthi recommends to apply the necessary patch updates at your earliest to avoid issues.
Affected Products	Ivanti Endpoint Manager 2021/EPM 2022 prior to 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	**IBM**
Severity	**Critical**
Affected Vulnerability	Server-Side Request Forgery Vulnerability (CVE-2022-2900)
Description	IBM has released security updates addressing multiple vulnerabilities that exists in IBM QRadar SIEM. Parse-url is vulnerable to server-side request forgery, caused by a flaw in the remote function. By sending a specially-crafted request, a remote attacker could exploit this vulnerability to conduct an SSRF attack, allowing the attacker to access or manipulate resources from the perspective of the affected server. IBM recommends to apply the necessary patch updates at your earliest to avoid issues.
Affected Products	IBM Security QRadar Analyst Workflow app 1.0.0 - 2.31.7
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://exchange.xforce.ibmcloud.com/vulnerabilities/236292

Affected Product	**IBM**
Severity	**High , Medium**
Affected Vulnerability	Denial of Service (CVE-2022-25883 , CVE-2022-25881, CVE-2022-24999)
Description	IBM has released security updates addressing multiple vulnerabilities that exist in their IBM Security QRadar Analyst Workflow App. CVE-2022-25883 - Node.js semver package is vulnerable to a denial of service, caused by a regular expression denial of service (ReDoS) flaw in the new Range function. By providing specially crafted regex input, a remote attacker could exploit this vulnerability to cause a denial of service. CVE-2022-25881 - Node.js http-cache-semantics module is vulnerable to a denial of service, caused by a regular expression denial of service (ReDoS) flaw. By sending a specially-crafted regex input using request header values, a remote attacker could exploit this vulnerability to cause a denial of service condition. CVE-2022-24999 - Express.js Express is vulnerable to a denial of service, caused by a prototype pollution flaw in qs. By adding or modifying properties of Object.prototype using a __proto__ or constructor payload, a remote attacker could exploit this vulnerability to cause a denial of service condition. IBM highly recommends to apply the necessary security updates at your earliest to avoid issues.
Affected Products	IBM Security QRadar Analyst Workflow app 1.0.0 - 2.31.7
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://exchange.xforce.ibmcloud.com/vulnerabilities/258647 https://exchange.xforce.ibmcloud.com/vulnerabilities/246089 https://exchange.xforce.ibmcloud.com/vulnerabilities/240815

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.