# Advisory Alert

**Alert Number:** AAA20230117 **Date:** January 17, 2023

**Document Classification Level :** Public Circulation Permitted | Public

**Information Classification Level :** TLP: WHITE

## Overview

| Product | Severity | Vulnerability |
|---|---|---|
| **IBM** | **High** | Information disclosure vulnerability |
| **Ubuntu** | **High, Medium** | Multiple vulnerabilities |

## Description

| | |
|---|---|
| Affected Product | **IBM** |
| Severity | **High** |
| Affected Vulnerability | Information disclosure vulnerability (CVE-2023-22875) |
| Description | IBM has released a security update addressing an Information disclosure vulnerability in their IBM Qradar SIEM. If exploited this vulnerability, A local user can access the webserver key and gain access to sensitive information.<br>**CVE-2023-22875-** The vulnerability exists due to incorrect default permissions for certificate key files used in the QRadar web user interface. QRadar SIEM copies the certificate key files used for SSL/TLS in the QRadar web user interface to manage hosts in the deployment that do not require a certificate key. A privileged user might be able to access the webserver key using these incorrect permission settings.<br>IBM recommends to apply the necessary fixes at your earliest to avoid issues. |
| Affected Products | IBM QRadar SIEM version 7.4<br>IBM QRadar SIEM version 7.5 |
| Officially Acknowledged by the Vendor | Yes |
| Patch/ Workaround Released | Yes |
| Reference | https://www.ibm.com/support/pages/node/6855643 |

| | |
|---|---|
| Affected Product | **Ubuntu** |
| Severity | **High, Medium** |
| Affected Vulnerability | Multiple vulnerabilities (CVE-2022-3643, CVE-2022-42896, CVE-2022-4378, CVE-2022-43945, CVE-2022-45934) |
| Description | Ubuntu has released a security update addressing Multiple vulnerabilities in their products. If exploited these vulnerabilities can lead to denial of service and arbitrary code execution.<br>Ubuntu recommends to apply the necessary patch updates at your earliest to avoid issues. |
| Affected Products | Ubuntu 14.04<br>Ubuntu 16.04<br>Ubuntu 18.04<br>Ubuntu 20.04<br>Ubuntu 22.04<br>Ubuntu 22.10 |
| Officially Acknowledged by the Vendor | Yes |
| Patch/ Workaround Released | Yes |
| Reference | https://ubuntu.com/security/notices/USN-5803-1<br>https://ubuntu.com/security/notices/USN-5804-1<br>https://ubuntu.com/security/notices/USN-5804-2 |

## 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.**