Advisory Alert

Alert Number: AAA20230330 **Date:** March 30, 2023

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Redhat	**High**	Multiple Vulnerabilities
IBM	**High**, **Medium**, **Low**	Multiple Vulnerabilities
Qnap	**High**, **Medium**, **Low**	Multiple Vulnerabilities
Ubuntu	**Medium**, **Low**	Multiple Vulnerabilities

Description

Affected Product	**Redhat**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2022-1471, CVE-2022-4492, CVE-2022-38752, CVE-2022-41853, CVE-2022-41854, CVE-2022-41881, CVE-2022-45787, CVE-2023-0482, CVE-2023-1108)
Description	Redhat has released security updates addressing multiple vulnerabilities that exists in the JBoss Enterprise Application Platform. Successful exploitation of these vulnerabilities could lead to Remote code execution, Denial of service, Information disclosure. Redhat recommends to apply necessary security fixes at earliest to avoid issues.
Affected Products	JBoss Enterprise Application Platform Text-Only Advisories x86_64
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://access.redhat.com/errata/RHSA-2023:1516

Affected Product	**IBM**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2022-1705, CVE-2022-1962, CVE-2022-23816, CVE-2022-23825, CVE-2022-2588, CVE-2022-26373, CVE-2022-27664 , CVE-2022-28131, CVE-2022-2879, CVE-2022-2880, CVE-2022-29900, CVE-2022-29901, CVE-2022-30580, CVE-2022-30629, CVE-2022-30630, CVE-2022-30631, CVE-2022-30632, CVE-2022-30633, CVE-2022-30635, CVE-2022-32148, CVE-2022-32189, CVE-2022-41715, CVE-2022-42898)
Description	IBM has released security updates addressing multiple vulnerabilities that exists in their products. Successful exploitation of these vulnerabilities could lead to Arbitrary code execution, Memory exhaustion, Information disclosure, Denial of service. IBM recommends to apply necessary security fixes at earliest to avoid issues.
Affected Products	IBM WebSphere Automation up to and including 1.5.1. IBM QRadar SIEM 7.5.0 - 7.5.0 UP4 IBM QRadar SIEM 7.4.3 GA - 7.4.3 FP8
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/6966998 https://www.ibm.com/support/pages/node/6967016

Affected Product	**Qnap**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2022-27597, CVE-2022-27598, CVE-2022-3437, CVE-2022-3592, CVE-2022-42898, CVE-2022-4304, CVE-2022-4450, CVE-2023-0215, CVE-2023-0286, CVE-2023-22809, CVE-2023-23355)
Description	Qnap has released security updates addressing multiple vulnerabilities that exists in their products. Successful exploitation of these vulnerabilities could lead to Privilege escalation, Denial of service, Buffer overflow, Sensitive information disclosure. Qnap recommends to apply necessary security fixes at earliest to avoid issues.
Affected Products	QNAP OS version prior QTS 5.0.1.2346 build 20230322 QNAP OS version prior QuTS hero h5.0.1.2348 build 20230324
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.qnap.com/go/security-advisory/qsa-23-15 https://www.qnap.com/go/security-advisory/qsa-23-11 https://www.qnap.com/go/security-advisory/qsa-23-10 https://www.qnap.com/go/security-advisory/qsa-23-06 https://www.qnap.com/go/security-advisory/qsa-23-03 https://www.qnap.com/go/security-advisory/qsa-23-02

Affected Product	**Ubuntu**
Severity	**Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-0210, CVE-2023-23454, CVE-2023-0266, CVE-2022-36280, CVE-2023-23559, CVE-2023-28328, CVE-2022-3424, CVE-2023-0045, CVE-2023-23455, CVE-2022-41218, CVE-2023-26606, CVE-2022-4382, CVE-2022-48423, CVE-2022-48424, CVE-2022-2196)
Description	Ubuntu has release security updates addressing Multiple Vulnerabilities that exist in their products. If exploited these vulnerabilities could lead to Sensitive information disclosure, Denial of service and Arbitrary code execution. Ubuntu recommends to apply necessary security fixes at earliest to avoid issues.
Affected Products	Ubuntu 22.04 Ubuntu 20.04
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://ubuntu.com/security/notices/USN-5987-1

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.