Advisory Alert

Alert Number: AAA20230517 **Date:** May 17, 2023

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

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

Description

Affected Product	**Redhat**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2021-26341, CVE-2021-33655, CVE-2021-33656, CVE-2021-46790, CVE-2022-1462, CVE-2022-1679, CVE-2022-1789, CVE-2022-20141, CVE-2022-2196, CVE-2022-25265, CVE-2022-2663, CVE-2022-3028, CVE-2022-30594, CVE-2022-30784, CVE-2022-30786, CVE-2022-30788, CVE-2022-30789, CVE-2022-3165, CVE-2022-3239, CVE-2022-3522, CVE-2022-3524, CVE-2022-3564, CVE-2022-3566, CVE-2022-3567, CVE-2022-3619, CVE-2022-3623, CVE-2022-3625, CVE-2022-3628, CVE-2022-3707, CVE-2022-39188, CVE-2022-39189, CVE-2022-41218, CVE-2022-4129, CVE-2022-41674, CVE-2022-42703, CVE-2022-42720, CVE-2022-42721, CVE-2022-42722, CVE-2022-43750, CVE-2022-47929, CVE-2023-0394, CVE-2023-0461, CVE-2023-1018, CVE-2023-1195, CVE-2023-1582, CVE-2023-23454)
Description	Redhat has released security updates addressing multiple vulnerabilities that exist in their products. Successful exploitation of these vulnerabilities could lead to Heap-based buffer overflow, Race condition, Use-after-free condition, memory corruption, Denial of Service. Redhat recommends to apply the necessary patch updates at your earliest to avoid issues.
Affected Products	Red Hat CodeReady Linux Builder for ARM 64 8 aarch64 Red Hat CodeReady Linux Builder for IBM z Systems 8 s390x Red Hat CodeReady Linux Builder for Power, little endian 8 ppc64le Red Hat CodeReady Linux Builder for x86_64 8 x86_64 Red Hat Enterprise Linux for ARM 64 8 aarch64 Red Hat Enterprise Linux for IBM z Systems 8 s390x Red Hat Enterprise Linux for Power, little endian 8 ppc64le Red Hat Enterprise Linux for x86_64 8 x86_64
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://access.redhat.com/errata/RHSA-2023:2951 https://access.redhat.com/errata/RHSA-2023:2757

Affected Product	**Ubuntu**
Severity	**Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2022-27672, CVE-2022-36280, CVE-2022-3707, CVE-2022-4129, CVE-2022-4842, CVE-2022-48423, CVE-2022-48424, CVE-2023-0210, CVE-2023-0394, CVE-2023-0458, CVE-2023-0459, CVE-2023-1073, CVE-2023-1074, CVE-2023-1075, CVE-2023-1078, CVE-2023-1118, CVE-2023-1513, CVE-2023-1652, CVE-2023-20938, CVE-2023-21102, CVE-2023-21106, CVE-2023-2162, CVE-2023-23454, CVE-2023-23455, CVE-2023-26544, CVE-2023-32269)
Description	Ubuntu has released security updates addressing multiple vulnerabilities that exist in their products. Successful exploitation of these vulnerabilities could lead to sensitive information disclosure, Denial of Service, Arbitrary code execution Ubuntu recommends to apply the necessary patch updates at your earliest to avoid issues.
Affected Products	Ubuntu 16.04 Ubuntu 18.04 Ubuntu 20.04 Ubuntu 22.04 Ubuntu 22.10
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://ubuntu.com/security/notices/USN-6079-1 https://ubuntu.com/security/notices/USN-6080-1 https://ubuntu.com/security/notices/USN-6081-1

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.