



Advisory Alert

Alert Number: AAA20230310

Date: March 10, 2023

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Redhat	High	Infinity Loop vulnerability
Ubuntu	High, Medium, Low	Multiple Vulnerabilities

Description

Affected Product	Redhat
Severity	High
Affected Vulnerability	Infinity Loop vulnerability (CVE-2023-1108)
Description	Redhat has released security updates addressing an infinity loop vulnerability that exist in their products. A flaw was found in undertow, caused by an unexpected handshake status updated in SslConduit, where the loop never terminates. As a result, it may lead to denial of service Redhat recommends to apply necessary security fixes at earliest to avoid issues
Affected Products	JBoss Enterprise Application Platform 7.4 for RHEL 9 x86_64 JBoss Enterprise Application Platform 7.4 for RHEL 8 x86_64 JBoss Enterprise Application Platform 7.4 for RHEL 7 x86_64 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-2023:1185 https://access.redhat.com/errata/RHSA-2023:1184

Affected Product	Ubuntu
Severity	High, Medium, Low
Affected Vulnerability	Multiple Vulnerabilities (CVE-2022-3169, CVE-2022-3344, CVE-2022-3424, CVE-2022-3435, CVE-2022-3521, CVE-2022-3545, CVE-2022-3623, CVE-2022-36280, CVE-2022-41218, CVE-2022-4139, CVE-2022-42328, CVE-2022-42329, CVE-2022-4379, CVE-2022-45869, CVE-2022-47518, CVE-2022-47519, CVE-2022-47520, CVE-2022-47521, CVE-2022-47929, CVE-2023-0045, CVE-2023-0179, CVE-2023-0266, CVE-2023-0394, CVE-2023-0461, CVE-2023-0468, CVE-2023-20938, CVE-2023-23454, CVE-2023-23455)
Description	Ubuntu has released security updates addressing multiple vulnerabilities that exist in their products. Exploitation of these vulnerabilities can lead to Information disclosure, denial of service and arbitrary code execution. Ubuntu recommends to apply necessary security fixes at earliest to avoid issues
Affected Products	Ubuntu 18.04 Ubuntu 22.04
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://ubuntu.com/security/notices/USN-5941-1 https://ubuntu.com/security/notices/USN-5940-1

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.

Financial Sector Computer Security Incident Response Team (FinCSIRT)

LankaPay Pvt Ltd, Level 18, Bank of Ceylon Head Office, BOC Square, 01 Bank of Ceylon Mawatha, Colombo 00100, Sri Lanka
Hotline: + 94 112039777

Public Circulation Permitted | Public

Report incident to incident@fincsirt.lk

TLP: WHITE