Advisory Alert

Alert Number: AAA20230531 **Date:** May 31, 2023

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Redhat	**High**	Use-after-free Vulnerability
Ubuntu	**High**, **Medium**, **Low**	Multiple Vulnerabilities
Zimbra	**High**, **Medium**, **Low**	Multiple Vulnerabilities
IBM	**High**, **Medium**, **Low**	Multiple Vulnerabilities
Joomla	**Medium**	Brute Force Vulnerability
OpenSSL	**Medium**	Denial of Service Vulnerability

Description

Affected Product	**Redhat**
Severity	**High**
Affected Vulnerability	Use-after-free Vulnerability (CVE-2023-32233)
Description	Redhat has released security updates addressing a Use-after-free vulnerability that exists in their products. **CVE-2023-32233** - A use-after-free vulnerability exist in Netfilter subsystem of the Linux kernel when processing batch requests to update nf_tables configuration. A local user (with CAP_NET_ADMIN capability) could use this flaw to crash the system or potentially escalate their privileges on the system. Redhat recommends to apply the necessary patch updates at your earliest to avoid issues.
Affected Products	Red Hat Enterprise Linux for Real Time 8 x86_64 Red Hat Enterprise Linux for Real Time for NFV 8 x86_64 Red Hat Enterprise Linux for Real Time - Telecommunications Update Service 8.8 x86_64 Red Hat Enterprise Linux for Real Time for NFV - Telecommunications Update Service 8.8 x86_64
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://access.redhat.com/errata/RHSA-2023:3350

Affected Product	**Ubuntu**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-30456, CVE-2023-32233, CVE-2023-2612, CVE-2022-4139, CVE-2022-3586, CVE-2023-1670, CVE-2023-26606)
Description	Ubuntu has released security updates addressing multiple vulnerabilities that exists 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 22.04 Ubuntu 18.04
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://ubuntu.com/security/notices/USN-6124-1 https://ubuntu.com/security/notices/USN-6123-1 https://ubuntu.com/security/notices/USN-6122-1 https://ubuntu.com/security/notices/USN-6118-1

Affected Product	**Zimbra**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Multiple vulnerabilities (CVE-2023-34193, CVE-2023-29381, CVE-2023-25690, CVE-2023-29382, CVE-2022-46364, CVE-2022-22970, CVE-2023-34192)
Description	Zimbra has released security updates addressing multiple vulnerabilities that exists in their products. Successful exploitation of these vulnerabilities could lead to Cross-site Scripting (XSS), Authentication bypass, Server-Side Request Forgery (SSRF) Zimbra recommends to apply the necessary patch updates at your earliest to avoid issues.
Affected Products	Zimbra Collaboration Joule 8.8.15 Zimbra Collaboration Kepler 9.0.0 Zimbra Collaboration Daffodil 10.0.1
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://wiki.zimbra.com/wiki/Zimbra_Releases/8.8.15/P40#Security_Fixes https://wiki.zimbra.com/wiki/Zimbra_Releases/9.0.0/P33#Security_Fixes https://wiki.zimbra.com/wiki/Zimbra_Releases/10.0.1

Affected Product	**IBM**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Multiple vulnerabilities (CVE-2022-40897, CVE-2023-25577, CVE-2023-23934, CVE-2022-24736, CVE-2022-35977, CVE-2023-22458, CVE-2022-24999, CVE-2018-20801, CVE-2021-29489)
Description	IBM has released security updates addressing multiple vulnerabilities that exists in their products. Successful exploitation of these vulnerabilities could lead to Denial of Service, Integer overflow, Cross-site Scripting (XSS). IBM recommends to apply the necessary patch updates at your earliest to avoid issues.
Affected Products	QRadar Advisor 2.5 - 2.6.4
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/6999327

Affected Product	**Joomla**
Severity	**Medium**
Affected Vulnerability	Brute Force Vulnerability (CVE-2023-23755)
Description	Joomla has released a security update for a Brute force vulnerability that exists in their products. **CVE-2023-23755** - An issue was discovered in Joomla! 4.2.0 through 4.3.1. The lack of rate limiting allowed brute force attacks against MFA methods. Joomla recommends to apply the necessary patch updates at your earliest to avoid issues.
Affected Products	Joomla! CMS versions 4.2.0-4.3.1
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://developer.joomla.org/security-centre/900-20230502-core-bruteforce-prevention-within-the-mfa-screen.html

Affected Product	**OpenSSL**
Severity	**Medium**
Affected Vulnerability	Denial of Service Vulnerability (CVE-2023-2650)
Description	OpenSSL has released a security update for a denial of service vulnerability that exists in their products. **CVE-2023-2650** – OpenSSL may lead to a Denial of Service, when processing crafted ASN.1 object identifiers. OpenSSL recommends to apply the necessary patch updates at your earliest to avoid issues.
Affected Products	OpenSSL 3.0 OpenSSL 3.1 OpenSSL 1.1.1 OpenSSL 1.0.2
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.openssl.org/news/secadv/20230530.txt

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.