Advisory Alert

Alert Number: AAA20231020 **Date:** October 20, 2023

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Redhat	**High**	Multiple Vulnerabilities
Zimbra	**High**	Security updates
Cisco	**High**, Medium	Multiple Vulnerabilities
Apache	**Medium**	Multiple Vulnerabilities

Description

Affected Product	**Redhat**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-34462, CVE-2023-40167, CVE-2023-41080, CVE-2023-44487)
Description	Redhat has released patch updates to address multiple flaws that exist in their products. Successful exploitation of these vulnerabilities could cause DDoS attack, Improper validation, Denial of service. Redhat highly recommends to apply necessary fixes to avoid issues.
Affected Products	Red Hat JBoss Middleware Text-Only Advisories for MIDDLEWARE 1 x86_64 JBoss Enterprise Application Platform Text-Only Advisories x86_64 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
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://access.redhat.com/errata/RHSA-2023:5946 https://access.redhat.com/errata/RHSA-2023:5945 https://access.redhat.com/errata/RHSA-2023:5922 https://access.redhat.com/errata/RHSA-2023:5920

Affected Product	**Zimbra**
Severity	**High**
Affected Vulnerability	Security updates (CVE-2020-7746)
Description	Zimbra has released security updates for their products. This affects the package chart.js before 2.9.4. The options parameter is not properly sanitized when it is processed. When the options are processed, the existing options (or the defaults options) are deeply merged with provided options. However, during this operation, the keys of the object being set are not checked, leading to a prototype pollution. Zimbra recommends to apply necessary updates to avoid issues.
Affected Products	Zimbra Collaboration Daffodil 10.0.5 Zimbra Collaboration Kepler 9.0.0 Zimbra Collaboration Joule 8.8.15
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://wiki.zimbra.com/wiki/Zimbra_Releases/10.0.5#Security_Fixes https://wiki.zimbra.com/wiki/Zimbra_Releases/9.0.0/P37#Security_Fixes https://wiki.zimbra.com/wiki/Zimbra_Releases/8.8.15/P44#Security_Fixes

Affected Product	**Cisco**
Severity	**High** , **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2021-1435, CVE-2023-44487)
Description	Cisco has released security updates addressing multiple vulnerabilities that exist in their products. If exploited these vulnerabilities could cause Command Injection, Denial of service (DoS). Cisco highly recommends to apply the necessary security updates at earliest to avoid issues.
Affected Products	Devices running a vulnerable version of Cisco IOS XE Software and had the web UI feature enabled Business Process Automation Crosswork Data Gateway IoT Field Network Director, formerly Connected Grid Network Management System Prime Infrastructure Prime Network Registrar IOx Fog Director Ultra Cloud Core - Session Management Function Unified Contact Center Domain Manager (CCDM) Unified Contact Center Management Portal (CCMP)
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-webcmdinjsh-UFJxTgZD https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-http2-reset-d8Kf32vZ

Affected Product	**Apache**
Severity	**Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-45802, CVE-2023-43622, CVE-2023-31122)
Description	Apache has released a security update to address multiple vulnerabilities in Apache HTTP Server. The vulnerabilities allows a remote attacker to perform a buffer overflow vulnerability and a resource consumption vulnerability. Apache recommends to apply the necessary security fixes at your earliest to avoid issues.
Affected Products	Apache HTTP Server 2.4.55 - 2.4.57
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://httpd.apache.org/security/vulnerabilities_24.html

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.