Advisory Alert

Alert Number: AAA20221111 **Date:** November 11, 2022

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Zimbra	**Critical**	Arbitrary file upload Vulnerability
Zimbra	**High**, **Medium**	Multiple Vulnerabilities

Description

Affected Product	**Zimbra**
Severity	**Critical**
Affected Vulnerability	Arbitrary file upload Vulnerability (CVE-2022-41352)
Description	Zimbra has released a Security Update addressing an Arbitrary file upload Vulnerability that exist in the Zimbra Collaboration (ZCS). **CVE-2022-41352** - An attacker can upload arbitrary files through amavisd via a cpio loophole (extraction to /opt/zimbra/jetty/webapps/zimbra/public) that can lead to incorrect access to any other user accounts Zimbra recommends to apply necessary security fixes at earliest to avoid issues.
Affected Products	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/9.0.0/P27#Security_Fixes https://wiki.zimbra.com/wiki/Zimbra_Releases/8.8.15/P34#Security_Fixes

Affected Product	**Zimbra**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2022-37393, CVE-2022-41348, CVE-2022-41350, CVE-2022-41349, CVE-2022-41351)
Description	Zimbra has released Security Updates addressing multiple Vulnerabilities that exist in their products. **CVE-2022-37393** - zimbra user to execute the zmslapd binary as root with arbitrary parameters. As part of its intended functionality, zmslapd can load a user-defined configuration file, which includes plugins in the form of .so files, which also execute as root. **CVE-2022-41348** - XSS can occur via the onerror attribute of an IMG element, leading to information disclosure. **CVE-2022-41350** - In Zimbra Collaboration Suite ZCS/h/search?action=voicemail&action=listen accepts a phone parameter that is vulnerable to Reflected XSS. This allows executing arbitrary JavaScript on the victim's machine. **CVE-2022-41349** - The URL at /h/compose accepts an attachUrl parameter that is vulnerable to Reflected XSS. This allows executing arbitrary JavaScript on the victim's machine. **CVE-2022-41351** - At the URL /h/calendar, one can trigger XSS by adding JavaScript code to the view parameter and changing the value of the uncheck parameter to a string (instead of default value of 10). Zimbra recommends to apply necessary security fixes at earliest to avoid issues
Affected Products	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/9.0.0/P27#Security_Fixes https://wiki.zimbra.com/wiki/Zimbra_Releases/8.8.15/P34#Security_Fixes

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.