Advisory Alert

Alert Number: AAA20221123 **Date:** November 23, 2022

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Zimbra	Medium, Low	Multiple Vulnerabilities

Affected Product	**Zimbra**
Severity	Medium, Low
Affected Vulnerability	Multiple Vulnerabilities (CVE-2022-26377, CVE-2022-20770, CVE-2022-20771)
Description	Zimbra has released security patch updates addressing Multiple Vulnerabilities that exist in their products. **CVE-2022-26377** - Interpretation of HTTP Requests (HTTP Request Smuggling) vulnerability in mod_proxy_ajp of Apache HTTP Server allows an attacker to smuggle requests to the AJP server it forwards requests to. This issue affects Apache HTTP Server Apache HTTP Server 2.4 version 2.4.53 and prior versions. **CVE-2022-20770** - A vulnerability in CHM file parser of Clam AntiVirus (ClamAV) versions 0.104.0 through 0.104.2 and LTS version 0.103.5 and prior versions could allow an unauthenticated, remote attacker to cause a denial of service condition on an affected device. **CVE-2022-20771 -** A vulnerability in the TIFF file parser of Clam AntiVirus (ClamAV) versions 0.104.0 through 0.104.2 and LTS version 0.103.5 and prior versions could allow an unauthenticated, remote attacker to cause a denial of service condition on an affected device. These vulnerabilities have been fixed in this Zimbra Collaboration Suite patch update.
Affected Products	Zimbra Collaboration Joule 8.8.15 Zimbra Collaboration Kepler 9.0.0
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://wiki.zimbra.com/wiki/Zimbra_Releases/8.8.15/P35#Security_Fixes https://wiki.zimbra.com/wiki/Zimbra_Releases/9.0.0/P28#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.