Advisory Alert

Alert Number: AAA20220729 **Date:** July 29, 2022

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Zimbra	Low	Multiple Vulnerabilities

Description

Affected Product	**Zimbra**
Severity	Low
Affected Vulnerability	Multiple vulnerabilities (CVE-2022-2068, CVE-2022-24407)
Description	Zimbra has released security updates addressing multiple vulnerabilities that exists in their Products. **CVE-2022-2068** - Due to a flaw that exists in the OpenSSL that is used by Zimbra, the c_rehash script where it possibly passed the file names of certificates being hashed to a command executed through the shell. Some operating systems distribute this script in a way that causes it to run automatically. On these kinds of operating systems, an attacker can execute arbitrary commands with the privileges of the script **CVE-2022-24407** - Due to an improper input validation vulnerability that exists as a result of the failure to properly escape SQL inputs in the SQL plugin shipped with Cyrus SASL that is used in the Zimbra, an attacker can execute arbitrary SQL commands and have the ability to change the passwords for other accounts leading to privilege escalation. Zimbra highly recommends to apply necessary 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/8.8.15/P33#Security_Fixes https://wiki.zimbra.com/wiki/Zimbra_Releases/9.0.0/P26#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.