Advisory Alert

Alert Number: AAA20211126 **Date:** November 26, 2021

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Zimbra	**High**	Multiple Vulnerabilities

Description

Affected Product	Zimbra
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2021-30641, CVE-2020-35452)
Description	Zimbra has released security patch updates addressing Multiple Vulnerabilities that exist in their products **CVE-2021-30641** - Apache HTTP Server versions 2.4.39 to 2.4.46 Unexpected matching behavior with 'MergeSlashes OFF' **CVE-2020-35452** - Apache HTTP Server versions 2.4.0 to 2.4.46 A specially crafted Digest nonce can cause a stack overflow in mod_auth_digest. The manipulation with an unknown input leads to a memory corruption vulnerability. The highest threat from this vulnerability is to data confidentiality and integrity as well as system availability.
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/9.0.0/P21#Security_Fixes https://wiki.zimbra.com/wiki/Zimbra_Releases/8.8.15/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.