# Advisory Alert

**Alert Number:** AAA20210701 **Date:** July 1, 2021

**Document Classification Level :** Public Circulation Permitted | Public

**Information Classification Level :** TLP: WHITE

## Overview

| Product | Severity | Vulnerability |
|---|---|---|
| **Zimbra** | **High** | Multiple Vulnerabilities |
| **cPanel** | **High** | Security Fixes |

## Description

| | |
|---|---|
| Affected Product | Zimbra |
| Severity | **High** |
| Affected Vulnerability | Multiple Vulnerabilities (CVE-2021-34807,CVE-2021-35209,CVE-2021-35208,CVE-2021-35207) |
| Description | Zimbra has released security patch updates addressing Multiple Vulnerabilities that exist in their products.The most severe could cause Open Redirect Vulnerability in preauth servlet,Proxy Servlet Open Redirect Vulnerability,Stored XSS Vulnerability in ZmMailMsgView.java Vulnerability, Scanner detects Cross Site Scripting Vulnerability.These vulnerabilities have been fixed in this Zimbra Collaboration Suite patch update |
| Affected Products | Prior to update ZCS 9.0.0 |
| Officially Acknowledged by the Vendor | Yes |
| Patch/ Workaround Released | Yes |
| Reference | https://wiki.zimbra.com/wiki/Security_Center#<br>https://wiki.zimbra.com/wiki/Zimbra_Releases/9.0.0/P16# |

| | |
|---|---|
| Affected Product | cPanel |
| Severity | **High** |
| Affected Vulnerability | Security Fixes (CVE-2021-35368) |
| Description | cPanel has released updates addressing security fixes that exist in Drupal ModSecurity OWASP rules. It is highly recommended to apply necessary fixes provided on the official cPanel website at the earliest to avoid these security issues and all cPanel users are encouraged to upgrade latest versions. |
| Affected Products | cPanel Drupal ModSecurity OWASP rules prior to June 30, 2021 |
| Officially Acknowledged by the Vendor | Yes |
| Patch/ Workaround Released | Yes |
| Reference | https://news.cpanel.com/easyapache-4-june-30-release/ |

## 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.**