# Advisory Alert

**Alert Number:** AAA20211124 **Date:** November 24, 2021

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

**Information Classification Level :** TLP: WHITE

## Overview

| Product | Severity | Vulnerability |
|---|---|---|
| **VMware** | **High** | Multiple Vulnerabilities |
| **cPanel** | **Medium** | Improper Input Validation Vulnerability |

## Description

| | |
|---|---|
| Affected Product | **VMware** |
| Severity | **High** |
| Affected Vulnerability | Multiple Vulnerabilities (CVE-2021-21980, CVE-2021-22049) |
| Description | VMware has released Security Updates addressing multiple vulnerabilities that exist with VMware products.<br>**CVE-2021-21980 -** A malicious actor with network access to port 443 on the vCenter Server may exploit the unauthorized arbitrary file read vulnerability in the vSphere Web Client (FLEX/Flash).<br>**CVE-2021-22049 -** The vSAN Web Client (vSAN UI) plug-in in the vSphere Web Client (FLEX/Flash) contains an SSRF (Server-Side Request Forgery) vulnerability. An attacker with network access to port 443 on the vCenter Server could exploit this flaw by accessing a URL request outside of the vCenter Server or internal service. |
| Affected Products | VMware vCenter Server (vCenter Server)<br>VMware Cloud Foundation (Cloud Foundation) |
| Officially Acknowledged by the Vendor | Yes |
| Patch/ Workaround Released | Yes |
| Reference | https://www.vmware.com/security/advisories/VMSA-2021-0027.html |

| | |
|---|---|
| Affected Product | **cPanel** |
| Severity | **Medium** |
| Affected Vulnerability | Improper Input Validation Vulnerability (CVE-2021-21707) |
| Description | cPanel has released an update for EasyApache 4, including new packages for EasyApache 4 with multiple PHP versions. This release addresses vulnerabilities related to CVE-2021-21707 which allows a remote attacker to inject arbitrary XML code. |
| Affected Products | All versions of PHP 8.0 through 8.0.12.<br>All versions of PHP 7.4 through 7.4.25.<br>All versions of PHP 7.3 through 7.3.32. |
| Officially Acknowledged by the Vendor | Yes |
| Patch/ Workaround Released | Yes |
| Reference | https://news.cpanel.com/easyapache-4-november-23-release-2/ |

## 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.**