# CVE Detail – CVE-2021-21972

The vSphere Client (HTML5) contains a remote code execution vulnerability in a vCenter Server plugin. A malicious actor with network access to port 443 may exploit this issue to execute commands with unrestricted privileges on the underlying operating system that hosts vCenter Server. This affects VMware vCenter Server (7.x before 7.0 U1c, 6.7 before 6.7 U3l and 6.5 before 6.5 U3n) and VMware Cloud Foundation (4.x before 4.2 and 3.x before 3.10.1.2).

## Threat-Mapped Scoring

Score: 1.8

Priority: P4 - Informational (Low)

## EPSS

EPSS Score: N/A

Percentile: 0.99844

## CVSS Scoring

CVSS v3.1 Score: 9.8

Severity: CRITICAL

## CISA KEV

KEV is present

## Mapped CWE(s)

* CWE-22: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')

## CAPEC(s)

* CAPEC-126: Path Traversal
* CAPEC-64: Using Slashes and URL Encoding Combined to Bypass Validation Logic
* CAPEC-76: Manipulating Web Input to File System Calls
* CAPEC-78: Using Escaped Slashes in Alternate Encoding
* CAPEC-79: Using Slashes in Alternate Encoding

## Affected Products

* cpe:2.3:a:vmware:cloud\_foundation:\*:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:vmware:cloud\_foundation:\*:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:vmware:vcenter\_server:6.5:-:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:vmware:vcenter\_server:6.5:a:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:vmware:vcenter\_server:6.5:b:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:vmware:vcenter\_server:6.5:c:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:vmware:vcenter\_server:6.5:d:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:vmware:vcenter\_server:6.5:e:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:vmware:vcenter\_server:6.5:f:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:vmware:vcenter\_server:6.5:update1d:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:vmware:vcenter\_server:6.5:update1e:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:vmware:vcenter\_server:6.5:update1g:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:vmware:vcenter\_server:6.5:update2:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:vmware:vcenter\_server:6.5:update2b:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:vmware:vcenter\_server:6.5:update2c:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:vmware:vcenter\_server:6.5:update2d:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:vmware:vcenter\_server:6.5:update2g:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:vmware:vcenter\_server:6.5:update3:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:vmware:vcenter\_server:6.5:update3d:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:vmware:vcenter\_server:6.5:update3f:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:vmware:vcenter\_server:6.5:update3k:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:vmware:vcenter\_server:6.7:-:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:vmware:vcenter\_server:6.7:a:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:vmware:vcenter\_server:6.7:b:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:vmware:vcenter\_server:6.7:d:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:vmware:vcenter\_server:6.7:update1:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:vmware:vcenter\_server:6.7:update1b:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:vmware:vcenter\_server:6.7:update2:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:vmware:vcenter\_server:6.7:update2a:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:vmware:vcenter\_server:6.7:update2c:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:vmware:vcenter\_server:6.7:update3:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:vmware:vcenter\_server:6.7:update3a:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:vmware:vcenter\_server:6.7:update3b:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:vmware:vcenter\_server:6.7:update3f:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:vmware:vcenter\_server:6.7:update3g:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:vmware:vcenter\_server:6.7:update3j:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:vmware:vcenter\_server:7.0:-:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:vmware:vcenter\_server:7.0:a:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:vmware:vcenter\_server:7.0:b:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:vmware:vcenter\_server:7.0:c:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:vmware:vcenter\_server:7.0:d:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:vmware:vcenter\_server:7.0:update1:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:vmware:vcenter\_server:7.0:update1a:\*:\*:\*:\*:\*:\*