Security Advisory 2021-025

Critical Vulnerability in VMWare vCenter Server

June 7, 2021 — v1.1

TLP:WHITE

History:

• 26/05/2021 — v1.0 – Initial publication
• 07/06/2021 — v1.1 – Update after PoC release

Summary

On the 25th of May 2021, VMware has revealed two vulnerabilities in vSphere Client (HTML5) with the updates to address these vulnerabilities [1]. One of the vulnerabilities (CVE-2021-21985) has a critical CVSSv3 score. It may allow an attacker to execute command with unrestricted privileges on the operating system that hosts vCenter Server.

As of the beginning of June, 2021, a proof-of-concept of a RCE exploit targeting the critical vulnerability has been published. This indicates imminent exploitation of this vulnerability in the wild.

Technical Details

The vulnerability tracked as CVE-2021-21985 was reported initially by Ricter Z. from 360 Noah Lab, and it can be remotely exploited by unauthenticated attackers in low complexity attacks which do not require user interaction [7].

A malicious actor with network access on port 443 of the vCenter Server appliances may execute command remotely with unrestricted privileges on the underlying host. This is due to a lack of input validation in the Virtual SAN Health Check plug-in, which is enabled by default. The severity of this issue has been evaluated with CVSSv3 score of 9.8 by VMware [1]. Additional information has also been provided by VMWare in [6].

At the beginning of June, Security Researchers have developed and published a proof-of-concept of a RCE exploit targeting CVE-2021-21985. Moreover, threat intelligence company has monitored attackers scanning actively for Internet-exposed VMware vCenter servers unpatched interface. According to Shodan, thousands of vCenter servers are still reachable from the Internet and may be vulnerable to CVE-2021-21985 [8].
Affected Products

The following products are affected by the vulnerabilities:

<table>
<thead>
<tr>
<th>Product</th>
<th>Affected Versions</th>
<th>Platform</th>
</tr>
</thead>
<tbody>
<tr>
<td>vCenter Server 7.0</td>
<td>vCenter Server 7.0 Update 2a and earlier</td>
<td>Any</td>
</tr>
<tr>
<td>vCenter Server 6.7</td>
<td>vCenter Server 6.7 Update 3m and earlier</td>
<td>Any</td>
</tr>
<tr>
<td>vCenter Server 6.5</td>
<td>vCenter Server 6.5 Update 3n and earlier</td>
<td>Any</td>
</tr>
</tbody>
</table>

Recommendations

VMware has released updates that fixes the two vulnerabilities CVE-2021-21985 and CVE-2021-21986 [2, 3, 4] and a workaround [5] showing how to disable VMware plugins in vCenter Server.

CERT-EU strongly recommends patching vCenter Server to the fixed version of the table below:

<table>
<thead>
<tr>
<th>Product</th>
<th>Fixed Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>vCenter Server 7.0</td>
<td>7.0 U2b</td>
</tr>
<tr>
<td>vCenter Server 6.7</td>
<td>6.7 U3n</td>
</tr>
<tr>
<td>vCenter Server 6.5</td>
<td>6.5 U3p</td>
</tr>
</tbody>
</table>

References