VMware vCenter Server updates address remote code execution vulnerability in the vSphere Client (CVE-2021-21972)

Various exposures in VMware ESXi as well as vSphere Client (HTML5) have been clandestinely notified to VMware. Revises are accessible to remediate these exposures in influenced VMware systems. The vSphere Client (HTML5) includes a remote code execution exposure in vCenter Server plugin. VMware has calculated the severity of the issue to be in the critical severity score of 9.8. The influenced vCenter Server plugin for vROPs is accessible in every defaulting installation. vROPs does not require to remain current to have this endpoint accessible.

The recognized attack routes, a malevolent actor with network admission to port 443 may take advantage of this matter to perform commands with unobstructed benefits on the underlying functioning network that hosts vCenter Server.

For a solution to remediate CVE-2021-21972 apply the updates recorded in the Fixed Versions column of the Response Matrix right to influenced placements. Also, for the workarounds for CVE-2021-21972 has been recorded in the Workarounds piece of the Response Matrix on the right. Adhere to the workarounds KB to disable it.

Response Matrix:

Product	Version	Running On	CVE Identifier	CVSSv3
vCenter Server	7.0	Any	CVE-2021-21972	9.8
vCenter Server	6.7	Any	CVE-2021-21972	9.8
vCenter Server	6.5	Any	CVE-2021-21972	9.8

Severity	Fixed Version	Workarounds	Additional Documentation
Critical	7.0 U1c	KB82374	None
Critical	6.7 U3l	KB82374	None
Critical	6.5 U3n	KB82374	None

Impacted Product Suites that Deploy Response Matrix 3a Components:

Product	Version	Running On	CVE Identifier	CVSSv3
Cloud Foundation (vCenter Server)	4.x	Any	CVE-2021-21972	9.8
Cloud Foundation (vCenter Server)	3.x	Any	CVE-2021-21972	9.8

Severity	Fixed Version	Workarounds	Additional Documentation
Critical	4.2	KB82374	None
Critical	3.10.1.2	KB82374	None

VMware vCenter Server updates address Server-Side Request Forgery (SSRF) Vulnerability in the vSphere Client [CVE-2021-21973]

OpenSLP such as utilized in ESXi has a heap-overflow exposure. VMware has calculated the severity of this issue to be in the Critical severity level with a score of 8.8. For the Security Configuration Guides for VMware vSphere, VMware currently advises deactivating the OpenSLP service in the ESXi if it is not utilized.

The recognized attack routes, a mischievous actor inhabiting inside the same system division as ESXi which has contact to port 427 may possibly be competent to prompt the heap-overflow concern in OpenSLP service stemming around remote code execution.

For a solution to remediate CVE-2021-21972 apply the updates recorded in the Fixed Versions column of the Response Matrix on the right to influenced placements. Also, for the workarounds for CVE-2021-21972 has been recorded in the Workarounds piece of the Response Matrix on the right. Workaround KB82705 documents measure to utilize ESXi hot patch asynchronously on top of latest VMware Cloud Foundation (VCF) endorsed by ESXi development.

Response Matrix:

Product	Version	Running On	CVE Identifier	CVSSv3
[1] ESXi	7.0	Any	CVE-2021-21974	8.8
[1] ESXi	6.7	Any	CVE-2021-21974	8.8
[1] ESXi	6.5	Any	CVE-2021-21974	8.8

Severity	Fixed Version	Workarounds	Additional Documentation
Important	ESXi70U1c-17325551	KB76372	None
Important	ESXi670-202102401-SG	KB76372	None
Important	ESXi650-202102101-SG	KB76372	None

Impacted Product Suites that Deploy Response Matrix 3b Components:

Product	Version	Running On	CVE Identifier	CVSSv3
[1] Cloud Foundation (ESXi)	4.x	Any	CVE-2021-21974	8.8
[1] Cloud Foundation (ESXi)	3.x	Any	CVE-2021-21974	8.8

Severity	Fixed Version	Workarounds	Additional Documentation
Important	4.2	KB76372	None
Important	[2] KB82705	KB76372	None

ESXi OpenSLP heap-overflow Vulnerability [CVE-2021-21974]

vSphere Client (HTML5) includes a SSRF exposure caused by inadequate certification of URLs dressed in a vCenter Server plugin. VMware has calculated the severity of this matter to be present in the medium severity level with a severity score of 5.3. The altered vCenter Server plugin used for vROPs is accessible in every defaulting installation. vROPs does not require to be present to carry out this endpoint accessible.

The recognized attack routes, a malevolent actor with system admissions to port 443 might manipulate this problem by delivering a post application to vCenter Server plugin primary to information discovery.

For a solution to remediate CVE-2021-21973 apply the updates recorded in the Fixed Versions column of the Response Matrix below to influenced placements. Also, for the workarounds for CVE-2021-21972 has been recorded in the Workarounds piece of the Response Matrix below. Adhere to the workarounds KB to disable it.

Response Matrix:

Product	Version	Running On	CVE Identifier	CVSSv3
vCenter Server	7.0	Any	CVE-2021-21973	5.3
vCenter Server	6.7	Any	CVE-2021-21973	5.3
vCenter Server	6.5	Any	CVE-2021-21973	5.3

Severity	Fixed Version	Workarounds	Additional Documentation
Moderate	7.0 U1c	KB82374	None
Moderate	6.7 U3l	KB82374	None
Moderate	6.5 U3n	KB82374	None

Impacted Product Suites that Deploy Response Matrix 3c Components:

Product	Version	Running On	CVE Identifier	CVSSv3
Cloud Foundation (vCenter Server)	4.x	Any	CVE-2021-21973	5.3
Cloud Foundation (vCenter Server)	3.x	Any	CVE-2021-21973	5.3

Severity	Fixed Version	Workarounds	Additional Documentation
Moderate	4.2	KB82374	None
Moderate	3.10.1.2	KB82374	None