VMSA-2021-0002:VMware ESXi and vCenter Server updates address multiple security vulnerabilities

Product/Component

VMware Cloud Foundation

2 more products

Notification Id	Last Updated	Initial Publication Date
23599	**21 February 2021**	**21 February 2021**
Status	**Severity**	**CVSS Base Score**
CLOSED	**CRITICAL**	**5.3-9.8**
WorkAround	Affected CVE	
	CVE-2021-21972,CVE-2021-21973,CVE-2021-21974	

Advisory ID: VMSA-2021-0002

CVSSv3 Range: 5.3-9.8

Issue Date:2021-02-23

Updated On: 2021-02-23 (Initial Advisory)

CVE(s): CVE-2021-21972, CVE-2021-21973, CVE-2021-21974

Synopsis: VMware ESXi and vCenter Server updates address multiple security vulnerabilities (CVE-2021-21972, CVE-2021-21973, CVE-2021-21974)

RSS Feed

Download PDF

Download Text File

Share this page on social media:

1. Impacted Products

- VMware ESXi
- VMware vCenter Server (vCenter Server)
- VMware Cloud Foundation (Cloud Foundation)

2. Introduction

Multiple vulnerabilities in VMware ESXi and vSphere Client (HTML5) were privately reported to VMware. Updates are available to remediate these vulnerabilities in affected VMware products.

3a. VMware vCenter Server updates address remote code execution vulnerability in the vSphere Client (CVE-2021-21972)

Description

The vSphere Client (HTML5) contains a remote code execution vulnerability in a vCenter Server plugin. VMware has evaluated the severity of this issue to be in the Critical severity range with a maximum CVSSv3 base score of 9.8.

Known Attack Vectors

Amalicious actor with network acc
hosts vCenter Server.

Resolution

To remediate CVE-2021-21972 ap

Workarounds

Workarounds for CVE-2021-2197

Additional Documentation

None.

Notes

The affected vCenter Server plugin for vROPs is available in all default installations. vROPs does not need be present to have this endpoint available. Follow the workarounds KB to disable it.

Acknowledgements

VMware would like to thank Mikhail Klyuchnikov of Positive Technologies for reporting this issue to us.

Response Matrix:

Product	Version	Running On	CVE Identifier	CVSSv3	Severity	Fixed Version	Workarounds	Additional Documentation
vCenter Server	7.0	Any	CVE-2021-21972	9.8	critical	7.0 U1c	KB82374	None
vCenter Server	6.7	Any	CVE-2021-21972	9.8	critical	6.7 U3l	KB82374	None
vCenter Server	6.5	Any	CVE-2021-21972	9.8	critical	6.5 U3n	KB82374	None

Impacted Product Suites that Deploy Response Matrix 3a Components:

Product	Version	Running On	CVE Identifier	CVSSv3	Severity	Fixed Version	Workarounds	Additional Documentation
Cloud Foundation (vCenter Server)	4.x	Any	CVE-2021-21972	9.8	critical	4.2	KB82374	None
Cloud Foundation (vCenter Server)	3.x	Any	CVE-2021-21972	9.8	critical	3.10.1.2	KB82374	None

3b. ESXi OpenSLP heap-overflow vulnerability (CVE-2021-21974)

Description

OpenSLP as used in ESXi has a heap-overflow vulnerability. VMware has evaluated the severity of this issue to be in the Important severity range with a maximum CVSSv3 base score of 8.8.

Known Attack Vectors

Amalicious actor residing within the same network segment as ESXi who has access to port 427 may be able to trigger the heap-overflow issue in OpenSLP service resulting in remote code execution.

Resolution

To remediate CVE-2021-21974 apply the updates listed in the 'Fixed Version' column of the 'Response Matrix' below to affected deployments.

Workarounds

Workarounds for CVE-2021-21974 have been listed in the 'Workarounds' column of the 'Response Matrix' below.

Additional Documentation

None.

Notes

[1] Per the Security Configuration Guides for VMware vSphere, VMware now recommends disabling the OpenSLP service in ESXi if it is not used. For more information, see our blog posting: https://blogs.vmware.com/vsphere/2021/02/evolving-the-vmware-vsphere-security-configuration-guides.html

[2] KB82705 documents steps to consume ESXi hot patch asynchronously on top of latest VMware Cloud Foundation (VCF) supported ESXi build.

Acknowledgements

VMware would like to thank Lucas Leong (@_wmliang_) of Trend Micro's Zero Day Initiative for reporting this issue to us.

Response Matrix:

Product	Version	Running On	CVE Identifier	CVSSv3	Severity	Fixed Version	Workarounds	Additional Documentation
[1] ESXi	7.0	Any	CVE-2021-21974	8.8	important	ESXi70U1c-17325551	KB76372	None
[1] ESXi	6.7	Any						
[1] ESXi	6.5	Any						

Impacted Product Suites that Deplo

Product	Ver
[1] Cloud Foundation (ESXi)	4.x

[1] Cloud Foundation (ESXi)	3.x	Any	CVE-2021-21974	8.8	important	[2] KB82705	KB76372	None

3c. VMware vCenter Server updates address SSRF vulnerability in the vSphere Client (CVE-2021-21973)

Description

The vSphere Client (HTML5) contains an SSRF (Server Side Request Forgery) vulnerability due to improper validation of URLs in a vCenter Server plugin. VMware has evaluated the severity of this issue to be in the Moderate severity range with a maximum CVSSv3 base score of 5.3.

Known Attack Vectors

A malicious actor with network access to port 443 may exploit this issue by sending a POST request to vCenter Server plugin leading to information disclosure.

Resolution

To remediate CVE-2021-21973 apply the updates listed in the 'Fixed Version' column of the 'Response Matrix' below to affected deployments.

Workarounds

Workarounds for CVE-2021-21973 have been listed in the 'Workarounds' column of the 'Response Matrix' below.

Additional Documentation

None.

Notes

The affected vCenter Server plugin for vROPs is available in all default installations. vROPs does not need be present to have this endpoint available. Follow the workarounds KB to disable it.

Acknowledgements

VMware would like to thank Mikhail Klyuchnikov of Positive Technologies for reporting this issue to us.

Response Matrix:

Product	Version	Running On	CVE Identifier	CVSSv3	Severity	Fixed Version	Workarounds	Additional Documentation
vCenter Server	7.0	Any	CVE-2021-21973	5.3	moderate	7.0 U1c	KB82374	None
vCenter Server	6.7	Any	CVE-2021-21973	5.3	moderate	6.7 U3l	KB82374	None
vCenter Server	6.5	Any	CVE-2021-21973	5.3	moderate	6.5 U3n	KB82374	None

Impacted Product Suites that Deploy Response Matrix 3c Components:

Product	Version	Running On	CVE Identifier	CVSSv3	Severity	Fixed Version	Workarounds	Additional Documentation
Cloud Foundation (vCenter Server)	4.x	Any	CVE-2021-21973	5.3	moderate	4.2	KB82374	None
Cloud Foundation (vCenter Server)	3.x	Any	CVE-2021-21973	5.3	moderate	3.10.1.2	KB82374	None

4. References

VMware ESXi 7.0 ESXi70U1c-17325551
https://my.vmware.com/group/vmware/patch
https://docs.vmware.com/en/VMware-vSphere/7.0/rn/vsphere-esxi-70u1c.html

VMware ESXi 6.7 ESXi670-202102401-SG
https://my.vmware.com/group/vmware/patch
https://docs.vmware.com/en/VMware-vSphere/6.7/rn/esxi670-202102001.html

VMware ESXi 6.5 ESXi650-202102101-SG
https://my.vmware.com/group/vmware/patch
https://docs.vmware.com/en/VMwa

VMware vCloud Foundation 4.2
Downloads and Documentation:
https://docs.vmware.com/en/VMwa

VMware vCloud Foundation 3.10.
Downloads and Documentation:
https://docs.vmware.com/en/VMwa

vCenter Server 7.0.1 Update 1
Downloads and Documentation:
https://my.vmware.com/web/vmware/downloads/details?downloadGroup=VC70U1C&productId=974
https://docs.vmware.com/en/VMware-vSphere/7.0/rn/vsphere-vcenter-server-70u1c-release-notes.html

vCenter Server 6.7 U3l
Downloads and Documentation:
https://my.vmware.com/web/vmware/downloads/details?downloadGroup=VC67U3L&productId=742&rPId=57171
https://docs.vmware.com/en/VMware-vSphere/6.7/rn/vsphere-vcenter-server-67u3l-release-notes.html

vCenter Server 6.5 U3n
Downloads and Documentation:
https://my.vmware.com/web/vmware/downloads/details?downloadGroup=VC65U3N&productId=614&rPId=60942
https://docs.vmware.com/en/VMware-vSphere/6.5/rn/vsphere-vcenter-server-65u3n-release-notes.html

Mitre CVE Dictionary Links:
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-21972
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-21973
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-21974

FIRST CVSSv3 Calculator:
CVE-2021-21972: https://www.first.org/cvss/calculator/3.1#CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
CVE-2021-21973: https://www.first.org/cvss/calculator/3.1#CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N
CVE-2021-21974: https://www.first.org/cvss/calculator/3.1#CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

5. Change Log

2021-02-23 VMSA-2021-0002
Initial security advisory.

6. Contact

E-mail list for product security notifications and announcements:

https://lists.vmware.com/cgi-bin/mailman/listinfo/security-announce

This Security Advisory is posted to the following lists:

security-announce@lists.vmware.com

bugtraq@securityfocus.com

fulldisclosure@seclists.org

E-mail: security@vmware.com

PGP key at:

https://kb.vmware.com/kb/1055

VMware Security Advisories

https://www.vmware.com/security/advisories

VMware Security Response Policy

https://www.vmware.com/support/p

VMware Lifecycle Support Phases

https://www.vmware.com/support/p

VMware Security & Compliance Bl

https://blogs.vmware.com/security

Twitter

https://twitter.com/VMwareSRC