



# CVE-2021-21973

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF](#)

## Summary

<b>CVE</b>	CVE-2021-21973
<b>State</b>	PUBLIC
<b>Assigner</b>	security@vmware.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2021-02-24 17:15:00 UTC
<b>Updated</b>	2021-08-24 10:59:00 UTC
<b>Description</b>	The vSphere Client (HTML5) contains an SSRF (Server Side Request Forgery) vulnerability due to improper validation of U

## Risk And Classification

**EPSS:** 0.903360000 probability, percentile 0.995990000 (date 2026-04-02)

**CISA KEV:** Listed on 2022-03-07; due 2022-03-21; ransomware use Unknown

**Problem Types:** CWE-918

## CISA Known Exploited Vulnerability

<b>Vendor</b>	VMware
<b>Product</b>	vCenter Server and Cloud Foundation
<b>Name</b>	VMware vCenter Server and Cloud Foundation Server Side Request Forgery (SSRF) Vulnerability
<b>Required Action</b>	Apply updates per vendor instructions.
<b>Notes</b>	<a href="https://nvd.nist.gov/vuln/detail/CVE-2021-21973">https://nvd.nist.gov/vuln/detail/CVE-2021-21973</a>

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Vmware	Cloud Foundation	All	All	All	All
Application	Vmware	Cloud Foundation	All	All	All	All
Application	Vmware	Vcenter Server	6.5	-	All	All
Application	Vmware	Vcenter Server	6.5	a	All	All
Application	Vmware	Vcenter Server	6.5	b	All	All
Application	Vmware	Vcenter Server	6.5	c	All	All
Application	Vmware	Vcenter Server	6.5	d	All	All
Application	Vmware	Vcenter Server	6.5	e	All	All

Application	Vmware	Vcenter Server	6.5	f	All	All
Application	Vmware	Vcenter Server	6.5	u1d	All	All
Application	Vmware	Vcenter Server	6.5	u1e	All	All
Application	Vmware	Vcenter Server	6.5	u1g	All	All
Application	Vmware	Vcenter Server	6.5	u2	All	All
Application	Vmware	Vcenter Server	6.5	u2b	All	All
Application	Vmware	Vcenter Server	6.5	u2c	All	All
Application	Vmware	Vcenter Server	6.5	u2d	All	All
Application	Vmware	Vcenter Server	6.5	u2g	All	All
Application	Vmware	Vcenter Server	6.5	u3	All	All
Application	Vmware	Vcenter Server	6.5	u3d	All	All
Application	Vmware	Vcenter Server	6.5	u3f	All	All
Application	Vmware	Vcenter Server	6.5	u3k	All	All
Application	Vmware	Vcenter Server	6.5	update1d	All	All
Application	Vmware	Vcenter Server	6.5	update1e	All	All
Application	Vmware	Vcenter Server	6.5	update1g	All	All
Application	Vmware	Vcenter Server	6.5	update2	All	All
Application	Vmware	Vcenter Server	6.5	update2b	All	All
Application	Vmware	Vcenter Server	6.5	update2c	All	All
Application	Vmware	Vcenter Server	6.5	update2d	All	All
Application	Vmware	Vcenter Server	6.5	update2g	All	All
Application	Vmware	Vcenter Server	6.5	update3	All	All
Application	Vmware	Vcenter Server	6.5	update3d	All	All
Application	Vmware	Vcenter Server	6.5	update3f	All	All
Application	Vmware	Vcenter Server	6.5	update3k	All	All
Application	Vmware	Vcenter Server	6.7	-	All	All
Application	Vmware	Vcenter Server	6.7	a	All	All
Application	Vmware	Vcenter Server	6.7	b	All	All
Application	Vmware	Vcenter Server	6.7	d	All	All
Application	Vmware	Vcenter Server	6.7	u1	All	All
Application	Vmware	Vcenter Server	6.7	u1b	All	All
Application	Vmware	Vcenter Server	6.7	u2	All	All
Application	Vmware	Vcenter Server	6.7	u2a	All	All
Application	Vmware	Vcenter Server	6.7	u2c	All	All
Application	Vmware	Vcenter Server	6.7	u3	All	All

Application	Vmware	Vcenter Server	6.7	u3a	All	All
Application	Vmware	Vcenter Server	6.7	u3b	All	All
Application	Vmware	Vcenter Server	6.7	u3f	All	All
Application	Vmware	Vcenter Server	6.7	u3g	All	All
Application	Vmware	Vcenter Server	6.7	u3j	All	All
Application	Vmware	Vcenter Server	6.7	update1	All	All
Application	Vmware	Vcenter Server	6.7	update1b	All	All
Application	Vmware	Vcenter Server	6.7	update2	All	All
Application	Vmware	Vcenter Server	6.7	update2a	All	All
Application	Vmware	Vcenter Server	6.7	update2c	All	All
Application	Vmware	Vcenter Server	6.7	update3	All	All
Application	Vmware	Vcenter Server	6.7	update3a	All	All
Application	Vmware	Vcenter Server	6.7	update3b	All	All
Application	Vmware	Vcenter Server	6.7	update3f	All	All
Application	Vmware	Vcenter Server	6.7	update3g	All	All
Application	Vmware	Vcenter Server	6.7	update3j	All	All
Application	Vmware	Vcenter Server	7.0	-	All	All
Application	Vmware	Vcenter Server	7.0	a	All	All
Application	Vmware	Vcenter Server	7.0	b	All	All
Application	Vmware	Vcenter Server	7.0	c	All	All
Application	Vmware	Vcenter Server	7.0	d	All	All
Application	Vmware	Vcenter Server	7.0	u1	All	All
Application	Vmware	Vcenter Server	7.0	u1a	All	All
Application	Vmware	Vcenter Server	7.0	update1	All	All
Application	Vmware	Vcenter Server	7.0	update1a	All	All
Application	Vmware	Vcenter Server	6.5	-	All	All
Application	Vmware	Vcenter Server	6.5	a	All	All
Application	Vmware	Vcenter Server	6.5	b	All	All
Application	Vmware	Vcenter Server	6.5	c	All	All
Application	Vmware	Vcenter Server	6.5	d	All	All
Application	Vmware	Vcenter Server	6.5	e	All	All
Application	Vmware	Vcenter Server	6.5	f	All	All
Application	Vmware	Vcenter Server	6.5	u1d	All	All
Application	Vmware	Vcenter Server	6.5	u1e	All	All
Application	Vmware	Vcenter Server	6.5	u1g	All	All

Application	Vmware	Vcenter Server	6.5	u2	All	All
Application	Vmware	Vcenter Server	6.5	u2b	All	All
Application	Vmware	Vcenter Server	6.5	u2c	All	All
Application	Vmware	Vcenter Server	6.5	u2d	All	All
Application	Vmware	Vcenter Server	6.5	u2g	All	All
Application	Vmware	Vcenter Server	6.5	u3	All	All
Application	Vmware	Vcenter Server	6.5	u3d	All	All
Application	Vmware	Vcenter Server	6.5	u3f	All	All
Application	Vmware	Vcenter Server	6.5	u3k	All	All
Application	Vmware	Vcenter Server	6.7	-	All	All
Application	Vmware	Vcenter Server	6.7	a	All	All
Application	Vmware	Vcenter Server	6.7	b	All	All
Application	Vmware	Vcenter Server	6.7	d	All	All
Application	Vmware	Vcenter Server	6.7	u1	All	All
Application	Vmware	Vcenter Server	6.7	u1b	All	All
Application	Vmware	Vcenter Server	6.7	u2	All	All
Application	Vmware	Vcenter Server	6.7	u2a	All	All
Application	Vmware	Vcenter Server	6.7	u2c	All	All
Application	Vmware	Vcenter Server	6.7	u3	All	All
Application	Vmware	Vcenter Server	6.7	u3a	All	All
Application	Vmware	Vcenter Server	6.7	u3b	All	All
Application	Vmware	Vcenter Server	6.7	u3f	All	All
Application	Vmware	Vcenter Server	6.7	u3g	All	All
Application	Vmware	Vcenter Server	6.7	u3j	All	All
Application	Vmware	Vcenter Server	7.0	-	All	All
Application	Vmware	Vcenter Server	7.0	a	All	All
Application	Vmware	Vcenter Server	7.0	b	All	All
Application	Vmware	Vcenter Server	7.0	c	All	All
Application	Vmware	Vcenter Server	7.0	d	All	All
Application	Vmware	Vcenter Server	7.0	u1	All	All
Application	Vmware	Vcenter Server	7.0	u1a	All	All

## References

Reference	Source	Link	Tags
VMSA-2021-0002	CONFIRM	<a href="http://www.vmware.com">www.vmware.com</a>	Vendor Advisory
CVE Program record	CVE.ORG	<a href="http://www.cve.org">www.cve.org</a>	canonical

NVD vulnerability detail	NVD	<a href="https://nvd.nist.gov">nvd.nist.gov</a>	canonical, analysis
CISA Known Exploited Vulnerabilities catalog	CISA	<a href="https://www.cisa.gov">www.cisa.gov</a>	kev

No vendor comments have been submitted for this CVE.

#### Legacy QID Mappings

[216253](#) VMware vCenter Server 7.0 Update 7.0 U1c Missing (VMSA-2021-0002)

[216254](#) VMware vCenter Server 6.7 Update 6.7 U3l Missing (VMSA-2021-0002)

[216255](#) VMware vCenter Server 6.5 Update 6.5 U3n Missing (VMSA-2021-0002)

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

**CVE.report and Source URL Uptime Status [status.cve.report](#)**