



CVE-2021-22048

Published on: 11/10/2021 12:00:00 AM UTC

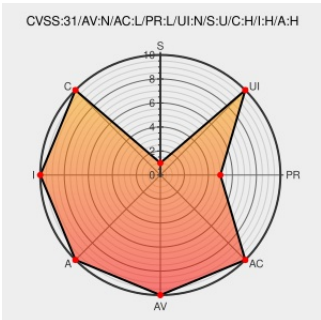
Last Modified on: 11/16/2021 02:35:00 PM UTC

CVE-2021-22048

[Source: Mitre](#)

[Source: Nist](#)

[Print: PDF](#)



Certain versions of [Cloud Foundation](#) from [Vmware](#) contain the following vulnerability:

The vCenter Server contains a privilege escalation vulnerability in the IWA (Integrated Windows Authentication) authentication mechanism. A malicious actor with non-administrative access to vCenter Server may exploit this issue to elevate privileges to a higher privileged group.

CVE-2021-22048 has been assigned by security@vmware.com to track the vulnerability - currently rated as **HIGH** severity.

CVSS3 Score: **8.8 - HIGH**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	LOW	NONE
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
UNCHANGED	HIGH	HIGH	HIGH

CVSS2 Score: **6.5 - MEDIUM**

Access Vector	Access Complexity	Authentication
NETWORK	LOW	SINGLE
Confidentiality Impact	Integrity Impact	Availability Impact
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
VMSA-2021-0025	www.vmware.com text/html	<input type="checkbox"/> MISC www.vmware.com/security/advisories/VMSA-2021-0025.html

By selecting these links, you may be leaving CVEreport webpage. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that

are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

Related QID Numbers

[216272](#) VMware vCenter Server 7.0 Privilege Escalation Vulnerability (VMSA-2021-0025)

[216273](#) VMware vCenter Server 6.7 Privilege Escalation Vulnerability (VMSA-2021-0025)

[216274](#) VMware vCenter Server 6.5 Privilege Escalation Vulnerability (VMSA-2021-0025)

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Vmware	Cloud Foundation	All	All	All	All
Operating System	Vmware	Cloud Foundation	All	All	All	All
Application	Vmware	Vcenter Server	6.5	-	All	All
Application	Vmware	Vcenter Server	6.7	-	All	All
Application	Vmware	Vcenter Server	7.0	-	All	All

`cpe:2.3:a:vmware:cloud_foundation:*:*:*:*:*:`

`cpe:2.3:o:vmware:cloud_foundation:*:*:*:*:*:`

`cpe:2.3:a:vmware:vcenter_server:6.5:-:*:*:*:*:`

`cpe:2.3:a:vmware:vcenter_server:6.7:-:*:*:*:*:`

`cpe:2.3:a:vmware:vcenter_server:7.0:-:*:*:*:*:`

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
<input type="checkbox"/> @DCIS_SUND	Varsel! ?KRITIKALITET: Øget risiko (Gul)? CVE-2021-22048 VMvare har informeret om en sårbarhed i deres vCenter Se... twitter.com/i/web/status/1...	2021-11-10 16:14:55
<input type="checkbox"/> @CVEreport	CVE-2021-22048 : The vCenter Server contains a privilege escalation vulnerability in the IWA Integrated #Windows A... twitter.com/i/web/status/1...	2021-11-10 18:02:39
<input type="checkbox"/> @makopicut	VMware vCenter Server IWA privilege escalation vulnerability (CVE-2021-22048) VMSA-2021-0025 vmware.com/security/advis...	2021-11-10 18:05:47

[← Previous ID](#)

[Next ID →](#)

© [CVE.report](#) 2022 |

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](#)