



CVE-2021-42306

Published on: Not Yet Published

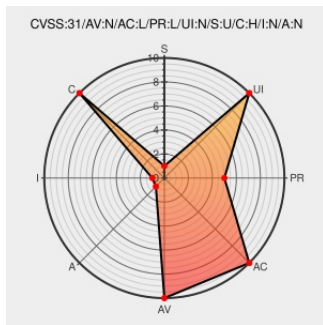
Last Modified on: 11/29/2021 07:13:00 PM UTC

CVE-2021-42306

Source: Mitre

Source: Nist

Print: PDF



Certain versions of [Azure Active Directory](#) from [Microsoft](#) contain the following vulnerability:

Azure Active Directory Information Disclosure Vulnerability

CVE-2021-42306 has been assigned by secure@microsoft.com to track the vulnerability - currently rated as **MEDIUM** severity.

Affected Vendor/Software: **Microsoft - Azure Automation** version

Affected Vendor/Software: **Microsoft - Azure Active Directory** version

Affected Vendor/Software: **Microsoft - Azure Site Recovery** version

Affected Vendor/Software: **Microsoft - Azure Migrate** version


CVSS3 Score: **6.5 - MEDIUM**

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

CVSS2 Score: **4 - MEDIUM**

Access Vector	Access Complexity	Authentication
NETWORK	LOW	SINGLE
Confidentiality Impact	Integrity Impact	Availability Impact
PARTIAL	NONE	NONE

CVE References

Description	Tags	Link
Security Update Guide - Microsoft Security Response Center	portal.msrc.microsoft.com text/html	 MISC portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-42306

By selecting these links, you may be leaving CVEreport webspace. 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.








There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)













Type	Vendor	Product	Version	Update	Edition	Language
Application	Microsoft	Azure Active Directory	All	All	All	All
Application	Microsoft	Azure Active Site Recovery	All	All	All	All
Application	Microsoft	Azure Automation	All	All	All	All
Application	Microsoft	Azure Migrate	All	All	All	All
<code>cpe:2.3:a:microsoft:azure_active_directory:*:*:*:*:*:*:</code>						
<code>cpe:2.3:a:microsoft:azure_active_site_recovery:*:*:*:*:*:*:</code>						
<code>cpe:2.3:a:microsoft:azure_automation:*:*:*:*:*:*:</code>						
<code>cpe:2.3:a:microsoft:azure_migrate:*:*:*:*:*:*:</code>						

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
 @kfosaaen	MSRC was great to work with on this one. Here are the associated MSRC links: msrc.microsoft.com/update-guide/v... msrc-blog.microsoft.com/2021/11/17/gui... (4/5)	2021-11-17 20:30:10
 @boxswapper	@NetSPI Uncovers a Critical Azure #Vulnerability , CVE-2021-42306: CredManifest & how to fix it netspi.com/news/press-rel...	2021-11-17 22:02:30
 @valdet_b	CVE-2021-42306 - Microsoft - Azure Active Directory Information Disclosure Vulnerability msrc.microsoft.com/update-guide/v...	2021-11-17 23:13:15
 @41thexplorer	Now found the thread by the researcher who found the CVE-2021-42306 vulnerability with links to @NetSPI informative... twitter.com/i/web/status/1...	2021-11-17 23:32:16
 @ianhellen	MSTICPy and I had a small part to play in CVE-2021-42306 (mitigating, not causing). Published a notebook to detect... twitter.com/i/web/status/1...	2021-11-18 00:00:36
 @EurekaBerry	AzureADの脆弱性 CVE-2021-42306 (修正済み) の公表と影響確認ガイダンスをいたしました。該当環境は通知でていますのでご確認を アプリケーションおよびサービス プリンシパル API での Azure Active... twitter.com/i/web/status/1...	2021-11-18 00:24:42
 @ntsuii	CVE-2021-42306 - Security Update Guide - Microsoft - Azure Active Directory Information	2021-11-18

	Disclosure Vulnerability msrc.microsoft.com/update-guide/v...	01:08:43
@kawn2020	#securityupdate #azure 2021.11.17 Azure Active Directory の情報漏えいの脆弱性 CVE-2021-42306 - マイクロソフト msrc.microsoft.com/update-guide/v...	2021-11-18 01:36:55
@faisal_asif	CVE-2021-42306 CredManifest: App Registration Certificates Stored in Azure Active Directory netspi.com/blog/technical...	2021-11-18 02:30:34
@merill	Let your Azure admins that manage the other affected services know. Scripts for the other services are available at aka.ms/CVE-2021-42306...	2021-11-18 03:32:03
@SantasaloJoosua	Top quality work by @NetSPI and @msftsecresponse - CVE-2021-42306 - For example "Automation Run As accounts created... twitter.com/i/web/status/1...	2021-11-18 05:18:03
@Sho2010	CVE-2021-42306 影響受けるかどうか判断するの難しすぎる 何が書いてあるのかようわからん	2021-11-18 05:33:50
@cyberkendra	CVE-2021-42306 CredManifest: App Registration Certificates Store bug.cyberkendra.com/2021/11/18/cve... #azure #security	2021-11-18 08:01:33
@kabukawa	"Microsoftは先日、情報漏えいの問題(CVE-2021-42306)を緩和、一部のAzureサービスがAzure Active Directory(Azure AD)Application及び/又はService Prin... twitter.com/i/web/status/1...	2021-11-18 09:45:08
@kabukawa	"Azure Active Directory の情報漏えいの脆弱性 CVE-2021-42306" msrc.microsoft.com/update-guide/v...	2021-11-18 09:45:09
@IT_news_for_all	CVE-2021-42306 CredManifest: App Registration Certificates Stored in Azure Active Directory... twitter.com/i/web/status/1...	2021-11-18 12:32:01
@Har_sia	CVE-2021-42306 har-sia.info/CVE-2021-42306... #HarsiaInfo	2021-11-18 15:01:13
@ArtyomSinitsyn	Microsoft recently mitigated an information disclosure issue CVE-2021-42306 to prevent private key data from being... twitter.com/i/web/status/1...	2021-11-18 15:15:04
@step9consulting	CVE-2021-42306 #CredManifest Vulnerability in App Registration Certificates Stored in #Azure Active Directory:... twitter.com/i/web/status/1...	2021-11-18 15:30:44
@ipssignatures	The vuln CVE-2021-42306 has a tweet created 0 days ago and retweeted 13 times. twitter.com/ianhellen/stat... #pow1rtrtwwcve	2021-11-18 16:06:00
@NormanOre	Azure Active Directory Information Disclosure Vulnerability CVE-2021-42306 Azure Migrate Azure Site Recovery Azure... twitter.com/i/web/status/1...	2021-11-18 18:50:07
@malwaresick	NetSPI Uncovers a Critical Azure Vulnerability, CVE-2021-42306: CredManifest #CyberSecurity netspi.com/news/press-rel...	2021-11-19 01:02:34
@etguenni	Schwachstelle CVE-2021-42306 in Microsoft Azure AD borncity.com/blog/2021/11/1... #Azure #Sicherheit Borns IT- & Windows-Blog	2021-11-19 03:03:58
@ohhara_shiojiri	"Microsoft recently addressed an information disclosure vulnerability, tracked as CVE-2021-42306, affecting Azure AD."	2021-11-19 05:40:18
@Ourghanlian	Microsoft recently mitigated an information disclosure issue, CVE-2021-42306, to prevent private key data from bein... twitter.com/i/web/status/1...	2021-11-19 06:08:11
@etguenni	Microsoft revealed Vulnerability CVE-2021-42306 in Microsoft Azure AD borncity.com/win/?p=22194 #Azure #Security Born's Tech and Windows World	2021-11-19 07:27:12
@niiconsulting	#Dailydose: Microsoft recently addressed an information disclosure #vulnerability, tracked as CVE-2021-42306, affec... twitter.com/i/web/status/1...	2021-11-19 10:07:15
@ITechnologySer1	NetSPI Uncovers a Critical Azure Vulnerability, CVE-2021-42306 CredManifest ow.ly/ktsa30s16HR #technology #IT... twitter.com/i/web/status/1...	2021-11-19 10:38:48
@Har_sia	CVE-2021-42306 har-sia.info/CVE-2021-42306... #HarsiaInfo	2021-11-19 15:02:06
@NetSPI	Do you utilize @Azure services? Then you should be aware of CVE-2021-42306: CredManifest	2021-11-19

 @NetSPI	Do you utilize @Azure services? Then you should be aware of CVE-2021-42306: CredManifest, identified by NetSPI's ve... twitter.com/i/web/status/1...	2021-11-19 17:07:34
 @MDowst	I was running the script to check for CVE-2021-42306 and received a 403 error from one client, even as a GA. In cas... twitter.com/i/web/status/1...	2021-11-19 17:39:43
 @Wicsplnt	Microsoft recently addressed an information disclosure vulnerability, tracked as CVE-2021-42306, affecting Azure AD... twitter.com/i/web/status/1...	2021-11-19 19:29:57
 @NetSPI	NetSPI in the News: @StackPublishing reported on @kfosaaen's discovery of CVE-2021-42306, a serious #Azure Active D... twitter.com/i/web/status/1...	2021-11-19 22:05:03
 @NetSPI	NetSPI's @Azure cloud pentesting lead @kfosaaen explains how we found and reported CVE-2021-42306 (CredManifest) to... twitter.com/i/web/status/1...	2021-11-20 15:05:05
 @AlirezaGhahrood	Offensive_security 1. CVE-2021-42306 CredManifest: App Registration Certificates Stored in Azure AD 2. Windows Sec... twitter.com/i/web/status/1...	2021-11-21 02:16:27
 @jaocabete	#azure #cve-2021-42306 lnkd.in/egJr87Fq	2021-11-21 13:20:45
 @IT_news_for_all	? CVE-2021-42306 CredManifest: App Registration Certificates Stored in Azure Active Directory Another security iss... twitter.com/i/web/status/1...	2021-11-22 06:27:34
 @328__	Azure Active Directory の情報漏えいの脆弱性 msrc.microsoft.com/update-guide/v...	2021-11-23 10:15:06
 @CVEreport	CVE-2021-42306 : Azure Active Directory Information Disclosure Vulnerability... cve.report/CVE-2021-42306	2021-11-24 01:16:03
 /r/sysadmin	PSA: Calling all Azure AD Admins. Find out if your Azure AD tenant has apps that are affected by https://aka.ms/CVE-2021-42306	2021-11-18 16:59:14
 /r/blueteamsec	CVE-2021-42306 CredManifest: App Registration Certificates Stored in Azure Active Directory	2021-11-20 19:09:53

[← Previous ID](#)

[Next ID →](#)

© CVE.report 2021   |

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