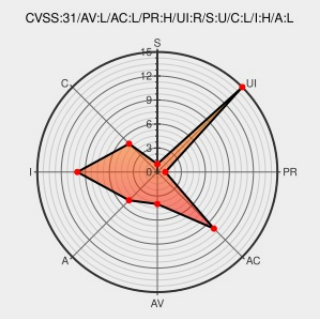
CVE-2022-23551

Published on: Not Yet Published

Last Modified on: 01/04/2023 07:54:00 PM UTC

CVE-2022-23551 - advisory for GHSA-p82q-rxpm-hjpc

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Azure Ad Pod Identity from Microsoft contain the following vulnerability:

aad-pod-identity assigns Azure Active Directory identities to Kubernetes applications and has now been deprecated as of 24 October 2022. The NMI component in AAD Pod Identity intercepts and validates token requests based on regex. In this case, a token request made with backslash in the request (example: `/metadata/identity\oauth2\token/`) would bypass the NMI validation and be sent to IMDS allowing a pod in the cluster to access identities that it shouldn't have access to. This issue has been fixed and has been included in AAD Pod Identity release version 1.8.13. If using the AKS pod-managed identities add-on, no action is required. The clusters should now be running the version 1.8.13 release.

CVE-2022-23551 has been assigned by security-advisories@github.com to track the vulnerability - currently rated as MEDIUM severity.

Affected Vendor/Software: **Azure** - **aad-pod-identity** version **= < 1.8.13**

CVSS3 Score: 5.3 - MEDIUM

Attack Vector	Attack Complexity	Privileges Required	User Interaction
LOCAL	LOW	HIGH	REQUIRED
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
UNCHANGED	LOW	HIGH	LOW

CVE References

Description	Tags	Link
Release v1.8.13 · Azure/aad-pod-identity · GitHub	github.com text/html	MISC github.com/Azure/aad-pod-identity/releases/tag/v1.8.13
fix: add handler for invalid token requests (#1325) ·	github.com	MISC github.com/Azure/aad-pod-

Azure/aad-pod-identity@7e01970 · GitHub	text/html	identity/commit/7e01970391bde6c360d077066ca17d059204cb5d
AAD Pod Identity obtaining token with backslash · Advisory · Azure/aad-pod-identity · GitHub	github.com text/html	MISC github.com/Azure/aad-pod-identity/security/advisories/GHSA-p82q-rxpm-hjpc

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 Ad Pod Identity	All	All	All	All

cpe:2.3:a:microsoft:azure_ad_pod_identity:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2022-23551 : aad-pod-identity assigns Azure Active Directory identities to Kubernetes applications and has now… twitter.com/i/web/status/1…	2022-12-21 20:07:31
/r/netcve	CVE-2022-23551	2022-12-21 21:38:46

← Previous ID

Next ID→