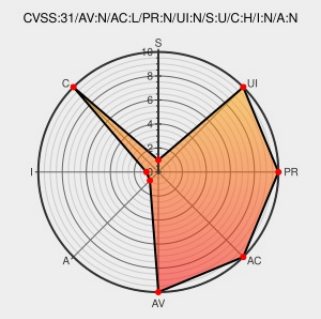
CVE-2022-38203

Published on: Not Yet Published

Last Modified on: 01/09/2023 07:11:00 PM UTC

CVE-2022-38203

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



Certain versions of Portal For Arcgis from Esri contain the following vulnerability:

Protections against potential Server-Side Request Forgery (SSRF) vulnerabilities in Esri Portal for ArcGIS versions 10.8.1 and below were not fully honored and may allow a remote, unauthenticated attacker to forge requests to arbitrary URLs from the system, potentially leading to network enumeration or reading from hosts inside the network perimeter, a different issue than CVE-2022-38211 and CVE-2022-38212.

CVE-2022-38203 has been assigned by esri psirt@esri.com to track the vulnerability - currently rated as HIGH severity.

Affected Vendor/Software: esri **Esri** - **Portal for ArcGIS** version **= 10.7.1 and 10.8.1**

CVSS3 Score: 7.5 - HIGH

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

CVE References

Description	Tags	Link
Portal for ArcGIS Security 2022 Update 2 Patch is Now Available	www.esri.com text/html	esri MISC www.esri.com/arcgis-blog/products/trust-arcgis/administration/portal-for-arcgis-security-2022-update-2-patch-is-now-available

There are currently no OIDs associated with this CVE

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Esri	Portal For Arcgis	All	All	All	All

cpe:2.3:a:esri:portal_for_arcgis:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2022-38203 : Protections against potential Server-Side Request Forgery #SSRF vulnerabilities in Esri Portal f… twitter.com/i/web/status/1…	2022-12-29 19:18:09
/r/netcve	CVE-2022-38203	2022-12-29 19:38:45

← Previous ID

Next ID→