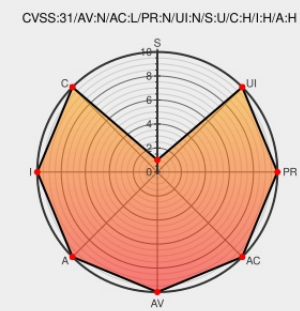
CVE-2021-40371

Published on: 10/25/2021 12:00:00 AM UTC

Last Modified on: 10/28/2021 10:18:00 PM UTC

CVE-2021-40371

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



Certain versions of Request Management from Gridprosoftware contain the following vulnerability:

Gridpro Request Management for Windows Azure Pack before 2.0.7912 allows Directory Traversal for remote code execution, as demonstrated by ..\\ in a scriptName JSON value to ServiceManagerTenant/GetVisibilityMap.

CVE-2021-40371 has been assigned by cve@mitre.org to track the vulnerability - currently rated as CRITICAL severity.

CVSS3 Score: 9.8 - CRITICAL

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

CVSS2 Score: 7.5 - HIGH

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

CVE References

Description	Tags	Link
Full Disclosure: [CSA-2021-003] Remote Code Execution in GridPro Request Management for Windows Azure Pack	seclists.org text/html	MISC seclists.org/fulldisclosure/2021/Oct/33
GridPro Request Management For Windows Azure	packetstormsecurity.com	MISC packetstormsecurity.com/files/164621/GridPro-

Pack 2.0.7905 Directory Traversal ≈ Packet Storm	text/html	Request-Management-For-Windows-Azure-Pack-2.0.7905-Directory-Traversal.html
Request Management - Gridpro	www.gridprosoftware.com text/html	MISC www.gridprosoftware.com/products/requestmanagement/

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	Gridprosoftware	Request Management	All	All	All	All

cpe:2.3:a:gridprosoftware:request_management:*:*:*:*:*:azure:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2021-40371 : Gridpro Request Management for #Windows Azure Pack before 2.0.7912 allows Directory Traversal for… twitter.com/i/web/status/1…	2021-10-25 07:06:07
@Robo_Alerts	Potentially Critical CVE Detected! CVE-2021-40371 Description: Gridpro Request Management for Windows Azure Pack be… twitter.com/i/web/status/1…	2021-10-25 08:00:11
@SecRiskRptSME	RT: CVE-2021-40371 Gridpro Request Management for Windows Azure Pack before 2.0.7912 allows Directory Traversal fo… twitter.com/i/web/status/1…	2021-10-25 08:33:25

← Previous ID

Next ID→