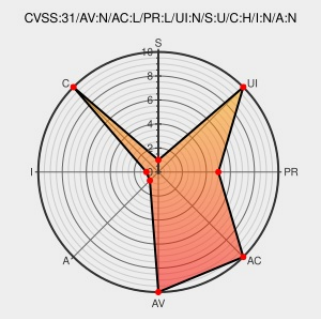
CVE-2022-27248

Published on: Not Yet Published

Last Modified on: 04/09/2022 03:10:00 PM UTC

CVE-2022-27248

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



Certain versions of Reftree from Idearespa contain the following vulnerability:

A directory traversal vulnerability in IdeaRE RefTree before 2021.09.17 allows remote authenticated users to download arbitrary .dwg files from a remote server by specifying an absolute or relative path when invoking the affected DownloadDwg endpoint. An attack uses the path field to CaddemServiceJS/CaddemService.svc/rest/DownloadDwg.

CVE-2022-27248 has been assigned by cve@mitre.org to track the vulnerability - currently rated as MEDIUM severity.

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
IDEARE – IT works for REal	www.idearespa.eu text/html	MISC www.idearespa.eu
IdeaRE RefTree Path Traversal ~ Packet	packetstormsecurity.com	MISC packetstormsecurity.com/files/166560/IdeaRE-RefTree-

IdeaRE RefTree Path Traversal ~ Packet Storm	packetstormsecurity.com text/html	MISC packetstormsecurity.com/files/166560/IdeaRE-RefTree-Path-Traversal.html

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Idearespa	Reftree	All	All	All	All

cpe:2.3:a:idearespa:reftree:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@SecurityNewsbot	IdeaRE RefTree Path Traversal packetstormsecurity.com/files/166560/C… #PacketStorm	2022-03-31 17:30:13
@CVEreport	CVE-2022-27248 : A directory traversal vulnerability in IdeaRE RefTree before 2021.09.17 allows remote authenticate… twitter.com/i/web/status/1…	2022-04-03 23:05:18
/r/netcve	CVE-2022-27248	2022-04-04 00:39:05

← Previous ID

Next ID→