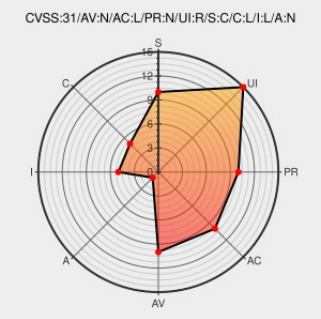
CVE-2022-34093

Published on: Not Yet Published

Last Modified on: 10/18/2023 03:52:00 PM UTC

CVE-2022-34093

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



Certain versions of I3geo from I3geo Project contain the following vulnerability:

Portal do Software Publico Brasileiro i3geo v7.0.5 was discovered to contain a cross-site scripting (XSS) vulnerability via access_token.php.

CVE-2022-34093 has been assigned by cve@mitre.org to track the vulnerability - currently rated as MEDIUM severity.

CVSS3 Score: 6.1 - MEDIUM

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

CVSS2 Score: 4.3 - MEDIUM

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

CVE References

Description	Tags	Link
Vulnerabilidade - XSS (Cross Site Scripting) or HTML Injection - access_token.php · Issue #4 · edmarmoretti/i3geo · GitHub	github.com text/html	MISC github.com/edmarmoretti/i3geo/issues/4
Cross Site Scripting (XSS) | OWASP	owasp.org	MISC owasp.org/www-community/attacks/xss/

Foundation	text/html	
Vulnerabilidade - XSS (Cross Site Scripting) or HTML Injection - access_token.php · Issue #4 · saladesituacao/i3geo · GitHub	github.com text/html	MISC github.com/saladesituacao/i3geo/issues/4
Sobre o Software - i3Geo	softwarepublico.gov.br text/html	MISC softwarepublico.gov.br/social/i3geo
ProofOfConcept/i3geo_proof_of_concept.txt at main · wagnerdracha/ProofOfConcept · GitHub	github.com text/html	MISC github.com/wagnerdracha/ProofOfConcept/blob/main/i3geo_proof_of_c

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	I3geo Project	I3geo	7.0.5	All	All	All
Application	Softwarepublico	I3geo	7.0.5	All	All	All

cpe:2.3:a:i3geo_project:i3geo:7.0.5:*:*:*:*:*:*:*:

cpe:2.3:a:softwarepublico:i3geo:7.0.5:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2022-34093 : Portal do Software Publico Brasileiro i3geo v7.0.5 was discovered to contain a cross-site scriptin… twitter.com/i/web/status/1…	2022-07-14 22:10:12
@LinInfoSec	Php - CVE-2022-34093: github.com/saladesituacao…	2022-07-15 01:00:25
@threatmeter	CVE-2022-34093 Portal do Software Publico Brasileiro i3geo v7.0.5 was discovered to contain a cross-site scripting… twitter.com/i/web/status/1…	2022-07-15 07:09:42
@ColorTokensInc	Emerging Vulnerability Found CVE-2022-34093 - Portal do Software Publico Brasileiro i3geo v7.0.5 was discovered to… twitter.com/i/web/status/1…	2022-07-15 07:09:48
/r/netcve	CVE-2022-34093	2022-07-14 22:38:46

← Previous ID

Next ID→

CVE.report and Source URL Uptime Status status.cve.report