

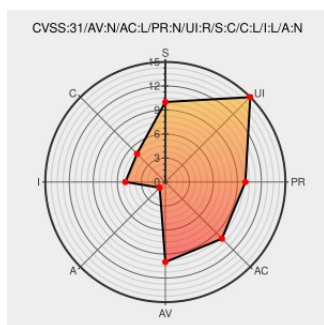


CVE-2022-34092

Published on: Not Yet Published

Last Modified on: 10/18/2023 03:51:00 PM UTC

CVE-2022-34092

[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 [svg2img.php](#).

CVE-2022-34092 has been assigned by [M](#) [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
Cross Site Scripting (XSS) OWASP Foundation	owasp.org text/html	MISC owasp.org/www-community/attacks/xss/
Vulnerabilidade - XSS (Cross Site Scripting) or HTML Injection - svg2img.php - Issue #3	github.com text/html	MISC github.com/saladesituacao/i3geo/issues/3

Vulnerabilidade - XSS (Cross Site Scripting) or HTML Injection - svg2img.php · Issue #3 · edmoretti/i3geo · GitHub

github.com
text/html

MISC github.com/edmoretti/i3geo/issues/3

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-2022-34092 : 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 22:09:52
 @LinInfoSec	Php - CVE-2022-34092: github.com/saladesituacao...	2022-07-15 01:00:25
 @threatmeter	CVE-2022-34092 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-2022-34092 - Portal do Software Publico Brasileiro i3geo v7.0.5 was discovered to... twitter.com/i/web/status/1...	2022-07-15 07:09:49
 /r/netcve	CVE-2022-34092	2022-07-14 22:38:45

← Previous ID

Next ID →

this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)