



CVE-2022-42466

Published on: Not Yet Published

Last Modified on: 10/21/2022 04:31:00 PM UTC

CVE-2022-42466

Source: Mitre

Source: NIST

CVE.ORG

Print: PDF



Certain versions of [Isis](#) from [Apache](#) contain the following vulnerability:

Prior to 2.0.0-M9, it was possible for an end-user to set the value of an editable string property of a domain object to a value that would be rendered unchanged when the value was saved. In particular, the end-user could enter javascript or similar and this would be executed. As of this release, the inputted strings are properly escaped when rendered.

CVE-2022-42466 has been assigned by security@apache.org to track the vulnerability - currently rated as **MEDIUM** severity.

Affected Vendor/Software: **Apache Software Foundation - Apache Isis** version < 2.0.0-M9

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

CVE References

Description	Tags	Link
No Description Provided	lists.apache.org text/html	MISC lists.apache.org/thread/83ftj5jgtv3mbm28w3trjyvd591jztrz
oss-security - CVE-2022-42466: Apache Isis: XSS vulnerability, eg for String properties.	www.openwall.com text/html	MLIST [oss-security] 20221019 CVE-2022-42466: Apache Isis: XSS vulnerability, eg for String properties.

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	Apache	Isis	All	All	All	All
Application	Apache	Isis	2.0.0	milestone1	All	All
Application	Apache	Isis	2.0.0	milestone2	All	All
Application	Apache	Isis	2.0.0	milestone3	All	All
Application	Apache	Isis	2.0.0	milestone4	All	All
Application	Apache	Isis	2.0.0	milestone5	All	All
Application	Apache	Isis	2.0.0	milestone6	All	All
Application	Apache	Isis	2.0.0	milestone7	All	All
Application	Apache	Isis	2.0.0	milestone8	All	All
cpe:2.3:a:apache:isis:*.***.***.***:						
cpe:2.3:a:apache:isis:2.0.0:milestone1:*.***.***.***:						
cpe:2.3:a:apache:isis:2.0.0:milestone2:*.***.***.***:						
cpe:2.3:a:apache:isis:2.0.0:milestone3:*.***.***.***:						
cpe:2.3:a:apache:isis:2.0.0:milestone4:*.***.***.***:						
cpe:2.3:a:apache:isis:2.0.0:milestone5:*.***.***.***:						
cpe:2.3:a:apache:isis:2.0.0:milestone6:*.***.***.***:						
cpe:2.3:a:apache:isis:2.0.0:milestone7:*.***.***.***:						
cpe:2.3:a:apache:isis:2.0.0:milestone8:*.***.***.***:						

Discovery Credit

Apache Isis would like to thank Qing Xu for reporting this issue

Social Mentions		
Source	Title	Posted (UTC)
 @CVEreport	CVE-2022-42466 : Prior to 2.0.0-M9, it was possible for an end-user to set the value of an editable string property... twitter.com/i/web/status/1...	2022-10-19 07:30:31
 /r/netcve	CVE-2022-42466	2022-10-19 08:38:42

© [CVE.report](#) 2023   |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to 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](#)