



CVE-2021-32106

Published on: 06/08/2021 12:00:00 AM UTC

Last Modified on: 09/16/2021 01:21:00 PM UTC

CVE-2021-32106

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

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

In ICEcoder 8.0 allows, a reflected XSS vulnerability was identified in the multiple-results.php page due to insufficient sanitization of the `_GET['replace']` variable. As a result, arbitrary Javascript code can get executed.

CVE-2021-32106 has been assigned by [M](#) cve@mitre.org to track the vulnerability - currently rated as **MEDIUM** severity.

CVSS3 Score: **5.4 - MEDIUM**

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

CVSS2 Score: **3.5 - LOW**

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

CVE References

Description	Tags	Link
XSS in multiple-results.php	groups.google.com text/html	MISC groups.google.com/g/icecoder/c/xAc8_1UPxQ
ICEcoder 8.0 multiple-results.php replace cross site scripting - Cloud WAF	prophaze.com text/html	MISC prophaze.com/cve/icecoder-8-0-multiple-results-php-replace-cross-site-scripting/

There are currently no QIDs associated with this CVE

Type	Vendor	Product	Version	Update	Edition	Language
Application	Icecoder	Icecoder	8.0	All	All	All
Application	Icecoder	Icecoder	8.0	-	All	All
cpe:2.3:a:icecoder:icecoder:8.0:*:*:*:*:*:						
cpe:2.3:a:icecoder:icecoder:8.0:-:*:*:*:*:						

No vendor comments have been submitted for this CVE

Source	Title	Posted (UTC)
@CVEreport	CVE-2021-32106 : In ICEcoder 8.0 allows, a reflected #XSS vulnerability was identified in the multiple-results.php p... twitter.com/i/web/status/1...	2021-06-08 13:05:10
/r/netcve	CVE-2021-32106	2021-06-08 13:41:18

Next ID→