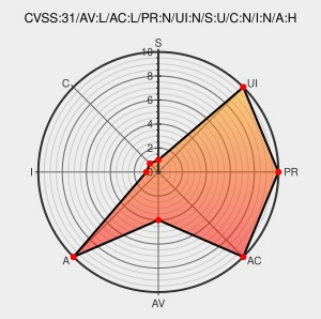
CVE-2021-32821

Published on: Not Yet Published

Last Modified on: 01/10/2023 03:02:00 PM UTC

CVE-2021-32821 - advisory for GHSL-2020-345

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



Certain versions of Mootools from Mootools contain the following vulnerability:

MooTools is a collection of JavaScript utilities for JavaScript developers. All known versions include a CSS selector parser that is vulnerable to Regular Expression Denial of Service (ReDoS). An attack requires that an attacker can inject a string into a CSS selector at runtime, which is quite common with e.g. jQuery CSS selectors. No patches are available for this issue.

CVE-2021-32821 has been assigned by security-advisories@github.com to track the vulnerability - currently rated as HIGH severity.

Affected Vendor/Software: **mootools** - **mootools-core** version **<= 1.6.0**

CVSS3 Score: 7.5 - HIGH

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

CVE References

Description	Tags	Link
GHSL-2020-345: Regular expression Denial of Service in mootools - CVE-2021-32821 | GitHub Security Lab	securitylab.github.com text/html	CONFIRM securitylab.github.com/advisories/GHSL-2020-345-redos-mootools/

There are currently no QIDs associated with this CVE

Exploit/POC from Github

MooTools is a collection of JavaScript utilities for JavaScript developers. All known versions include a CSS selector…

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Mootools	Mootools	All	All	All	All

cpe:2.3:a:mootools:mootools:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@GHSecurityLab	GHSL-2020-345: Regular expression Denial of Service in mootools - CVE-2021-32821 github.co/3oXWwiH	2021-05-27 19:51:01
/r/netcve	CVE-2021-32821	2023-01-03 17:38:44

← Previous ID

Next ID→