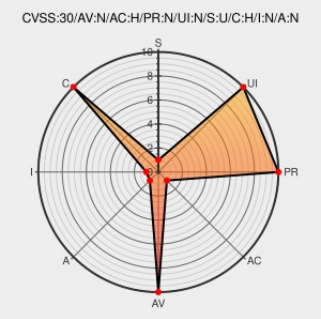
CVE-2016-10535

Published on: 05/31/2018 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:59 PM UTC

CVE-2016-10535

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



Certain versions of Csrf-lite from Csrf-lite Project contain the following vulnerability:

csrf-lite is a cross-site request forgery protection library for framework-less node sites. csrf-lite uses `===`, a fail first string comparison, instead of a time constant string comparison This enables an attacker to guess the secret in no more than (16*18)288 guesses, instead of the 16^18 guesses required were the timing attack not present.

CVE-2016-10535 has been assigned by support@hackerone.com to track the vulnerability - currently rated as MEDIUM severity.

Affected Vendor/Software: **HackerOne** - **csrf-lite node module** version **<=0.1.1**

CVSS3 Score: 5.9 - MEDIUM

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

CVSS2 Score: 4.3 - MEDIUM

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

CVE References

Description	Tags	Link
Overview	Third Party Advisory	MISC

	nodesecurity.io text/html	nodesecurity.io/advisories/94
Added time constant string comparison by twolfson · Pull Request #1 · isaacs/csrf-lite · GitHub	Third Party Advisory github.com text/html	MISC github.com/isaacs/csrf-lite/pull/1

Related QID Numbers

983978 Nodejs (npm) Security Update for csrf-lite (GHSA-hjhr-r3gq-qvp6)

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Csrf-lite Project	Csrf-lite	All	All	All	All

cpe:2.3:a:csrf-lite_project:csrf-lite:*:*:*:*:*:node.js:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→