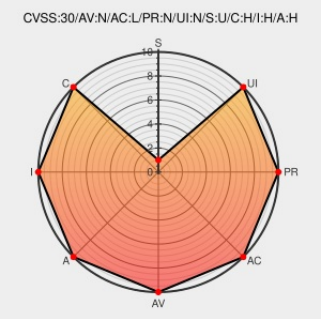
CVE-2019-1010191

Published on: 07/24/2019 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:27:56 PM UTC

CVE-2019-1010191

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



Certain versions of Marginalia from Marginalia Project contain the following vulnerability:

marginalia < 1.6 is affected by: SQL Injection. The impact is: The impact is a injection of any SQL queries when a user controller argument is added as a component. The component is: Affects users that add a component that is user controller, for instance a parameter or a header. The attack vector is: Hacker inputs a SQL to a vulnerable vector(header, http parameter, etc). The fixed version is: 1.6.

CVE-2019-1010191 has been assigned by cve-assign@distributedweaknessfiling.org to track the vulnerability - currently rated as CRITICAL severity.

Affected Vendor/Software: **marginalia** - **marginalia** version **< 1.6 [fixed: 1.6]**

CVSS3 Score: 9.8 - CRITICAL

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

CVSS2 Score: 7.5 - HIGH

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

CVE References

Description	Tags	Link

Description	Tags	Link
improved sql comment handling by igorwwwwwwwwwwwwwwwwwwww · Pull Request #73 · basecamp/marginalia · GitHub	Issue Tracking Third Party Advisory github.com text/html	MISC github.com/basecamp/marginalia/pull/73/

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Marginalia Project	Marginalia	All	All	All	All
Application	Marginalia Project	Marginalia	All	All	All	All

cpe:2.3:a:marginalia_project:marginalia:*:*:*:*:*:*:*:*:

cpe:2.3:a:marginalia_project:marginalia:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→