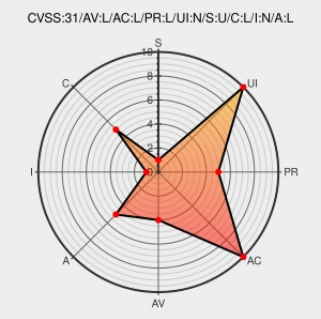
CVE-2020-7617

Published on: 04/02/2020 12:00:00 AM UTC

Last Modified on: 06/28/2022 02:11:00 PM UTC

CVE-2020-7617

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



Certain versions of Ini-parser from Ini-parser Project contain the following vulnerability:

ini-parser through 0.0.2 is vulnerable to Prototype Pollution.The library could be tricked into adding or modifying properties of Object.prototype using a '__proto__' payload.

CVE-2020-7617 has been assigned by report@snyk.io to track the vulnerability - currently rated as CRITICAL severity.

```
var a = require("ini-parser"); a.parse('[__proto__]\ntoString=JHU'); console.log({}.toString);
```

Affected Vendor/Software: **rawiroaisen** - **ini-parser** version **<= 0.0.2**

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

Prototype Pollution in ini-parser | Snyk	Mitigation Third Party Advisory snyk.io text/html	CONFIRM N/A
node-ini-parser/index.js at master · rawiroaisen/node-ini-parser · GitHub	Patch Third Party Advisory github.com text/html	MISC github.com/rawiroaisen/node-ini-parser/blob/master/index.js#L14

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

Related QID Numbers

981451 Nodejs (npm) Security Update for ini-parser (GHSA-96r7-mrqf-jhcc)

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Ini-parser Project	Ini-parser	All	All	All	All

cpe:2.3:a:ini-parser_project:ini-parser:*:*:*:*:*:*:*:*:

Discovery Credit

JHU System Security Lab

← Previous ID

Next ID→