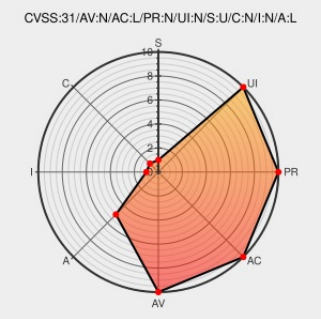
CVE-2021-21317

Published on: 02/16/2021 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:28:57 PM UTC

CVE-2021-21317 - advisory for GHSA-p4pj-mg4r-x6v4

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



Certain versions of Uap-core from Uap-core Project contain the following vulnerability:

uap-core in an open-source npm package which contains the core of BrowserScope's original user agent string parser. In uap-core before version 0.11.0, some regexes are vulnerable to regular expression denial of service (REDoS) due to overlapping capture groups. This allows remote attackers to overload a server by setting the User-Agent header in an HTTP(S) request to maliciously crafted long strings. This is fixed in version 0.11.0. Downstream packages such as uap-python, uap-ruby etc which depend upon uap-core follow different version schemes.

CVE-2021-21317 has been assigned by security-advisories@github.com to track the vulnerability - currently rated as MEDIUM severity.

Affected Vendor/Software: **ua-parser** - **uap-core** version **< 0.11.0**

CVSS3 Score: 5.3 - MEDIUM

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

CVSS2 Score: 5 - MEDIUM

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

CVE References

Description	Tags	Link
Merge pull request from GHSA-p4pj-mg4r-x6v4 · ua-parser/uap-core@dc9925d · GitHub	Patch Third Party Advisory github.com text/html	MISC github.com/ua-parser/uap-core/commit/dc9925d458214cfe87b93e35346980612f6ae96c
Denial of Service in uap-core <=0.10.0 when processing crafted User-Agent strings · Advisory · ua-parser/uap-core · GitHub	Third Party Advisory github.com text/html	CONFIRM github.com/ua-parser/uap-core/security/advisories/GHSA-p4pj-mg4r-x6v4
uap-core - npm	Product Third Party Advisory www.npmjs.com text/html	MISC www.npmjs.com/package/uap-core

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

982947 Nodejs (npm) Security Update for uap-core (GHSA-p4pj-mg4r-x6v4)

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Uap-core Project	Uap-core	All	All	All	All
Application	Uap-core Project	Uap-core	All	All	All	All

cpe:2.3:a:uap-core_project:uap-core:*:*:*:*:*:node.js:*:*

cpe:2.3:a:uap-core_project:uap-core:*:*:*:*:*:node.js:*:*

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→