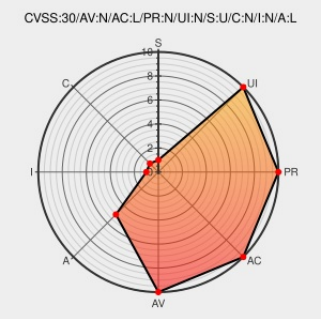
CVE-2018-20164

Published on: 02/13/2019 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:24:37 PM UTC

CVE-2018-20164

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



Certain versions of User Agent Parser-core from Uaparser contain the following vulnerability:

An issue was discovered in regex.yaml (aka regexes.yaml) in UA-Parser UAP-Core before 0.6.0. A Regular Expression Denial of Service (ReDoS) issue allows remote attackers to overload a server by setting the User-Agent header in an HTTP(S) request to a value containing a long digit string. (The UAP-Core project contains the vulnerability, propagating to all implementations.)

CVE-2018-20164 has been assigned by cve@mitre.org to track the vulnerability - currently rated as MEDIUM severity.

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
Performance issue with backtracking caused by some regexes · Issue #332 · ua-parser/uap-core · GitHub	github.com text/html	MISC github.com/ua-parser/uap-core/issues/332

0.6.0 · ua-parser/uap-core@010ccdc · GitHub	Patch Third Party Advisory github.com text/html	MISC github.com/ua-parser/uap-core/commit/010ccdc7303546cd22b9da687c29f4a996990014
Advisory X41-2018-009: DoS Vulnerability in UA-Parser | X41 D-SEC GmbH	Exploit Third Party Advisory www.x41-dsec.de text/html	MISC www.x41-dsec.de/lab/advisories/x41-2018-009-uaparser/
Merge pull request #363 from commenthol/safe-regex · ua-parser/uap-core@156f7e1 · GitHub	Patch Third Party Advisory github.com text/html	MISC github.com/ua-parser/uap-core/commit/156f7e12b215bddbaf3df4514c399d683e6cdadc

Related QID Numbers

981095 Nodejs (npm) Security Update for uap-core (GHSA-fx7m-j728-mjw3)

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Uaparser	User Agent Parser-core	All	All	All	All
Application	Uaparser	User Agent Parser-core	All	All	All	All

cpe:2.3:a:uaparser:user_agent_parser-core:*:*:*:*:*:*:*:*:

cpe:2.3:a:uaparser:user_agent_parser-core:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→