



# CVE-2019-1020012

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF](#)

## Summary

<b>CVE</b>	CVE-2019-1020012
<b>State</b>	PUBLIC
<b>Assigner</b>	cve-assign@distributedweaknessfiling.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2019-07-29 13:15:00 UTC
<b>Updated</b>	2019-08-02 20:25:00 UTC
<b>Description</b>	parse-server before 3.4.1 allows DoS after any POST to a volatile class.

## Risk And Classification

**Problem Types:** CWE-444

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	<a href="#">Parseplatform</a>	<a href="#">Parse-server</a>	All	All	All	All
Application	<a href="#">Parseplatform</a>	<a href="#">Parse-server</a>	All	All	All	All

## References

Reference	S
Potentially critical bug when making POST request against /parse/classes/_Audience · Advisory · parse-community/parse-server · GitHub	M
CVE Program record	C
NVD vulnerability detail	N

No vendor comments have been submitted for this CVE.

## Legacy QID Mappings

981442 Nodejs (npm) Security Update for parse-server (GHSA-2479-qvv7-47qq)

site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

**CVE.report and Source URL Uptime Status [status.cve.report](#)**