



CVE-2018-20745

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

Summary

CVE	CVE-2018-20745
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2019-01-28 08:29:00 UTC
Updated	2019-02-20 16:26:00 UTC
Description	Yii 2.x through 2.0.15.1 actively converts a wildcard CORS policy into reflecting an arbitrary Origin header value, which is in

Risk And Classification

Problem Types: CWE-346

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Yiiframework	Yii	All	All	All	All

References

Reference	Source	Link
CORS security: reflecting any origin header value when configured to * is dangerous · Issue #16193 · yiisoft/yii2 · GitHub	MISC	github
www.usenix.org/system/files/conference/usenixsecurity18/sec18-chen.pdf	MISC	www.
CVE Program record	CVE.ORG	www.
NVD vulnerability detail	NVD	nvd.n

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

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](#).

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status status.cve.report