



CVE-2022-31106

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

Summary

CVE	CVE-2022-31106
State	PUBLIC
Assigner	security-advisories@github.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-06-28 18:15:00 UTC
Updated	2022-07-08 13:40:00 UTC
Description	Underscore.deep is a collection of Underscore mixins that operate on nested objects. Versions of `underscore.deep` prior to

Risk And Classification

Problem Types: CWE-1321

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Clever	Underscore.deep	All	All	All	All

References

Reference
Improperly Controlled Modification of Object Prototype Attributes ('Prototype Pollution') in underscore.deep · Advisory · Clever/underscore.dee
Merge pull request from GHSA-8j79-hfj5-f2xm · Clever/underscore.deep@b5e109a · GitHub
CVE Program record
NVD vulnerability detail

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