



CVE-2020-14942

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

Summary

CVE	CVE-2020-14942
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-06-21 15:15:00 UTC
Updated	2020-06-26 19:34:00 UTC
Description	Tendenci 12.0.10 allows unrestricted deserialization in apps\helpdesk\views\staff.py.

Risk And Classification

Problem Types: CWE-502

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Tendenci	Tendenci	12.0.10	All	All	All
Application	Tendenci	Tendenci	12.0.10	All	All	All

References

Reference	Source	Link	Tags
Unrestricted deserialization · Issue #867 · tendenci/tendenci · GitHub	MISC	github.com	Third Party Advisory
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[982207](#) Python (pip) Security Update for tendenci (GHSA-jqmc-fxxp-r589)

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