



CVE-2019-19461

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

Summary

CVE	CVE-2019-19461
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-03-16 20:15:00 UTC
Updated	2020-03-19 19:29:00 UTC
Description	Post-authentication Stored XSS in Team Password Manager through 7.93.204 allows attackers to steal other users' creden

Risk And Classification

Problem Types: CWE-79

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Teampasswordmanager	Team Password Manager	All	All	All	All

References

Reference	Source	Link
Security issues in TeamPasswordManager and Combodo iTop (CVE-2019-19461, CVE-2019-19821) Pentagrid AG	MISC	www.pen
Team Password Manager Change log	MISC	teampass
CVE Program record	CVE.ORG	www.cve
NVD vulnerability detail	NVD	nvd.nist.g

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