



# CVE-2017-11747

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF !\[\]\(003082e50e3009141f59bd5df831749f\_img.jpg\)](#)

## Summary

<b>CVE</b>	CVE-2017-11747
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2017-07-30 16:29:00 UTC
<b>Updated</b>	2020-03-31 15:15:00 UTC
<b>Description</b>	main.c in Tinyproxy 1.8.4 and earlier creates a /run/tinyproxy/tinyproxy.pid file after dropping privileges to a non-root account

## Risk And Classification

**Problem Types:** CWE-269

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	<a href="#">Tinyproxy Project</a>	<a href="#">Tinyproxy</a>	All	All	All	All

## References

Reference	Source	Link
tinyproxy should create its PID file before dropping privileges (CVE-2017-11747) - Issue #106 - tinyproxy/tinyproxy - GitHub	MISC	<a href="#">github</a>
[SECURITY] [DLA 2163-1] tinyproxy security update	MLIST	<a href="#">list</a>
CVE Program record	CVE.ORG	<a href="#">www</a>
NVD vulnerability detail	NVD	<a href="#">nvd</a>

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](https://cve.report/api)

**CVE.report and Source URL Uptime Status** [status.cve.report](https://status.cve.report)