



# CVE-2018-20552

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

## Summary

<b>CVE</b>	CVE-2018-20552
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2018-12-28 16:29:00 UTC
<b>Updated</b>	2022-04-02 03:30:00 UTC
<b>Description</b>	Tcpreplay before 4.3.1 has a heap-based buffer over-read in packet2tree in tree.c.

## Risk And Classification

**Problem Types:** CWE-125

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	<a href="#">Appneta</a>	<a href="#">Tcpreplay</a>	All	All	All	All
Application	<a href="#">Appneta</a>	<a href="#">Tcpreplay</a>	All	All	All	All
Application	<a href="#">Broadcom</a>	<a href="#">Tcpreplay</a>	All	All	All	All

## References

Reference	Source	Li
Bug #530 Fix heap overflow on zero or 0xFFFF packet length by fklassen · Pull Request #532 · appneta/tcpreplay · GitHub	MISC	<a href="#">git</a>
AddressSanitizer: 2 heap-buffer-overflow problems (packet2tree() && get_l2len()) · Issue #530 · appneta/tcpreplay · GitHub	MISC	<a href="#">git</a>
CVE Program record	CVE.ORG	<a href="#">wv</a>
NVD vulnerability detail	NVD	<a href="#">nv</a>

No vendor comments have been submitted for this CVE.

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

completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

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)