



CVE-2018-13112

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF !\[\]\(003082e50e3009141f59bd5df831749f_img.jpg\)](#)

Summary

CVE	CVE-2018-13112
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2018-07-03 17:29:00 UTC
Updated	2022-04-02 03:30:00 UTC
Description	get_I2len in common/get.c in Tcpsreplay 4.3.0 beta1 allows remote attackers to cause a denial of service (heap-based buffer overflow) via crafted packets.

Risk And Classification

Problem Types: CWE-125

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Appneta	Tcpsreplay	4.3.0	beta1	All	All
Application	Appneta	Tcpsreplay	4.3.0	beta1	All	All
Application	Broadcom	Tcpsreplay	4.3.0	beta1	All	All

References

Reference	Source	Link	Tags
heap-buffer-overflow in /src/common/get.c:174 function get_I2len · Issue #477 · appneta/tcpsreplay · GitHub	MISC	github.com	Exploit
CVE Program record	CVE.ORG	www.cve.org	Canonical
NVD vulnerability detail	NVD	nvd.nist.gov	Canonical

No vendor comments have been submitted for this CVE.

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

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

CVE.report and Source URL Uptime Status status.cve.report