



CVE-2017-6429

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

Summary

CVE	CVE-2017-6429
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-03-15 15:59:00 UTC
Updated	2022-06-03 14:34:00 UTC
Description	Buffer overflow in the tcpcapinfo utility in Tcpreplay before 4.2.0 Beta 1 allows remote attackers to have unspecified impact

Risk And Classification

Problem Types: CWE-119

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Appneta	Tcpreplay	All	All	All	All
Application	Broadcom	Tcpreplay	All	All	All	All

References

Reference	Source	Link	Tag
SecurityFocus	BUGTRAQ	www.securityfocus.com	
tcpcapinfo buffer overflow vulnerablily · Issue #278 · appneta/tcpreplay · GitHub	CONFIRM	github.com	Exp
#278 fail if capture has a packet that is too large (#286) · appneta/tcpreplay@d689d14 · GitHub	CONFIRM	github.com	Pat
Tcpreplay 'Tcpcapinfo' Utility CVE-2017-6429 Buffer Overflow Vulnerability	BID	www.securityfocus.com	Thir
Release v4.2.0-beta1 · appneta/tcpreplay · GitHub	CONFIRM	github.com	Rel
CVE Program record	CVE.ORG	www.cve.org	can
NVD vulnerability detail	NVD	nvd.nist.gov	can

No vendor comments have been submitted for this CVE.

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

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, 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](#)

CVE.report and Source URL Uptime Status [status.cve.report](#)