CVE-2019-8376

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2019-8376
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2019-02-17 02:29:00 UTC
Updated	2023-11-07 03:13:00 UTC
Description	An issue was discovered in Tcpreplay 4.3.1. A NULL pointer dereference occurred in the function get_layer4_v6() located a

Risk And Classification

Problem Types: CWE-476

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Appneta	Tcpreplay	4.3.1	All	All	All
Application	Appneta	Tcpreplay	4.3.1	All	All	All
Application	Broadcom	Tcpreplay	4.3.1	All	All	All
Operating System	Fedoraproject	Fedora	28	All	All	All
Operating System	Fedoraproject	Fedora	29	All	All	All
Operating System	Fedoraproject	Fedora	30	All	All	All
Operating System	Fedoraproject	Fedora	28	All	All	All
Operating System	Fedoraproject	Fedora	29	All	All	All

References

Reference	Source
[SECURITY] Fedora 29 Update: tcpreplay-4.3.2-1.fc29 - package-announce - Fedora Mailing-Lists	FEDORA
Malformed Request	BID
[SECURITY] Fedora 30 Update: tcpreplay-4.3.2-1.fc30 - package-announce - Fedora Mailing-Lists	
[SECURITY] Fedora 30 Update: tcpreplay-4.3.2-1.fc30 - package-announce - Fedora Mailing-Lists	FEDORA
CVE-2019-8376: NULL POINTER DEREFERENCE Vulnerability in function get_layer4_v6() - tcpreplay-4.3.1 - Loginsoft Research	MISC
[SECURITY] Fedora 28 Update: tcpreplay-4.3.2-1.fc28 - package-announce - Fedora Mailing-Lists	FEDORA

NULL pointer dereference in get_layer4_v6() · Issue #537 · appneta/tcpreplay · GitHub	MISC
[SECURITY] Fedora 28 Update: tcpreplay-4.3.2-1.fc28 - package-announce - Fedora Mailing-Lists	
[SECURITY] Fedora 29 Update: tcpreplay-4.3.2-1.fc29 - package-announce - Fedora Mailing-Lists	
CVE Program record	CVE.OR
NVD vulnerability detail	NVD

No vendor comments have been submitted for this CVE.

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

Free CVE JSON API cve.report/api

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