



CVE-2018-18409

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

Summary

CVE	CVE-2018-18409
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2018-10-17 04:29:00 UTC
Updated	2023-11-07 02:55:00 UTC
Description	A stack-based buffer over-read exists in setbit() at iptree.h of TCPFLOW 1.5.0, due to received incorrect values causing inc

Risk And Classification

Problem Types: CWE-125

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Canonical	Ubuntu Linux	16.04	All	All	All
Operating System	Canonical	Ubuntu Linux	18.04	All	All	All
Operating System	Canonical	Ubuntu Linux	18.10	All	All	All
Operating System	Canonical	Ubuntu Linux	16.04	All	All	All
Operating System	Canonical	Ubuntu Linux	18.04	All	All	All
Operating System	Canonical	Ubuntu Linux	18.10	All	All	All
Application	Digitalcorpora	Tcpflow	1.5.0	All	All	All
Application	Digitalcorpora	Tcpflow	1.5.0	All	All	All
Operating System	Fedoraproject	Fedora	28	All	All	All
Operating System	Fedoraproject	Fedora	29	All	All	All
Operating System	Fedoraproject	Fedora	28	All	All	All
Operating System	Fedoraproject	Fedora	29	All	All	All

References

Reference	Source	Link	Tags
[SECURITY] Fedora 28 Update: tcpflow-1.5.0-4.fc28 - package-announce - Fedora Mailing-Lists	FEDORA	lists.fedoraproject.org	Mailir
[SECURITY] Fedora 28 Update: tcpflow-1.5.0-4.fc28 - package-announce - Fedora Mailing-Lists		lists.fedoraproject.org	

[SECURITY] Fedora 29 Update: tcpflow-1.5.0-4.fc29 - package-announce - Fedora Mailing-Lists		lists.fedoraproject.org	
[SECURITY] Fedora 29 Update: tcpflow-1.5.0-4.fc29 - package-announce - Fedora Mailing-Lists	FEDORA	lists.fedoraproject.org	Mailing
Stack-based buffer overflow in setbit() · Issue #195 · simsong/tcpflow · GitHub	MISC	github.com	Exploit
USN-3955-1: tcpflow vulnerabilities Ubuntu security notices	UBUNTU	usn.ubuntu.com	Third
CVE Program record	CVE.ORG	www.cve.org	canon
NVD vulnerability detail	NVD	nvd.nist.gov	canon



No vendor comments have been submitted for this CVE.

Legacy QID Mappings
500689 Alpine Linux Security Update for tcpflow
504458 Alpine Linux Security Update for tcpflow

© [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