CVE-2003-0671

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

Summary

CVE	CVE-2003-0671
State	PUBLISHED
Assigner	mitre
Source Priority	CVE Program / NVD first with legacy fallback
Published	2003-08-27 04:00:00 UTC
Updated	2025-04-03 01:03:51 UTC
Description	Format string vulnerability in tcpflow, when used in a setuid context, allows local users to execute arbitrary code via the dev

Risk And Classification

Primary CVSS: v2.0 7.2 from nvd@nist.gov

AV:L/AC:L/Au:N/C:C/I:C/A:C

Problem Types: NVD-CWE-Other | n/a

CVSS v2.0 Breakdown

Access Vector

Local

Access Complexity

Low

Authentication

None

Confidentiality

Complete

Integrity

Complete

Availability

Complete

AV:L/AC:L/Au:N/C:C/I:C/A:C

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Jeremy Elson	Tcpflow	0.10	All	All	All

Application	Jeremy Elson	Tcpflow	0.11	All	All	All
Application	Jeremy Elson	Tcpflow	0.12	All	All	All
Application	Jeremy Elson	Tcpflow	0.20	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Na	N/a	affected n/a	Not specified

References

Reference	Source	Link	Tags
www.atstake.com/research/advisories/2003/a080703-1.txt	af854a3a-2127-422b-91ae-364da2661108	www.atstake.com	Exploit, Patch,
www.atstake.com/research/advisories/2003/a080703-2.txt	af854a3a-2127-422b-91ae-364da2661108	www.atstake.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analy

No vendor comments have been submitted for this CVE.

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