



CVE-2010-2799

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

Summary

CVE	CVE-2010-2799
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2010-09-14 21:00:00 UTC
Updated	2010-09-15 04:00:00 UTC
Description	Stack-based buffer overflow in the nestlex function in nestlex.c in Socat 1.5.0.0 through 1.7.1.2 and 2.0.0-b1 through 2.0.0-

Risk And Classification

Problem Types: CWE-119

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Dest-unreach	Socat	1.5.0.0	All	All	All
Application	Dest-unreach	Socat	1.6.0.0	All	All	All
Application	Dest-unreach	Socat	1.6.0.1	All	All	All
Application	Dest-unreach	Socat	1.7.0.0	All	All	All
Application	Dest-unreach	Socat	1.7.0.1	All	All	All
Application	Dest-unreach	Socat	1.7.1.0	All	All	All
Application	Dest-unreach	Socat	1.7.1.1	All	All	All
Application	Dest-unreach	Socat	2.0.0	b1	All	All
Application	Dest-unreach	Socat	2.0.0	b2	All	All
Application	Dest-unreach	Socat	2.0.0	b3	All	All
Application	Dest-unreach	Socat	1.5.0.0	All	All	All
Application	Dest-unreach	Socat	1.6.0.0	All	All	All
Application	Dest-unreach	Socat	1.6.0.1	All	All	All
Application	Dest-unreach	Socat	1.7.0.0	All	All	All
Application	Dest-unreach	Socat	1.7.0.1	All	All	All
Application	Dest-unreach	Socat	1.7.1.0	All	All	All
Application	Dest-unreach	Socat	1.7.1.1	All	All	All

Application	Dest-unreach	Socat	2.0.0	b1	All	All
Application	Dest-unreach	Socat	2.0.0	b2	All	All
Application	Dest-unreach	Socat	2.0.0	b3	All	All

References

Reference	Source	Link
Socat security advisory 2	CONFIRM	www.des
www.dest-unreach.org/socat/download/socat-1.7.1.3.patch	CONFIRM	www.des
620426 – (CVE-2010-2799) CVE-2010-2799 Socat: Stack overflow by lexical scanning of nested character patterns	CONFIRM	bugzilla.r
330785 – (CVE-2010-2799) <net-misc/socat-1.7.1.3: stack overflow vulnerability (CVE-2010-2799)	CONFIRM	bugs.ger
#591443 - CVE-2010-2799: Stack overflow by lexical scanning of nested character patterns - Debian Bug report logs	CONFIRM	bugs.deb
Debian -- Security Information -- DSA-2090-1 socat	DEBIAN	www.deb
CVE Program record	CVE.ORG	www.cve
NVD vulnerability detail	NVD	nvd.nist.g

No vendor comments have been submitted for this CVE.

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