CVE-2012-0219

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

Summary

CVE	CVE-2012-0219
State	PUBLISHED
Assigner	debian
Source Priority	CVE Program / NVD first with legacy fallback
Published	2012-06-21 15:55:11 UTC
Updated	2026-04-29 01:13:23 UTC
Description	Heap-based buffer overflow in the xioscan_readline function in xio-readline.c in socat 1.4.0.0 through 1.7.2.0 and 2.0.0-b1 t

Risk And Classification

Primary CVSS: v2.0 6.2 from nvd@nist.gov

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

Problem Types: CWE-119 | n/a

CVSS v2.0 Breakdown

Access Vector

Local

Access Complexity

High

Authentication

None

Confidentiality

Complete

Integrity

Complete

Availability

Complete

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Dest-unreach	Socat	1.4.0.0	All	All	All

Application	Dest-unreach	Socat	1.4.0.1	All	All	All
Application	Dest-unreach	Socat	1.4.0.2	All	All	All
Application	Dest-unreach	Socat	1.4.0.3	All	All	All
Application	Dest-unreach	Socat	1.4.1.0	All	All	All
Application	Dest-unreach	Socat	1.4.2.0	All	All	All
Application	Dest-unreach	Socat	1.4.3.1	All	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	1.7.1.2	All	All	All
Application	Dest-unreach	Socat	1.7.1.3	All	All	All
Application	Dest-unreach	Socat	1.7.2.0	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	2.0.0	b4	All	All

Vendor Declared Affected Products

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

References

Reference	Source
Security Alerts - Secunia	af854a3a-2127-422b-91ae-364da2
Socat security advisory 3	af854a3a-2127-422b-91ae-364da2
www.osvdb.org/81969	af854a3a-2127-422b-91ae-364da2
Gentoo Linux Documentation -- socat: Arbitrary code execution	af854a3a-2127-422b-91ae-364da2
socat Buffer Overflow in xioscan_readline() Lets Local Users Gain Elevated Privileges - SecurityTracker	af854a3a-2127-422b-91ae-364da2
oss-security - socat security advisory	af854a3a-2127-422b-91ae-364da2
openSUSE alert openSUSE-SU-2012:0809-1 (socat) [LWN.net]	af854a3a-2127-422b-91ae-364da2
Malformed Request	af854a3a-2127-422b-91ae-364da2
[SECURITY] Fedora 17 Update: socat-1.7.2.1-1.fc17	af854a3a-2127-422b-91ae-364da2
[SECURITY] Fedora 16 Update: socat-1.7.2.1-1.fc16	af854a3a-2127-422b-91ae-364da2

[SECURITY] Fedora 16 Update: socat-1.7.2.1-1.fc16	af854a3a-2127-422b-91ae-364da2
Security Alerts - Secunia	af854a3a-2127-422b-91ae-364da2
Support / Security / Advisories / / MDVSA-2013:169 | Mandriva	af854a3a-2127-422b-91ae-364da2
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD

No vendor comments have been submitted for this CVE.

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