CVE-2001-1104

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

Summary

CVE	CVE-2001-1104
State	PUBLISHED
Assigner	mitre
Source Priority	CVE Program / NVD first with legacy fallback
Published	2001-07-25 04:00:00 UTC
Updated	2025-04-03 01:03:51 UTC
Description	SonicWALL SOHO uses easily predictable TCP sequence numbers, which allows remote attackers to spoof or hijack sessi

Risk And Classification

Primary CVSS: v2.0 7.5 from nvd@nist.gov

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

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

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Low

Authentication

None

Confidentiality

Partial

Integrity

Partial

Availability

Partial

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Sonicwall	Soho	-	All	All	All

Operating System	Sonicwall	Soho Firmware	4.0.0	All	All	All
Operating System	Sonicwall	Soho Firmware	5.0.0	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
SecurityFocus home mailing list: BugTraq	af854a3a-2127-422b-91ae-364da2661108	www.secur
SonicWALL SOHO Firewall Predictable TCP Initial Sequence Number Vulnerability	af854a3a-2127-422b-91ae-364da2661108	www.secur
CVE Program record	CVE.ORG	www.cve.o
NVD vulnerability detail	NVD	nvd.nist.go

No vendor comments have been submitted for this CVE.

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