CVE-2003-1250

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

Summary

CVE	CVE-2003-1250
State	PUBLISHED
Assigner	mitre
Source Priority	CVE Program / NVD first with legacy fallback
Published	2003-12-31 05:00:00 UTC
Updated	2025-04-03 01:03:51 UTC
Description	Efficient Networks 5861 DSL router, when running firmware 5.3.80 configured to block incoming TCP SYN, packets allows

Risk And Classification

Primary CVSS: v2.0 5 from nvd@nist.gov

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

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

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Low

Authentication

None

Confidentiality

None

Integrity

None

Availability

Partial

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Efficient Networks	5861 Dsl Router	5.3.80_firmware	All	All	All

Vendor Declared Affected Products

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

References

Reference
SecurityFocus
archives.neohapsis.com/archives/vulnwatch/2003-q1/0015.html
SecurityFocus
Efficient Networks DSL Router Denial Of Service Vulnerability
Efficient Networks 5861 DSL Router Processing Bug Lets Remote Users Crash the Router - SecurityTracker
ISS X-Force Database:efficient-dsl-portscan-dos(11032): Efficient Networks Business Class DSL router port scan denial of service
(Vendor Describes Fixes) Re: Efficient Networks 5861 DSL Router Processing Bug Lets Remote Users Crash the Router - SecurityTracker
CVE Program record
NVD vulnerability detail

No vendor comments have been submitted for this CVE.

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