CVE-2002-0603

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

Summary

CVE	CVE-2002-0603
State	PUBLISHED
Assigner	mitre
Source Priority	CVE Program / NVD first with legacy fallback
Published	2002-06-18 04:00:00 UTC
Updated	2025-04-03 01:03:51 UTC
Description	Snapgear Lite+ firewall 1.5.3 allows remote attackers to cause a denial of service (IPSEC crash) via a zero length packet to

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
Application	Snapgear	Snapgear Lite Firewall	1.5.3	All	All	All

Vendor Declared Affected Products

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

References

Reference	Source
ISS X-Force Database: snapgear-vpn-ipsec-dos (8987): SnapGear LITE+ VPN router IPSEC denial of service	af854a3a-2127-422b-91ae-3
marc.info	af854a3a-2127-422b-91ae-3
Snap Gear - Internet Security Appliances, VPN Routers	af854a3a-2127-422b-91ae-3
Snapgear Lite+ Firewall IPSEC Denial of Service Vulnerability	af854a3a-2127-422b-91ae-3
archives.neohapsis.com/archives/vulnwatch/2002-q2/0050.html	af854a3a-2127-422b-91ae-3
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.