CVE-2009-2918

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

Summary

CVE	CVE-2009-2918
State	PUBLISHED
Assigner	mitre
Source Priority	CVE Program / NVD first with legacy fallback
Published	2009-08-21 11:30:00 UTC
Updated	2026-04-23 00:35:47 UTC
Description	The tgbvpn.sys driver in TheGreenBow IPSec VPN Client 4.61.003 allows local users to cause a denial of service (NULL pc

Risk And Classification

Primary CVSS: v2.0 2.1 from nvd@nist.gov

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

Problem Types: CWE-20 | n/a

CVSS v2.0 Breakdown

Access Vector

Local

Access Complexity

Low

Authentication

None

Confidentiality

None

Integrity

None

Availability

Partial

AV:L/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	Thegreenbow	Thegreenbow Vpn Client	4.61.003	All	All	All

Vendor Declared Affected Products

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

References

Reference	Source
TheGreenBow IPSec VPN Client TgbVPN.sys Denial of Service - Secunia Advisories - Vulnerability Information - Secunia.com	af854a3a-21
SecurityFocus	af854a3a-21
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	af854a3a-21
EvilFingers - TheGreenBow VPN Client tgbvpn.sys DoS and Potential Local Privilege Escalation Vulnerability.	af854a3a-21
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.