



CVE-2003-0554

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

CVE	CVE-2003-0554
State	PUBLISHED
Assigner	mitre
Source Priority	CVE Program / NVD first with legacy fallback
Published	2003-08-18 04:00:00 UTC
Updated	2025-04-03 01:03:51 UTC
Description	NeoModus Direct Connect 1.0 build 9, and possibly other versions, allows remote attackers to cause a denial of service (co

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	Neomodus	Direct Connect	1.0	All	All	All

Vendor Declared Affected Products				
Source	Vendor	Product	Version	Platforms
CNA	Na	N/a	affected n/a	Not specified
References				
Reference			Source	
'[sec-labs] Remote Denial of Service vulnerability in NeoModus' - MARC			af854a3a-2127-422b-91ae-364d	
[Full-Disclosure] [sec-labs] Remote Denial of Service vulnerability in NeoModus Direct Connect 1.0 build 9			af854a3a-2127-422b-91ae-364d	
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.				