CVE-1999-0909

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

Summary

CVE	CVE-1999-0909
State	PUBLISHED
Assigner	mitre
Source Priority	CVE Program / NVD first with legacy fallback
Published	1999-09-20 04:00:00 UTC
Updated	2025-04-03 01:03:51 UTC
Description	Multihomed Windows systems allow a remote attacker to bypass IP source routing restrictions via a malformed packet with

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: CWE-264 | 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
Application	Microsoft	Terminal Server	All	All	All	All

Operating System	Microsoft	Windows 95	0a	All	All	All
Operating System	Microsoft	Windows 95	0b	All	All	All
Operating System	Microsoft	Windows 98se	All	All	All	All
Operating System	Microsoft	Windows Nt	4.0	All	All	All
Operating System	Microsoft	Windows Nt	4.0	sp1	All	All
Operating System	Microsoft	Windows Nt	4.0	sp2	All	All
Operating System	Microsoft	Windows Nt	4.0	sp3	All	All
Operating System	Microsoft	Windows Nt	4.0	sp4	All	All
Operating System	Microsoft	Windows Nt	4.0	sp5	All	All

Vendor Declared Affected Products

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

References

Reference	Source	Link	Tags
Microsoft Security Bulletin MS99-038 - Critical | Microsoft Docs	af854a3a-2127-422b-91ae-364da2661108	docs.microsoft.com	
Microsoft Windows IP Source Routing Vulnerability	af854a3a-2127-422b-91ae-364da2661108	www.securityfocus.com	
Microsoft Support	af854a3a-2127-422b-91ae-364da2661108	support.microsoft.com	
Microsoft Support	MITRE	support.microsoft.com	
CVE Program record	CVE.ORG	www.cve.org	canc
NVD vulnerability detail	NVD	nvd.nist.gov	canc

No vendor comments have been submitted for this CVE.

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