CVE-2000-0070

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

Summary

CVE	CVE-2000-0070
State	PUBLISHED
Assigner	mitre
Source Priority	CVE Program / NVD first with legacy fallback
Published	2000-01-12 05:00:00 UTC
Updated	2025-04-03 01:03:51 UTC
Description	NtImpersonateClientOfPort local procedure call in Windows NT 4.0 allows local users to gain privileges, aka "Spoofed LPC

Risk And Classification

Primary CVSS: v2.0 7.2 from nvd@nist.gov

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

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

CVSS v2.0 Breakdown

Access Vector

Local

Access Complexity

Low

Authentication

None

Confidentiality

Complete

Integrity

Complete

Availability

Complete

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
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
Operating System	Microsoft	Windows Nt	4.0	sp6	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 Support	af854a3a-2127-422b-91ae-364da2661108	support.microsoft.com	
xforce.iss.net/search.php3	af854a3a-2127-422b-91ae-364da2661108	xforce.iss.net	
NT LPC Privilege Escalation Vulnerability	af854a3a-2127-422b-91ae-364da2661108	www.securityfocus.com	
BindView Security Advisory	af854a3a-2127-422b-91ae-364da2661108	www.bindview.com	Expl
Microsoft Security Bulletin MS00-003 - Critical | Microsoft Docs	af854a3a-2127-422b-91ae-364da2661108	docs.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.