CVE-2002-0971

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

Summary

CVE	CVE-2002-0971
State	PUBLISHED
Assigner	mitre
Source Priority	CVE Program / NVD first with legacy fallback
Published	2002-09-24 04:00:00 UTC
Updated	2025-04-03 01:03:51 UTC
Description	Vulnerability in VNC, TightVNC, and TridiaVNC allows local users to execute arbitrary code as LocalSystem by using the W

Risk And Classification

Primary CVSS: v2.0 4.6 from nvd@nist.gov

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

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

CVSS v2.0 Breakdown

Access Vector

Local

Access Complexity

Low

Authentication

None

Confidentiality

Partial

Integrity

Partial

Availability

Partial

AV:L/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	Att	Winvnc Server	3.3.3_r7	All	All	All

Application	Att	Winvnc Server	All	All	All	All
Application	Tightvnc	Tightvnc	1.2.0	All	All	All
Application	Tightvnc	Tightvnc	1.2.1	All	All	All
Application	Tightvnc	Tightvnc	1.2.5	All	All	All
Application	Tridia	Tridiavnc	1.5	All	All	All
Application	Tridia	Tridiavnc	1.5.1	All	All	All
Application	Tridia	Tridiavnc	1.5.2	All	All	All
Application	Tridia	Tridiavnc	1.5.4	All	All	All

Vendor Declared Affected Products

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

References

Reference
Multiple VNC Products For Windows Win32 Messaging API Vulnerability
'Win32 API 'shatter' vulnerability found in VNC-based products' - MARC
ISS X-Force Database: vnc-win32-messaging-privileges (9979): Multiple VNC products could allow an attacker to use the Win32 Messaging A
CVE Program record
NVD vulnerability detail

No vendor comments have been submitted for this CVE.

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