



CVE-2001-0168

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

Summary

CVE	CVE-2001-0168
State	PUBLISHED
Assigner	mitre
Source Priority	CVE Program / NVD first with legacy fallback
Published	2001-05-03 04:00:00 UTC
Updated	2025-04-03 01:03:51 UTC
Description	Buffer overflow in AT&T WinVNC (Virtual Network Computing) server 3.3.3r7 and earlier allows remote attackers to execute

Risk And Classification

Primary CVSS: v2.0 10 from nvd@nist.gov

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

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

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Low

Authentication

None

Confidentiality

Complete

Integrity

Complete

Availability

Complete

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Att	Winvnc	All	All	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	
AT&T WinVNC Server Buffer Overflow Vulnerability	af854a3a-2127-422b-91ae-364da2661108	www.securityfocus.com	Patch, V	
IBM X-Force Exchange	af854a3a-2127-422b-91ae-364da2661108	exchange.xforce.ibmcloud.com		
marc.info	af854a3a-2127-422b-91ae-364da2661108	marc.info		
CERT/CC Vulnerability Note VU#598581	af854a3a-2127-422b-91ae-364da2661108	www.kb.cert.org	US Gove	
CVE Program record	CVE.ORG	www.cve.org	canonica	
NVD vulnerability detail	NVD	nvd.nist.gov	canonica	
No vendor comments have been submitted for this CVE.				
There are currently no legacy QID mappings associated with this CVE.				