



CVE-2007-5057

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

Summary

CVE	CVE-2007-5057
State	PUBLISHED
Assigner	mitre
Source Priority	CVE Program / NVD first with legacy fallback
Published	2007-09-24 22:17:00 UTC
Updated	2026-04-23 00:35:47 UTC
Description	NetSupport Manager Client before 10.20.0004 allows remote attackers to bypass the (1) basic and (2) authentication scher

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: CWE-287 | 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	Netsupport	Netsupport Manager Client	10.00	All	All	All

Application	Netsupport	Netsupport Manager Client	10.20	All	All	All
Application	Netsupport	Netsupport Manager Client	5.00	All	All	All
Application	Netsupport	Netsupport Manager Client	5.01	All	All	All
Application	Netsupport	Netsupport Manager Client	5.02	All	All	All
Application	Netsupport	Netsupport Manager Client	5.02_f1	All	All	All
Application	Netsupport	Netsupport Manager Client	5.03	All	All	All
Application	Netsupport	Netsupport Manager Client	5.05	All	All	All
Application	Netsupport	Netsupport Manager Client	5.30	All	All	All
Application	Netsupport	Netsupport Manager Client	5.31	All	All	All
Application	Netsupport	Netsupport Manager Client	6.00	All	All	All
Application	Netsupport	Netsupport Manager Client	6.10	All	All	All
Application	Netsupport	Netsupport Manager Client	6.11	All	All	All
Application	Netsupport	Netsupport Manager Client	7.01	All	All	All
Application	Netsupport	Netsupport Manager Client	7.10	All	All	All
Application	Netsupport	Netsupport Manager Client	8.00	All	All	All
Application	Netsupport	Netsupport Manager Client	8.10	All	All	All
Application	Netsupport	Netsupport Manager Client	8.50	All	All	All
Application	Netsupport	Netsupport Manager Client	8.60	All	All	All
Application	Netsupport	Netsupport Manager Client	9.00	All	All	All
Application	Netsupport	Netsupport Manager Client	9.10	All	All	All
Application	Netsupport	Netsupport Manager Client	9.50	All	All	All
Application	Netsupport	Netsupport Manager Client	9.60	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	
NetSupport Manager Client Lets Remote Users Execute Commands - SecurityTracker			af854a3a-2127-422b-91ae-364da2661108		www.se	
NetSupport Manager Remote Authentication Bypass Vulnerability			af854a3a-2127-422b-91ae-364da2661108		www.se	
NetSupport Manager Authentication Bypass - CXSecurity.com			af854a3a-2127-422b-91ae-364da2661108		security	
NetSupport Technical Document 543			af854a3a-2127-422b-91ae-364da2661108		www.n	
NetSupport Manager Client Authentication Bypass Vulnerability - Advisories - Secunia			af854a3a-2127-422b-91ae-364da2661108		secunia	
IBM X-Force Exchange			af854a3a-2127-422b-91ae-364da2661108		exchan	
SecurityFocus			af854a3a-2127-422b-91ae-364da2661108		www.se	
CVE Program record			CVE ID		www.c	

CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov
No vendor comments have been submitted for this CVE.		
There are currently no legacy QID mappings associated with this CVE.		

© CVE.report 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of The MITRE Corporation and the authoritative source of CVE content is MITRE's CVE web site. This site includes MITRE data granted under the following license.

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status status.cve.report