



CVE-2003-0711

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

Summary

CVE	CVE-2003-0711
State	PUBLISHED
Assigner	mitre
Source Priority	CVE Program / NVD first with legacy fallback
Published	2003-11-17 05:00:00 UTC
Updated	2025-04-03 01:03:51 UTC
Description	Stack-based buffer overflow in the PCHealth system in the Help and Support Center function in Windows XP and Windows

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: NVD-CWE-Other | 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
Operating System	Microsoft	Windows 2000	All	All	All	All

Operating System	Microsoft	Windows 2000	All	sp1	All	All
Operating System	Microsoft	Windows 2000	All	sp2	All	All
Operating System	Microsoft	Windows 2000	All	sp3	All	All
Operating System	Microsoft	Windows 2000	All	sp4	All	All
Operating System	Microsoft	Windows 2003 Server	enterprise	All	64-bit	All
Operating System	Microsoft	Windows 2003 Server	enterprise_64-bit	All	All	All
Operating System	Microsoft	Windows 2003 Server	r2	All	64-bit	All
Operating System	Microsoft	Windows 2003 Server	r2	All	datacenter_64-bit	All
Operating System	Microsoft	Windows 2003 Server	standard	All	64-bit	All
Operating System	Microsoft	Windows 2003 Server	web	All	All	All
Operating System	Microsoft	Windows Me	All	All	All	All
Operating System	Microsoft	Windows Nt	4.0	All	enterprise_server	All
Operating System	Microsoft	Windows Nt	4.0	All	server	All
Operating System	Microsoft	Windows Nt	4.0	All	terminal_server	All
Operating System	Microsoft	Windows Nt	4.0	All	workstation	All
Operating System	Microsoft	Windows Nt	4.0	sp1	enterprise_server	All
Operating System	Microsoft	Windows Nt	4.0	sp1	server	All
Operating System	Microsoft	Windows Nt	4.0	sp1	terminal_server	All
Operating System	Microsoft	Windows Nt	4.0	sp1	workstation	All
Operating System	Microsoft	Windows Nt	4.0	sp2	enterprise_server	All
Operating System	Microsoft	Windows Nt	4.0	sp2	server	All
Operating System	Microsoft	Windows Nt	4.0	sp2	terminal_server	All
Operating System	Microsoft	Windows Nt	4.0	sp2	workstation	All
Operating System	Microsoft	Windows Nt	4.0	sp3	enterprise_server	All
Operating System	Microsoft	Windows Nt	4.0	sp3	server	All
Operating System	Microsoft	Windows Nt	4.0	sp3	terminal_server	All
Operating System	Microsoft	Windows Nt	4.0	sp3	workstation	All
Operating System	Microsoft	Windows Nt	4.0	sp4	enterprise_server	All
Operating System	Microsoft	Windows Nt	4.0	sp4	server	All
Operating System	Microsoft	Windows Nt	4.0	sp4	terminal_server	All
Operating System	Microsoft	Windows Nt	4.0	sp4	workstation	All
Operating System	Microsoft	Windows Nt	4.0	sp5	enterprise_server	All
Operating System	Microsoft	Windows Nt	4.0	sp5	server	All
Operating System	Microsoft	Windows Nt	4.0	sp5	terminal_server	All
Operating System	Microsoft	Windows Nt	4.0	sp5	workstation	All
Operating System	Microsoft	Windows Nt	4.0	sp6	enterprise_server	All

Operating System	Microsoft	Windows Nt	4.0	sp6	server	All
Operating System	Microsoft	Windows Nt	4.0	sp6	terminal_server	All
Operating System	Microsoft	Windows Nt	4.0	sp6	workstation	All
Operating System	Microsoft	Windows Nt	4.0	sp6a	enterprise_server	All
Operating System	Microsoft	Windows Nt	4.0	sp6a	server	All
Operating System	Microsoft	Windows Nt	4.0	sp6a	workstation	All
Operating System	Microsoft	Windows Xp	All	All	64-bit	All
Operating System	Microsoft	Windows Xp	All	All	home	All
Operating System	Microsoft	Windows Xp	All	gold	professional	All
Operating System	Microsoft	Windows Xp	All	sp1	64-bit	All
Operating System	Microsoft	Windows Xp	All	sp1	home	All

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

References			
Reference	Source	Link	
Repository / Oval Repository	af854a3a-2127-422b-91ae-364da2661108	oval.cve.org	
Microsoft Windows Help And Support Center URI Handler Buffer Overflow Vulnerability	af854a3a-2127-422b-91ae-364da2661108	www.microsoft.com/technet/security/bulletin/MS03-044.mspx	
www.ngssoftware.com/advisories/ms-pchealth.txt	af854a3a-2127-422b-91ae-364da2661108	www.ngssoftware.com/advisories/ms-pchealth.txt	
Microsoft Security Bulletin MS03-044 - Critical Microsoft Docs	af854a3a-2127-422b-91ae-364da2661108	docs.microsoft.com/en-us/security/advisories/ms03-044	
Repository / Oval Repository	af854a3a-2127-422b-91ae-364da2661108	oval.cve.org	
Repository / Oval Repository	af854a3a-2127-422b-91ae-364da2661108	oval.cve.org	
'Microsoft PCHealth 2003/XP Buffer Overflow (#NISR15102003)' - MARC	af854a3a-2127-422b-91ae-364da2661108	marc.info/?l=msrc&m=2003030401	
'Microsoft PCHealth 2003/XP Buffer Overflow (#NISR15102003)' - MARC	af854a3a-2127-422b-91ae-364da2661108	marc.info/?l=msrc&m=2003030401	
CERT/CC Vulnerability Note VU#467036	af854a3a-2127-422b-91ae-364da2661108	www.cve.org/2003/03/04/VU/467036.html	
CERT Advisory CA-2003-27 Multiple Vulnerabilities in Microsoft Windows and Exchange	af854a3a-2127-422b-91ae-364da2661108	www.cve.org/2003/03/04/CA/2003-27.html	
Repository / Oval Repository	af854a3a-2127-422b-91ae-364da2661108	oval.cve.org	
CVE Program record	CVE.ORG	www.cve.org/2003/03/04/CVE-2003-044.html	
NVD vulnerability detail	NVD	nvd.nist.gov/vuln/detail/CVE-2003-044	

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](#)