



The Nachi Worm and Its Variants Important Security Information

(Version 0.10 Draft - 19/09/2003)

This document is intended to provide interim information for the avoidance of a present security threat. It, and any subsequent updates, are available at

<http://www.medway.org.uk/mgfl/nachiinfo.pdf>

1	Who Is Vulnerable?	1
2	Scan tool for Network Administrators available.....	1
3	How to Tell If the Worm Is Affecting Your Computer	2
3.1	Notable symptoms.....	2
4	What to do now	2
4.1	Actions for Network Administrators	2
4.2	Steps for All Computers	2
4.2.1	Update Windows	2
4.2.2	Use Antivirus Software	3
4.3	Remove the Worm	3

1 Who Is Vulnerable?

Users of the following products could be affected by this worm:

- Microsoft® Windows NT® 4.0
- Microsoft Windows® 2000
- Microsoft Windows XP
- Microsoft Windows Server™ 2003

2 Scan tool for Network Administrators available

IT professionals can download a free tool from Microsoft to help them scan their networks for the one of the principal security updates required to provide protection from this worm. The tool is available at:

<http://www.microsoft.com/downloads/details.aspx?FamilyID=c8f04c6c-b71b-4992-91f1-aaa785e709da&DisplayLang=en>

3 How to Tell If the Worm Is Affecting Your Computer

3.1 Notable symptoms

The most evident symptom of Nachi virus infection is slow performance of a network and its Internet connection.

Whether you are experiencing these symptoms or not, we recommend that you apply the patches described in Security Bulletin.

4 What to do now

4.1 Actions for Network Administrators

We recommend that network administrators take the following actions immediately:

- Read the Microsoft Product Support Services (PSS) Security Response Team alert for technical guidance.
- Download the MS03-026 Scanning Tool to identify computers that need the security update addressed in Microsoft Security Bulletin MS03-026.

4.2 Steps for All Computers

If you are using Microsoft® Windows NT® 4.0, Windows® 2000, Windows XP, or Windows Server™ 2003, you should follow the steps in this sequence to help protect your computer and to recover if your computer has been infected.

4.2.1 Update Windows

Download and install all current security update for the version of Windows that you are using from either Windows Update, the Microsoft Download Center or your system supplier if they distribute repackaged security updates. Remember, you must actually install the update to help protect your computer.

To get the security update from Windows Update goto <http://windowsupdate.microsoft.com/>

To Get the Security Update from the Download Center use the links below to go to the appropriate Download Center page. Click Download and a dialog box appears. To begin the download process, do one of the following:

To start the installation immediately, click Open or Run this program from its current location.

To copy the download to your computer for installation, click Save or Save this program to disk. After saving, open the file and follow the installation instructions.

Windows NT Server 4.0 and Windows NT Workstation 4.0

<http://www.microsoft.com/downloads/details.aspx?FamilyID=2cc66f4e-217e-4fa7-bdbf-df77a0b9303f&displaylang=en>

Windows NT Server 4.0, Terminal Server Edition

<http://www.microsoft.com/downloads/details.aspx?FamilyID=6c0f0160-64fa-424c-a3c1-c9fad2dc65ca&DisplayLang=en>

Windows 2000 (requires Windows 2000 Service Pack 2 or later)

<http://www.microsoft.com/downloads/details.aspx?FamilyID=c8b8a846-f541-4c15-8c9f-220354449117&displaylang=en>

Windows XP (32 bit) {Most users have this edition}

4.2.2 Use Antivirus Software

Use antivirus software and make sure you have the latest updates installed. There are several variants of this worm, and the most up-to-date information about them can be found at your antivirus vendor's Web site.

- If you already have antivirus software installed, go to your antivirus vendor's Web site to get the latest updates, also known as virus definitions.
- If you do not have antivirus software installed, get it immediately*. The Sophos antivirus package is licensed for all Medway Grid for Learning applications and is freely available at the support site (<http://support.medway.org.uk/>).

4.3 Remove the Worm

* Use and maintenance of antivirus software is a prerequisite for the good management of a computer network. As documented in other Medway Grid for Learning policies and guidance you should already be running up to date antivirus software.