

CERT Advisory CA-2003-20 W32/Blaster worm

Original issue date: August 11, 2003
Last revised: August 14, 2003
Source: CERT/CC

A complete revision history is at the end of this file.

Systems Affected

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

Overview

The CERT/CC is receiving reports of widespread activity related to a new piece of malicious code known as W32/Blaster. This worm appears to exploit known vulnerabilities in the Microsoft Remote Procedure Call (RPC) Interface.

I. Description

The W32/Blaster worm exploits a vulnerability in Microsoft's DCOM RPC interface as described in [VU#568148](#) and [CA-2003-16](#). Upon successful execution, the worm attempts to retrieve a copy of the file msblast.exe from the compromising host. Once this file is retrieved, the compromised system then runs it and begins scanning for other vulnerable systems to compromise in the same manner. In the course of propagation, a TCP session to port 135 is used to execute the attack. However, access to TCP ports 139 and 445 may also provide attack vectors and should be considered when applying mitigation strategies. Microsoft has published information about this vulnerability in Microsoft Security Bulletin [MS03-026](#).

Lab testing has confirmed that the worm includes the ability to launch a TCP SYN flood denial-of-service attack against [windowsupdate.com](#). We are investigating the conditions under which this attack might manifest itself. Unusual or unexpected traffic to windowsupdate.com may indicate an infection on your network, so you may wish to monitor network traffic.

Sites that do not use windowsupdate.com to manage patches may wish to block outbound traffic to windowsupdate.com. In practice, this may be difficult to achieve, since windowsupdate.com may not resolve to the same address every time. Correctly blocking traffic to windowsupdate.com will require detailed understanding of your network routing architecture, system management needs, and name resolution environment. You should not block traffic to windowsupdate.com without a thorough understanding of your operational needs.

We have been in contact with Microsoft regarding this possibility of this denial-of-service attack.

II. Impact

A remote attacker could exploit these vulnerabilities to execute arbitrary code with Local System privileges or to cause a denial-of-service condition.

III. Solutions

(NOTE: Detailed instructions for recovering Windows XP systems from the W32/Blaster worm can be found in the [W32/Blaster Recovery Tech Tip](#))

Apply patches

All users are encouraged to apply the patches referred to in Microsoft Security Bulletin [MS03-026](#) as soon as possible in order to mitigate the vulnerability described in [VU#568148](#). These patches are also available via Microsoft's [Windows Update](#) service.

Systems running Windows 2000 may still be vulnerable to at least a denial-of-service attack via [VU#326746](#) if their DCOM RPC service is available via the network. Therefore, sites are encouraged to use the packet filtering tips below in addition to applying the patches supplied in [MS03-026](#).

It has been reported that some affected machines are not able to stay connected to the network long enough to download patches from Microsoft. For hosts in this situation, the CERT/CC recommends the following:

1. Physically disconnect the system from the network.
2. Check the system for signs of compromise.
 - In most cases, an infection will be indicated by the presence of the registry key "HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\windows auto update" with a value of msblast.exe. Other possible values include teekids.exe and penis32.exe. If this key is present, remove it using a registry editor.
3. If you're infected, terminate the running copy of msblast.exe, teekids.exe or penis32.exe using the Task Manager.
4. Search for and delete files named msblast.exe, teekids.exe or penis32.exe.
5. Take one of the following steps to protect against the compromise prior to installing the Microsoft patch:
 - Disable DCOM as described in [MS03-026](#) and Microsoft Knowledge Base Article [825750](#).
 - Enable Microsoft's Internet Connection Firewall (ICF) or another host-level packet filtering program to block incoming connections to port 135/TCP. Information about ICF is available in Microsoft Knowledge Base Article [283673](#).
6. Reconnect the system to the network and apply the patches referenced in [MS03-026](#).

Trend Micro, Inc. has [published](#) a set of steps to accomplish these goals. Symantec has also [published](#) a set of steps to accomplish these goals.

Disable DCOM

Depending on site requirements, you may wish to disable DCOM as described in [MS03-026](#). Disabling DCOM will help protect against this vulnerability but may also cause undesirable side effects. Additional details on disabling DCOM and possible side effects are available in Microsoft Knowledge Base Article [825750](#).

Filter network traffic

Sites are encouraged to block network access to the following relevant ports at network borders. This can minimize the potential of denial-of-service attacks originating from outside the perimeter. The specific services that should be blocked include

- 69/UDP
- 135/TCP
- 135/UDP
- 139/TCP
- 139/UDP
- 445/TCP
- 445/UDP
- 593/TCP
- 4444/TCP

Sites should consider blocking both inbound *and* outbound traffic to these ports, depending on network requirements, at the host and network level. Microsoft's [Internet Connection Firewall](#) can be used to accomplish these goals.

If access cannot be blocked for all external hosts, the CERT/CC recommends limiting access to only those hosts that require it for normal operation. As a general rule, the CERT/CC recommends filtering **all** types of network traffic that are not required for normal operation.

Because current exploits for [VU#568148](#) create a backdoor, which is in some cases 4444/TCP, blocking inbound TCP sessions to ports on which no legitimate services are provided may limit intruder access to compromised hosts.

Recovering from a system compromise

If you believe a system under your administrative control has been compromised, please follow the steps outlined in

[Steps for Recovering from a UNIX or NT System Compromise](#)

Reporting

The CERT/CC is tracking activity related to this worm as CERT#30479. Relevant artifacts or activity can be sent to cert@cert.org with the appropriate CERT# in the subject line.

Appendix A. Vendor Information

This appendix contains information provided by vendors. When vendors report new information, this section is updated and the changes are noted in the revision history. If a vendor is not listed below, we have not received their comments.

Microsoft

Please see Microsoft Security Bulletin [MS03-026](#).

Appendix B. References

- CERT/CC Advisory CA-2003-19 - <http://www.cert.org/advisories/CA-2003-19.html>
- CERT/CC Vulnerability Note VU#561284 - <http://www.kb.cert.org/vuls/id/561284>
- CERT/CC Vulnerability Note VU#326746 - <http://www.kb.cert.org/vuls/id/326746>
- Microsoft Security Bulletin MS03-026 - <http://microsoft.com/technet/security/bulletin/MS03-026.asp>
- Microsoft Knowledge Base article 823980 - <http://support.microsoft.com?kbid=823980>

Thanks

Our thanks to Microsoft Corporation for their review of and input to this advisory.

Authors: Chad Dougherty, Jeffrey Havrilla, Shawn Hernan, and Marty Lindner

Copyright 2003 Carnegie Mellon University.

Revision History

August 11, 2003: Initial release

August 12, 2003: Updated recovery steps

August 12, 2003: Added link to the W32/Blaster Tech Tip

August 13, 2003: Added filenames of known variants to removal instructions

August 14, 2003: Added port to filter (593/TCP)