Symantec.

Symantec Security Response

http://www.symantec.com/security_response/index.jsp

W32.Welchia.Worm

Risk Level 2: Low

Discovered:
August 18, 2003
Updated:
February 13, 2007 12:05:08 PM
Also Known As:
W32/Welchia.worm10240 [AhnLab], W32/Nachi.worm [McAfee], WORM_MSBLAST.D [Trend], Lovsan.D [F-Secure], W32/Nachi-A [Sophos], Win32.Nachi.A [CA], Worm.Win32.Welchia [Kaspersky]
Type:
Worm
Systems Affected:
Microsoft IIS, Windows 2000, Windows XP
CVE References:
CAN-2003-0109 CAN-2003-0352

SUMMARY

As of February 26, 2004, due to a decreased rate of submissions, Symantec Security Response has downgraded this threat to a Category 2 from a Category 3.

W32.Welchia.Worm is a worm that exploits multiple vulnerabilities, including:

- The DCOM RPC vulnerability (first described in Microsoft Security Bulletin MS03-026) using TCP port 135. The worm specifically targets Windows XP machines using this exploit. Users are recommended to patch this vulnerability by applying Microsoft Security Bulletin MS03-039.
- The WebDav vulnerability (described in Microsoft Security Bulletin MS03-007) using TCP port 80. The worm specifically targets machines running Microsoft IIS 5.0 using this exploit. As coded in this worm, this exploit will impact Windows 2000 systems and may impact Windows NT/XP systems.

W32.Welchia.Worm does the following:

- Attempts to download the DCOM RPC patch from Microsoft's Windows Update Web

site, install it, and then restart the computer
- Checks for active machines to infect by sending an ICMP echo request, or PING, which will result in increased ICMP traffic
- Attempts to remove W32.Blaster.Worm

Security Response has provided some information to aid network administrators in ongoing efforts to track down the machines that W32.Welchia.Worm has infected on their respective network. Read the document, "Detecting traffic due to RPC worms," for additional information.

Antivirus Protection Dates

- **Initial Rapid Release version** August 18, 2003
- **Latest Rapid Release version** July 20, 2011 revision 039
- **Initial Daily Certified version** August 18, 2003
- **Latest Daily Certified version** July 21, 2011 revision 003
- **Initial Weekly Certified release date** August 18, 2003

Click here for a more detailed description of Rapid Release and Daily Certified virus definitions.

Threat Assessment

Wild

- **Wild Level:** Low
- **Number of Infections:** More than 1000
- **Number of Sites:** More than 10
- **Geographical Distribution:** High
- **Threat Containment:** Moderate
- **Removal:** Moderate

Damage

- **Damage Level:** Medium

Distribution

- **Distribution Level:** Medium

TECHNICAL DETAILS

When W32.Welchia.Worm is executed, it performs the following actions:

1. Copies itself to:

%System%\Wins\Dllhost.exe

NOTE: %System% is a variable. The worm locates the System folder and copies itself to that location. By default, this is C:\Winnt\System32 (Windows 2000) or C:\Windows\System32 (Windows XP).

2. Makes a copy of %System%\Dllcache\Tftpd.exe as %System%\Wins\svchost.exe.

   NOTE: Tftpd is a legitimate program, which is not malicious, and therefore Symantec antivirus products do not detect it.

3. Adds the subkeys:

   `RpcPatch`

   and:

   `RpcTftpd`

   to the registry key:

   `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services`

4. Creates the following services:

   Service Name: RpcTftpd
   Service Display Name: Network Connections Sharing
   Service Binary: %System%\wins\svchost.exe

   This service will be set to start manually.

   Service Name: RpcPatch
   Service Display Name: WINS Client
   Service Binary: %System%\wins\dllhost.exe

   This service will be set to start automatically.

5. Ends the process, Msblast, and deletes the %System%\msblast.exe file, which W32.Blaster.Worm drops.

6. Selects the victim IP address in two different ways: The worm uses either A.B.0.0 from the infected machine's IP of A.B.C.D and counts up, or it will construct a random IP address based on some hard-coded addresses.

   After selecting the start address, the worm counts up through a range of Class B-sized networks; for example, if the worm starts at A.B.0.0, it will count up to at least A.B.255.255.

7. Sends an ICMP echo request, or PING, to check whether the constructed IP address is

an active machine on the network.

8. Once the worm identifies a machine as being active on the network, it will either send data to TCP port 135, which exploits the DCOM RPC vulnerability, or it will send data to TCP port 80 to exploit the WebDav vulnerability.

9. Creates a remote shell on the vulnerable host, which reconnects to the attacking computer on a random TCP port, between 666 and 765, to receive instructions.

Note: In the vast majority of the cases, the port is 707, because of the way the worm-threading model interacts with the implementation of the Windows C runtime .dll.

---

10. Launches the TFTP server on the attacking machine and instructs the victim machine to connect and download Dllhost.exe and Svchost.exe from the attacking machine. If the %System%\dllcache\tftpd.exe file exists, the worm may not download svchost.exe.

11. Checks the computer's operating system version, Service Pack number, and System Locale. It also attempts to connect to Microsoft's Windows Update and download the appropriate DCOM RPC vulnerability patch.

12. Once the update has been downloaded and executed, the worm restarts the computer so that the patch is installed.

13. Checks the computer's system date. If the year is 2004, the worm will disable and remove itself as follows:
    - Deletes the file %System%\Wins\Dllhost.exe
    - Deletes the services, RpcPatch and RpcTftpd, and removes the associated registry keys:

      ```
      HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\RpcPatch
      HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\RpcTftpd
      ```

    The worm does not delete the file, %System%\Wins\Svchost.exe, which is a nonmalicious tftp server.

Notes:
- The worm activates its removal routine only if the worm is started in the year 2004. If the worm has been running continuously since 2003, it will not remove itself after January 1, 2004 unless you manually restart the computer or worm.
- The W32.Welchia.Worm removal tool will still function normally in 2004.

Intruder Alert
On August 19, 2003, Symantec released Intruder Alert 3.6 W32_Welchia_Worm Policy.

Norton Internet Security/Norton Internet Security Professional

On August 20, 2003, Symantec released IDS signatures via LiveUpdate to detect W32.Welchia.Worm activity.

Symantec Client Security
On August 20, 2003, Symantec released IDS signatures via LiveUpdate to detect W32.Welchia.Worm activity.

Symantec ManHunt

- Symantec ManHunt Protocol Anomaly Detection technology detects the activity associated with this exploit as "Portsweep." Although ManHunt can detect activity associated with this exploit with the Protocol Anomaly Detection technology, you can use the "Microsoft DCOM RPC Buffer Overflow" custom signature, released in Security Update 4, to precisely identify the exploit being sent.
- Security Update 7 has been released to provide signatures specific to W32.Welchia.Worm to include the detection of more W32.Welchia.Worm attributes.

Symantec Gateway Security

- On August 18, 2003, Symantec released an update for Symantec Gateway Security 1.0.
- Symantec's full application inspection firewall technology protects against this Microsoft vulnerability, blocking all the above listed TCP ports by default. For maximum security, third-generation, full application inspection technology intelligently blocks the tunneling of DCOM traffic over HTTP channels; thus, providing an extra layer of protection not readily available on most common network filtering firewalls.

Symantec Host IDS
On August 19, 2003, Symantec released an update for Symantec Host IDS 4.1.

Recommendations

Symantec Security Response encourages all users and administrators to adhere to the following basic security "best practices":

- Use a firewall to block all incoming connections from the Internet to services that should not be publicly available. By default, you should deny all incoming connections and only allow services you explicitly want to offer to the outside world.
- Enforce a password policy. Complex passwords make it difficult to crack password files on compromised computers. This helps to prevent or limit damage when a computer is compromised.
- Ensure that programs and users of the computer use the lowest level of privileges necessary to complete a task. When prompted for a root or UAC password, ensure that the program asking for administration-level access is a legitimate application.
- Disable AutoPlay to prevent the automatic launching of executable files on network and removable drives, and disconnect the drives when not required. If write access is not required, enable read-only mode if the option is available.
- Turn off file sharing if not needed. If file sharing is required, use ACLs and password

protection to limit access. Disable anonymous access to shared folders. Grant access only to user accounts with strong passwords to folders that must be shared.

- Turn off and remove unnecessary services. By default, many operating systems install auxiliary services that are not critical. These services are avenues of attack. If they are removed, threats have less avenues of attack.
- If a threat exploits one or more network services, disable, or block access to, those services until a patch is applied.
- Always keep your patch levels up-to-date, especially on computers that host public services and are accessible through the firewall, such as HTTP, FTP, mail, and DNS services.
- Configure your email server to block or remove email that contains file attachments that are commonly used to spread threats, such as .vbs, .bat, .exe, .pif and .scr files.
- Isolate compromised computers quickly to prevent threats from spreading further. Perform a forensic analysis and restore the computers using trusted media.
- Train employees not to open attachments unless they are expecting them. Also, do not execute software that is downloaded from the Internet unless it has been scanned for viruses. Simply visiting a compromised Web site can cause infection if certain browser vulnerabilities are not patched.
- If Bluetooth is not required for mobile devices, it should be turned off. If you require its use, ensure that the device's visibility is set to "Hidden" so that it cannot be scanned by other Bluetooth devices. If device pairing must be used, ensure that all devices are set to "Unauthorized", requiring authorization for each connection request. Do not accept applications that are unsigned or sent from unknown sources.
- For further information on the terms used in this document, please refer to the Security Response glossary.

REMOVAL

Removal using the W32.Welchia.Worm Removal Tool
Symantec Security Response has developed a removal tool to clean the infections of W32.Welchia.Worm. This is the easiest way to remove this threat and should be tried first. To obtain the W32.Welchia.Worm removal tool, read the document, "W32.Welchia.Worm Removal Tool."

Manual Removal
As an alternative to using the removal tool, you can manually remove this threat. The following instructions pertain to all current and recent Symantec antivirus products, including the Symantec AntiVirus and Norton AntiVirus product lines.

1. Disable System Restore (Windows XP).
2. Update the virus definitions.
3. Restart the computer or stop the Worm.
4. Run a full system scan and delete all the files detected as W32.Welchia.Worm.
5. Delete the values from the registry.
6. Delete the Svchost.exe file.

For details on each of these steps, read the following instructions.

1. Disabling System Restore (Windows Me/XP)

If you are running Windows Me or Windows XP, we recommend that you temporarily turn off System Restore. Windows Me/XP uses this feature, which is enabled by default, to restore the files on your computer in case they become damaged. If a virus, worm, or Trojan infects a computer, System Restore may back up the virus, worm, or Trojan on the computer.

Windows prevents outside programs, including antivirus programs, from modifying System Restore. Therefore, antivirus programs or tools cannot remove threats in the System Restore folder. As a result, System Restore has the potential of restoring an infected file on your computer, even after you have cleaned the infected files from all the other locations.

Also, a virus scan may detect a threat in the System Restore folder even though you have removed the threat.

For instructions on how to turn off System Restore, read your Windows documentation, or one of the following articles:

- "How to disable or enable Windows Me System Restore"
- "How to turn off or turn on Windows XP System Restore"

For additional information, and an alternative to disabling Windows Me System Restore, see the Microsoft Knowledge Base article, "Antivirus Tools Cannot Clean Infected Files in the _Restore Folder," Article ID: Q263455.

2. Updating the virus definitions

Symantec Security Response fully tests all the virus definitions for quality assurance before they are posted to our servers. There are two ways to obtain the most recent virus definitions:

- Running LiveUpdate, which is the easiest way to obtain virus definitions: These virus definitions are posted to the LiveUpdate servers once each week (usually on Wednesdays), unless there is a major virus outbreak. To determine whether definitions for this threat are available by LiveUpdate, refer to the Virus Definitions (LiveUpdate).
- Downloading the definitions using the Intelligent Updater: The Intelligent Updater virus definitions are posted on U.S. business days (Monday through Friday). You should download the definitions from the Symantec Security Response Web site and manually install them. To determine whether definitions for this threat are available by the Intelligent Updater, refer to the Virus Definitions (Intelligent Updater).

  The Intelligent Updater virus definitions are available: Read "How to update virus definition files using the Intelligent Updater" for detailed instructions.

3. Restarting the computer in Safe mode or stopping the services of the worm

Windows 95/98/Me

Restart the computer in Safe mode. All the Windows 32-bit operating systems, except for Windows NT, can be restarted in Safe mode. For instructions, read the document, "How to start the computer in Safe Mode."

Windows NT/2000/XP

To stop the Worm services:

a. Open Services in the Administrative Tools located in the Control Panel.
b. Scroll through the list in the right pane and look for the following names:
   - Network Connections Sharing
   - WINS Client
c. If you find the services, right-click them, and then click Stop.
d. Exit the Services.

4. Scanning for and deleting the infected files

a. Start your Symantec antivirus program and make sure that it is configured to scan all the files.
   - For **Norton AntiVirus consumer products:** Read the document, "How to configure Norton AntiVirus to scan all files."
   - For **Symantec AntiVirus Enterprise products:** Read the document, "How to verify that a Symantec Corporate antivirus product is set to scan all files."
b. Run a full system scan
c. If any files are detected as infected with W32.Welchia.Worm, click Delete.

5. Deleting the values from the registry

WARNING: Symantec strongly recommends that you back up the registry before making any changes to it. Incorrect changes to the registry can result in permanent data loss or corrupted files. Modify the specified keys only. Read the document, "How to make a backup of the Windows registry," for instructions.

---

a. Click Start, and then click Run. (The Run dialog box appears.)
b. Type `regedit`

   Then click OK. (The Registry Editor opens.)

c. Navigate to the key:

   `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services`

d. Delete the subkeys:

   `RpcPatch`

   and:

   `RpcTftpd`

e. Exit the Registry Editor.

6. Deleting the Svchost.exe file
Navigate to the %System%\Wins folder and delete the Svchost.exe file.