The **CERT** for **France Industry, Services and Tertiary** sector

"Conficker" worm on Microsoft Windows systems

Reference :	CERT-IST/AV-2008.504
Version :	1.3
Version date :	02 February 2009

Vulnerability classification

Risk :	🟥 Very high
Impact :	Take control
Attack expertise :	Beginner
Attack requirements :	Remote (no account) over a standard service

System Information

Affected Platform(s) :

- Windows 2000 SP4
- Windows XP SP2 and SP3
- Windows XP Professional x64 Edition and Windows XP Professional x64 Edition SP2
- Windows Server 2003 SP1 and Windows Server 2003 SP2
- Windows Server 2003 SP1 (Itanium) and Windows Server 2003 SP2 (Itanium)
- Windows Server 2003 x64 Edition and Windows Server 2003 x64 Edition SP2
- Windows Vista and Windows Vista SP1
- Windows Vista X64 Edition and Windows Vista X64 Edition SP1
- Windows Server 2008 for 32-bit, 64-bit and Itanium systems

Affected Software :

- NA

Remarks :

- System patched with patches provided in the MS08-067 bulletin are protected against this worm.

Exhaustive list of affected products in the Cert-IST catalog :

Description

Problem description :

"Conficker" is a computer worm that spreads through local networks on infected systems, by exploiting the RPC vulnerability of the "Server" service **(MS08-067)**of Microsoft Windows systems, described in the**CERT-IST/AV-2008.460**advisory.

"Conficker" tries to open a backdoor on ifected systems.

Note: "Conficker" is also known as**"Confick", "Downadup"**or**"Downad".**

Technical information :

In addition to the overall behaviour already described, it should be noticed the following points:

- "Conficker" starts an HTTP server on a random port on infected systems in order to host a copy of the worm.
- "Conficker" scans the network to detect machines vulnerable to the**MS08-067**flaw. When it finds vulnerable systems, the remote machine connects to the HTTP server and downloads a copy of the worm.
- On Windows 2000 systems, "Conficker" injects a copy of its malicious code in the "services.exe" process.
- On other systems, "Conficker" creates a service called "netsvcs".
- "Conficker" tries to call an API function to reset the computer's system restore point, potentially defeating recovery using system restore.

Solution

Solution to the "Conficker" worm infection

Update your anti-virus software :

- Use the anti-virus automatic update feature.
- Or use the following instructions for a manual update.
- Computer Associates updates
  - http://www3.ca.com/support/vicdownload/
- F-Secure update - update date : 26/11/2008 or use the following updates
  - ftp://ftp.f-secure.com/anti-virus/updates/fsupdate.exe
  - http://f-secure.com/download-purchase/latest.zip
- NAI update - DAT file 5444 or later, to be released on 24/11/2008
  - http://download.nai.com/products/mcafee-avert/daily_dats/DAILYDAT.ZIP

  - http://download.nai.com/products/mcafee-avert/daily_dats/SDATDAILY.EXE
- Sophos Update - IDE file for that specific worm
  - http://www.sophos.com/downloads/ide/436_ides.zip
- Symantec update - Use "Intelligent Updater" (see URL below) or "LiveUpdate" updated26/11/2008
  - http://securityresponse.symantec.com/avcenter/defs.download.html
- TrendMicro update - Signature file 5.679.00 or later
  - http://www.trendmicro.com/ftp/products/pattern/lpt679.zip
  - http://www.trendmicro.com/ftp/products/pattern/lpt679.tar

CVSS score(s)

- Cert-IST - CERT-IST/AV-2008.504
  - Base score : 10.0 - AV:A/AC:L/Au:N/C:C/I:C/A:C
  - Temporal score : 7.4 - AV:A/AC:L/Au:N/C:C/I:C/A:C/E:U/RL:OF/RC:C

Standard vulnerability ID(s)

- CVE: CVE-2008-4250

Additional Resources

- F-Secure document regarding the "Conficker" worm
  - http://www.f-secure.com/v-descs/worm_w32_downadup_a.shtml
- NAI document regarding the "Conficker" worm
  - http://vil.nai.com/vil/content/v_153464.htm
- Sophos documents regarding the "Conficker" worm
  - http://www.sophos.com/security/analyses/viruses-and-spyware/w32conficka.html http://www.sophos.com/security/analyses/viruses-and-spyware/malconfickera.html
- Symantec document regarding the "Conficker" worm
  - http://www.symantec.com/business/security_response/writeup.jsp?docid=2008-112203-2408-99
- TrendMicro document regarding the "Conficker" worm
  - http://www.trendmicro.com/vinfo/virusencyclo/default5.asp?VName=WORM_DOWNAD.A&VSect=P
- Computer Associates document regarding the "Conficker" worm
  - http://www.ca.com/us/securityadvisor/virusinfo/virus.aspx?id=75911
- Panda document regarding the "Conficker" worm
  - http://www.pandasecurity.com/enterprise/security-info/about-malware/encyclopedia/overview.aspx?IdVirus=202881
- Microsoft security alert regarding the Conficker.B variant (KB962007)
  - http://support.microsoft.com/kb/962007

Version	Comment	Date
1.0	Advisory creation	27/11/2008
1.1	Precision regarding the sites contacted by the worm	28/11/2008
1.2	Second Sophos document regarding the "Conficker" worm	05/01/2009
1.3	Microsoft security alert regarding the Conficker.B worm variant	02/02/2009

Copyright © 1999-2014 Cert-IST