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

Alert detail

Spreading of the "Conficker" worm (MS08-067 vulnerability)

Reference :	CERT-IST/AL-2008.002
Version :	1.0
Version date :	27 November 2008

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

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

Description

Problem description :

We send this alert because we received confirmed reports of infection by the "Conficker" worm within our IST constituency. The "Conficker" worm is described in the**CERT-IST/AV-2008.504**advisory. This worm spreads by exploiting the RPC vulnerability of the "Server" service (MS08-067) of Microsoft Windows systems and enables to open a backdoor on infected systems.

It seems that some "Conficker" variants are not correctly detected by anti-virus (up to date). We recommend thus to block the URL used by the worm (see solution 02).

Systems that have applied the patches mentionned in the MS08-067 bulletin are not impacted.

Solution

01 - Apply the solutions described in the CERT-IST/AV-2008.460 advisory

The CERT-IST/AV-2008.460 advisory indicates the available patches to fix the MS08-067 vulnerability in Microsoft Windows. It also gives workarounds as well as tools and signatures available to detect attack attempts.

02 - Block the web sites contacted by "Conficker"

It seems that some anti-virus editors do not detect completely the "Conficker" worm (or its variants). A workaround is to filter the following sites on the Internet gateways :

[http://]trafficconverter.biz/4vir/antispyware/loada[removed]

[http://]www.maxmind.com/download/geoip/database/GeoIP.[removed]

"Conficker" also attempts to contact the following sites to obtain the IP address of the infected computer:
[http://]www.getmyip.org
[http://]/getmyip.co.uk
[http://]checkip.dyndns.org

The worm also attempts to contact the following sites to obtain the current date:
[http://]www.w3.org
[http://]www.ask.com
[http://]www.msn.com
[http://]www.yahoo.com
[http://]www.google.com
[http://]www.baidu.com

CVSS score(s)

- Cert-IST - CERT-IST/AL-2008.002
  - Base score : -
  - Temporal score : -

Standard vulnerability ID(s)

- CVE: CVE-2008-4250

Additional Resources

- Microsoft blog regarding the MS08-067 exploits
  - http://blogs.technet.com/mmpc/archive/2008/11/25/more-ms08-067-exploits.aspx
- SANS archive dated November 26, 2008
  - http://isc.sans.org/diary.html?storyid=5401
- Trend Micro blog regarding the MS08-067 exploits
  - http://blog.trendmicro.com/ms08-067-vulnerability-botnets-reloaded/

Version	Comment	Date
1.0	Alert creation	27/11/2008