


Potential Danger notice detail

New critical vulnerability in Microsoft Windows (MS08-067)

Reference : CERT-IST/DG-2008.009
Version : 1.0
Version date : 24 October 2008

Vulnerability classification

Risk :  Very high
Impact : Take control
Attack expertise : Skilled
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 :

- Windows "Server" service

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

Description

Publication context :

This potential DanGer follows the publication by Microsoft of the out-of-band security bulletin MS08-067 regarding a critical vulnerability in Microsoft Windows. The vulnerability described in this security bulletin is detailed in the CERT-IST/AV-2008.460 advisory.

Problem description :

We release this potential DanGer regarding the vulnerability in the "Server" service in Microsoft Windows because there is a significant probability to see public functional exploits for this flaw appearing on the Internet. Moreover, Microsoft reports that such an exploit could easily be "wormable" - a malicious code such as a worm or a virus exploiting the vulnerability could spread rather quickly and automatically.

We are especially encouraging the community to patch systems for several reasons:

- the vulnerability can be exploited remotely,
- a successful attack does not require the attacker to be authenticated on Windows 2000, XP and 2003,
- the possibility to have a worm spreading on the Internet has to be seriously considered.

Consequently the Cert-IST recommends:

- to apply Microsoft's patches as soon as possible,
- to set the workarounds discussed in the second solution to protect vulnerable systems while waiting for the patches to be applied,
- finally, to use the signatures provided within the third solution in order to be able to detect attack attempts.

Solution

01 - Apply the Microsoft patches (KB958644) regarding the Windows "Server" service vulnerability

Patches are available for the various impacted platforms.

See the Microsoft security bulletin MS08-067 to get the appropriate patch.

The patches described in this Microsoft security bulletin replace the ones described in the MS06-040 bulletin (see the CERT-IST/AV-2006.315 advisory).

- Microsoft security bulletin MS08-067
 - <http://www.microsoft.com/technet/security/Bulletin/MS08-067.msp>

02 - Recommendations to mitigate the "Server" service vulnerability

- Filter the TCP ports 139 and 445 on network devices located in the LAN boundary and/or near the vulnerable Microsoft Windows systems.
- Keep the anti-virus software updated.

Note : A workaround could be to disable the "Server" service on vulnerable systems. However, this solution leads to some significant side-effects. For example:

- you will be unable to share local resources (folders or printers),
- you will be unable to be remotely managed by classical Microsoft tools.

03 - Tools and signatures to detect the flaw and its exploitation

The following signatures enable to detect exploitations of this vulnerability (not exhaustive list).

- Snort rules to detect attacks targeting the vulnerability (MS08-067)
 - <http://www.snort.org/vrt/advisories/vrt-rules-2008-10-23.html>
- CA signature 31.6.6167
 - <http://www3.ca.com/support/vicdownload/>
- Symantec Initial Rapid Release version October 23, 2008 revision 040
 - http://www.symantec.com/business/security_response/definitions/download/index.jsp
- NAI update - DAT file 5414 or later, to be released on 10/24/08
 - <http://www.mcafee.com/us/enterprise/downloads/index.html>
- Nessus plugin #34476 allowing the detection of vulnerable systems
 - <http://www.nessus.org/plugins/index.php?view=single&id=34476>

CVSS score(s)

- Cert-IST - CERT-IST/DG-2008.009
 - Base score : -
 - Temporal score : -

Standard vulnerability ID(s)

- CVE: [CVE-2008-4250](#)
- Microsoft: [KB958644](#)
- CERT/CC: [VU#827267](#)

Additional Resources

- Microsoft security advisory MS08-067 dated October 23, 2008
 - <http://www.microsoft.com/technet/security/Bulletin/MS08-067.msp>
- Post in the Microsoft SWI blog dated October 23, 2008
 - <http://blogs.technet.com/swi/archive/2008/10/23/More-detail-about-MS08-067.aspx>
- US-CERT security advisory TA08-297A dated October 23, 2008
 - <http://www.us-cert.gov/cas/techalerts/TA08-297A.html>
- Symantec generic detection "Bloodhound.Exploit.212"
 - http://www.symantec.com/business/security_response/writeup.jsp?docid=2008-102323-4508-99&tabid=1
- F-Secure document regarding the "Gimmiv" Trojan
 - http://www.f-secure.com/v-descs/trojan-spy_w32_gimmiv_a.shtml
- CA document regarding the "Gimmiv" Trojan
 - <http://www.ca.com/us/securityadvisor/virusinfo/virus.aspx?id=74579>
- Sophos document regarding the "Gimmiv" Trojan
 - <http://www.sophos.com/security/analyses/viruses-and-spyware/trojgimmiva.html>
- NAI document regarding the "Spy-Agent.da" Trojan
 - http://vil.nai.com/vil/content/v_152898.htm

Version	Comment	Date
1.0	Potential danger creation	24/10/2008