

[NT] Korean Input Method Editor Privileges Elevation (MS06-009)

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2006-02/msg00053.html>

- *From:* SecuriTeam <support@xxxxxxxxxxxxxx>
 - *Date:* 15 Feb 2006 11:30:11 +0200
-

The following security advisory is sent to the securiteam mailing list, and can be found at the SecuriTeam web site: <http://www.securiteam.com>
-- promotion

The SecuriTeam alerts list – Free, Accurate, Independent.

Get your security news from a reliable source.
<http://www.securiteam.com/maillinglist.html>

Korean Input Method Editor Privileges Elevation (MS06-009)

SUMMARY

A <<http://go.microsoft.com/fwlink/?LinkId=21142>> privilege elevation vulnerability exists in the Windows and Office Korean Input Method Editor (IME). This vulnerability could allow a malicious user to take complete control of an affected system.

For an attack to be successful an attacker must be able to interactively logon to the affected system.

DETAILS

Vulnerable Systems:

* Microsoft Windows XP Service Pack 1 and Microsoft Windows XP Service Pack 2

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=290453DF-1CAE-4691-B20C-5D65D92216BF>>

Download the update

* Microsoft Windows XP Professional x64 Edition

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=7D75BF5C-2E1D-4793-B7D1-DD372A99ECA5>>

Download the update

* Microsoft Windows Server 2003 and Microsoft Windows Server 2003 Service Pack 1

[NT] Korean Input Method Editor Privileges Elevation (MS06-009)

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=A092BA0F-C753-444B-A572-492E4ECB2D3F>>

Download the update

* Microsoft Windows Server 2003 for Itanium-based Systems and Microsoft

Windows Server 2003 with SP1 for Itanium-based Systems

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=8479C2EB-0FB6-4879-9C3D-B49BD864A71C>>

Download the update

* Microsoft Windows Server 2003 x64 Edition

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=66E495E8-CD52-4E76-B20A-4471FA941556>>

Download the update

* Microsoft Office 2003 Software:

* Microsoft Office 2003 Service Pack 1 and Service Pack 2 –

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=8E6F16E9-CD73-47D5-887E-616DB9B09591&disp>>

Download the update (KB905645)

* Microsoft Office 2003 Multilingual User Interface Packs

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=986F9A8D-AFE7-455A-B78D-0795CBB0E80E&disp>>

Download the update (KB905645)

* Microsoft Office Visio 2003 Multilingual User Interface Packs

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=5A4D0A92-2DFC-4F8B-9D14-138CEA57AF96&disp>>

Download the update (KB909115)

* Microsoft Office Project 2003 Multilingual User Interface Packs

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=22C96D7F-F384-4678-9AC0-3A11B81A4C1D&disp>>

Download the update (KB909118)

* Microsoft Office 2003 Proofing Tools

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=32CF9F59-FFBD-45E5-A4D2-690183462D0F&disp>>

Download the update (KB905645)

* Microsoft Office Visio 2003 –

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=8E6F16E9-CD73-47D5-887E-616DB9B09591&disp>>

Download the update (KB905645)

* Microsoft Office OneNote 2003 –

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=8E6F16E9-CD73-47D5-887E-616DB9B09591&disp>>

Download the update (KB905645)

* Microsoft Office Project 2003 –

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=8E6F16E9-CD73-47D5-887E-616DB9B09591&disp>>

Download the update (KB905645)

Note The security updates for Microsoft Windows Server 2003, Microsoft Windows Server 2003 Service Pack 1, and Microsoft Windows Server 2003 x64 Edition also apply to Microsoft Windows Server 2003 R2.

Note Only the Korean language versions of Windows are by default affected by this vulnerability. Customers running East Asian language versions of Windows have the affected component present on the system, but are only vulnerable if the Korean language IME is enabled. Customers running any other language version of Windows only need to take action if they have installed and enabled the Korean language IME.

Note Only the Korean language versions of the listed Office 2003 products are affected, with the exception of Office 2003 Proofing Tools. Customers who have installed the Microsoft Office 2003 Proofing Tools product will need to install this security update even if they did not specifically install the Korean Proofing Tools component. When this security bulletin

[NT] Korean Input Method Editor Privileges Elevation (MS06-009)

was issued, the most recent update for non-Korean versions of Microsoft Office 2003 Multilingual User Interface Pack was Microsoft Security Bulletin <<http://go.microsoft.com/fwlink/?LinkId=44168>> MS06-003.

Immune Systems:

- * Microsoft Windows 2000 Service Pack 4
- * Microsoft Windows 98, Microsoft Windows 98 Second Edition (SE), and Microsoft Windows Millennium Edition (ME)
- * Microsoft Office XP Service Pack 3
- * Microsoft Office 2000 Service Pack 3

Mitigating Factors for Korean IME Vulnerability –

<<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2006-0008>>
CVE-2006-0008:

- * To exploit this vulnerability an attacker must have access to the system to perform an interactive logon, either locally or via a Remote Desktop Protocol (RDP) session.

- * Firewall best practices and standard default firewall configurations can help protect networks from attacks that originate outside the enterprise perimeter. Best practices recommend that systems that are connected to the Internet have a minimal number of ports exposed.

- * By default, RDP is not enabled on any operating system version. On Windows XP and Windows Server 2003, Remote Assistance can enable RDP. On Windows XP Media Center Edition, RDP is enabled if a Media Center Extender has been installed. For information about Media Center Extenders, visit the following Web site.

- On Small Business Server 2000 and on Windows Small Business Server 2003, RDP is enabled by default. However, by default, on Windows Small Business Server 2003 and earlier versions, the RDP Protocol communication ports are blocked from the Internet. RDP is available only on the local network unless Terminal Services or the Remote Web Workplace features have been enabled by using the Configure E-mail and Internet Connection Wizard (CEICW).

- * If Remote Desktop is manually enabled, the following Windows Firewall changes will occur, depending on the operating system version:
 - * On Windows XP Service Pack 2 systems that have Windows Firewall enabled, enabling the Remote Desktop feature will automatically enable the Remote Desktop exception in the firewall, with the scope of All computers (including those on the Internet). When you disable Remote Desktop, this firewall exception is automatically disabled.

 - * On Windows XP Service Pack 1, Windows Server 2003, and Windows Server 2003 Service Pack 1, enabling the Remote Desktop Feature does not enable the Remote Desktop exception in the firewall. Enabling Remote Desktop causes a dialog box to appear that indicates that you must manually enable this exception. There is a Remote Desktop entry in the exception in the

[NT] Korean Input Method Editor Privileges Elevation (MS06-009)

list of the firewall exceptions that a user would have to manually enable. Disabling Remote Desktop does not change the exception status in the firewall. However, although the system is no longer vulnerable to this issue through Remote Desktop, it could still be vulnerable through Remote Assistance and Terminal Services, where available.

Workarounds for Korean IME Vulnerability –

<<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2006-0008>>
CVE-2006-0008:

Microsoft has tested the following workarounds. While these workarounds will not correct the underlying vulnerability, they help block known remote attack vectors. When a workaround reduces functionality, it is identified in the following section.

Disable Terminal Services, Remote Desktop, Remote Assistance, and Windows Small Business Server 2003 Remote Web Workplace if they are no longer required.

* If you no longer need these services on your system, consider disabling them as a security best practice. Disabling unused and unneeded services helps reduce your exposure to security vulnerabilities.

* For information about how to disable Remote Desktop manually, visit the following

<http://www.microsoft.com/resources/documentation/windows/xp/all/proddocs/en-us/rdesktop_disable.mspx>
Web site.

* For information about how to disable Remote Desktop by using Group Policy, see the following <<http://support.microsoft.com/kb/306300>>
Microsoft Knowledge Base Article.

* For information about Remote Assistance, including instructions on how to disable Remote Assistance manually and by using Group Policy, visit the following

<http://www.microsoft.com/technet/prodtechnol/winxppro/maintain/intmgmt/20_xprem.mspx> Web site.

* For information about how to disable the Windows Small Business Server 2003 Terminal Services and Remote Web Workplace features, visit the following

<http://www.microsoft.com/technet/security/secnews/articles/sec_sbs2003_network.mspx#EIAA> Web site.

Block TCP port 3389 at the enterprise perimeter firewall.

This port is used to initiate a connection with the affected component. Blocking it at the network perimeter firewall will help protect systems that are behind that firewall from attempts to exploit this vulnerability. This can help protect networks from attacks that originate outside the enterprise perimeter. Blocking the affected ports at the enterprise perimeter is the best defense to help avoid Internet-based attacks. However, systems could still be vulnerable to attacks from within their enterprise perimeter. Additionally, on Windows XP and Windows Server 2003, Windows Firewall can help protect individual systems. By default, Windows Firewall does not allow connections to this port, except in Windows XP Service Pack 2 when the Remote Desktop feature is enabled. For information about how to disable the Windows Firewall exception for Remote Desktop on

[NT] Korean Input Method Editor Privileges Elevation (MS06-009)

these platforms, visit the following

<http://www.microsoft.com/technet/prodtechnol/windowsserver2003/library/ServerHelp/8b5e3b52-b77b-4d98-a058->

Web site. If you cannot disable the Windows Firewall exception for Remote Desktop, you may be able to reduce the scope of this vulnerability by setting the default value of All computers (Including those on the Internet), to the local network. Doing this helps reduce the likelihood of attacks from the Internet.

Note Windows Small Business Server 2003 uses a feature named Remote Web Workplace. This feature uses TCP port 4125 to listen for RDP connections.

If you are using this feature, you should validate that this port is also blocked from the Internet in addition to port 3389.

Note It is possible to manually change the affected components to use other ports. If you have performed these actions, you should also block those additional ports.

Help secure Remote Desktop connections by using an IPsec policy.

Specific configurations would be dependent upon the individual environment. For information about Internet Protocol Security (IPsec), visit the following

<http://www.microsoft.com/windowsserver2003/technologies/networking/ipsec/default.msp>> Web site.

Detailed information about IPsec and about how to apply filters is available in

<http://support.microsoft.com/kb/313190>> Microsoft Knowledge Base Article 313190 and

<http://support.microsoft.com/kb/813878>> Microsoft Knowledge Base Article 813878.

Help secure Remote Desktop connections by using a virtual private network (VPN) connection.

Specific configurations depend on the individual environment. For information about Virtual Private Networks, visit the following

<http://www.microsoft.com/technet/prodtechnol/windowsserver2003/library/ServerHelp/a08da8ea-a616-4422-bbd7->

Web site.

FAQ for Korean IME Vulnerability –

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2006-0008>>

CVE-2006-0008:

What is the scope of the vulnerability?

This is a <http://go.microsoft.com/fwlink/?LinkId=21142>> privilege elevation vulnerability. An attacker who successfully exploited this vulnerability could take complete control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

What causes the vulnerability?

Under certain conditions, the Input Method Editor (IME) for the Korean language inappropriately exposes functionality that runs in the LocalSystem context.

What is the Korean IME?

IMEs help solve a problem associated with entering information in certain languages via a keyboard. Languages like Korean contain thousands of

different characters, and it isn't feasible to build a keyboard that includes all of them. IMEs allow the characters to be built using a standard 101-key keyboard, by specifying the strokes that compose each character.

An IME consists of an engine that converts keystrokes into phonetic and ideographic characters and a dictionary of commonly-used ideographic words. As the user enters keystrokes via the keyboard, the IME identifies the keystrokes and converts them into characters.

Which IMEs are affected by this vulnerability?

Only the Korean language IME is affected. All other languages' IMEs correctly identify when they're running as part of the logon screen and only expose the appropriate functions.

Why Is Office 2003 also affected by the Korean IME vulnerability?

Office 2003 as part of its multilingual capabilities can install its own Korean IME which overwrites the version of the Korean IME provided by the operating system. It is highly recommended that customers who have installed the Office 2003 Korean IME apply the Office security update in this security bulletin at the earliest opportunity.

What might an attacker use the vulnerability to do?

An attacker who successfully exploited this vulnerability could take complete control of the affected system.

Who could exploit the vulnerability?

Users who can access an affected system's logon screen, either locally or remotely.

How could an attacker exploit the vulnerability?

A malicious user who could access the logon screen either locally or via Remote Desktop or Terminal Services on an affected system and could use this functionality to run code to take any desired action on the system.

What systems are primarily at risk from the vulnerability?

Workstations and terminal servers that have the Korean language IME installed are primarily at risk.

Are Windows 98, Windows 98 Second Edition, or Windows Millennium Edition critically affected by this vulnerability?

No. Windows 98, Windows 98 Second Edition, and Windows Millennium Edition do not contain the affected component.

Could the vulnerability be exploited over the Internet?

Yes. An attacker could try to exploit this vulnerability over the Internet. Firewall best practices and standard default firewall configurations can help protect against attacks that originate from the Internet. Microsoft has provided information about how you can help protect your PC. End users can visit the <http://go.microsoft.com/fwlink/?LinkId=21169> Protect Your PC Web site. <http://go.microsoft.com/fwlink/?LinkId=21171> IT professionals can visit

[NT] Korean Input Method Editor Privileges Elevation (MS06-009)

the TechNet Security Center Web site.

What does the update do?

The update removes the vulnerability by disabling the affected Korean IME functionality that runs in the LocalSystem context.

When this security bulletin was issued, had this vulnerability been publicly disclosed?

No. Microsoft received information about this vulnerability through responsible disclosure. Microsoft had not received any information to indicate that this vulnerability had been publicly disclosed when this security bulletin was originally issued.

When this security bulletin was issued, had Microsoft received any reports that this vulnerability was being exploited?

No. Microsoft had not received any information to indicate that this vulnerability had been publicly used to attack customers.

ADDITIONAL INFORMATION

The information has been provided by Microsoft Security.

The original article can be found at:

<<http://www.microsoft.com/technet/security/Bulletin/MS06-009.msp>>

<http://www.microsoft.com/technet/security/Bulletin/MS06-009.msp>

=====

This bulletin is sent to members of the SecuriTeam mailing list.

To unsubscribe from the list, send mail with an empty subject line and body to:

list-unsubscribe@xxxxxxxxxxxxxx

In order to subscribe to the mailing list, simply forward this email to: list-subscribe@xxxxxxxxxxxxxx

=====

=====

DISCLAIMER:

The information in this bulletin is provided "AS IS" without warranty of any kind.

In no event shall we be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages.