

# [NT] ShellAbout() API Elevation of Privilege (MS06-009)

---

*Source:* <http://www.derkeiler.com/Mailing-Lists/Securiteam/2006-02/msg00057.html>

---

- *From:* SecuriTeam <[support@xxxxxxxxxxxxxx](mailto:support@xxxxxxxxxxxxxx)>
  - *Date:* 16 Feb 2006 13:24:14 +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>

-----

ShellAbout() API Elevation of Privilege (MS06-009)

---

## SUMMARY

"

<<http://msdn.microsoft.com/library/default.asp?url=/library/en-us/shellcc/platform/shell/reference/functions/shellabout>>  
ShellAbout Function Displays a ShellAbout dialog box."

A vulnerability in the Korean ShellAbout() API allows attackers to gain elevated privileges.

## DETAILS

### Vulnerable Systems:

- \* Microsoft Windows XP Service Pack 1 and Microsoft Windows XP Service Pack 2
- \* Microsoft Windows XP Professional x64 Edition
- \* Microsoft Windows Server 2003 and Microsoft Windows Server 2003 Service Pack 1
- \* Microsoft Windows Server 2003 for Itanium-based Systems and Microsoft Windows Server 2003 with SP1 for Itanium-based Systems
- \* Microsoft Windows Server 2003 x64 Edition
- \* Microsoft Office 2003 Software:

## [NT] ShellAbout() API Elevation of Privilege (MS06-009)

- \* Microsoft Office 2003 Service Pack 1 and Service Pack 2
- \* Microsoft Office 2003 Multilingual User Interface Packs
- \* Microsoft Office Visio 2003 Multilingual User Interface Packs
- \* Microsoft Office Project 2003 Multilingual User Interface Packs
- \* Microsoft Office 2003 Proofing Tools
- \* Microsoft Office Visio 2003
- \* Microsoft Office OneNote 2003
- \* Microsoft Office Project 2003

ShellAbout() API displays 'shell about dialog box'. If attackers clicks on 'End-User License Agreement' link in about box, the program will execute notepad.exe and display 'EULA'. If the program which displays about box is running as LocalSystem account, it will execute notepad.exe as LocalSystem account too. In result, attacker can gain LocalSystem authority taking advantage of the notepad.exe process.

To test this vulnerability, it is possible to use a shell about dialog box of korean IME language bar attached to winlogon.exe process. Because winlogon.exe process was running as LocalSystem account, it is possible to control the notepad.exe process to have a LocalSystem authority.

Above-mentioned, we used winlogon.exe process to test the vulnerability. Winlogon.exe process handles many things about user session. The main job is transacting logon process with user name and password. In case of windows korean edition, korean IME is attached to the user name edit control. If attackers click on the right-button in the korean IME language bar and select about box item in context menu, the 'shell about dialog box' will be displayed. And if attackers click on the 'End-User License Agreement' link, notepad.exe process will be created as LocalSystem. If attackers are connected to local session, winlogon.exe process displays the notepad.exe in 'Service-0x0-3e7\$\Default' desktop which is for window services and if they are connected to a remote session, it will displays notepad.exe in 'WinSta0\Default' desktop of the current user. Of course there are some cases that notepad.exe process is displayed in 'WinSta0\Default' desktop even if it is local session, but it will only be considered remote session case as a matter of convenience.

So if users uses Windows XP they might have an activate 'remote desktop' and, if they using Windows Server 2003 they might install 'terminal service'.

Proof of Concept:

Using remote desktop:

1. Select 'about Korean IME' context menu item:

After connecting to terminal service, press right-click on Korean IME language bar which is attached to the user name edit control in 'Windows Logon' dialog box, And select the 'about Korean IME' context menu item which displays 'shell about dialog box'.

2. Click on 'End-User License Agreement' link

## [NT] ShellAbout() API Elevation of Privilege (MS06-009)

If you click on 'End-User License Agreement' link, notepad.exe will be executed.

Winlogon.exe process creates notepad.exe as 'LocalSystem' account. But notepad.exe does not display because of the current desktop 'WinSta0\Winlogon' while notepad's desktop is 'WinSta0\Default'.

### 3. Login as non-privileged user 'test'

If you login as common user 'test' who has no administrative authority, you can see the notepad.exe process in 'WinSta0\Default' desktop.

This notepad.exe process is created by winlogon.exe process as 'LocalSystem' account, and user 'test' can do everything with 'LocalSystem' authority. For example, user 'test' can modify system files to his or her own thing with 'Save As' common control.

### 4. Advanced topic: Hack without logon id or password.

Until now, we saw how to gain 'LocalSystem' privilege for non-privileged user 'test'.

There are also other ways to gain 'LocalSystem' privilege without logon id or password:

After step 2, click on 'cancel' button on login screen. You don't have to write login id or password.

Just before the disconnection, 'notepad.exe' is displayed, the user is split for a second.

At this point, if you can do a mouse click on notepad, you can gain 'LocalSystem' privilege of all 3389 port opened in Windows 2003 Server Korean Edition, just by using mouse clicking.

## ADDITIONAL INFORMATION

The information has been provided by <<mailto:ryan.lee@xxxxxxxxxxxxx>> Ryan Lee.

The original article can be found at:

<[http://www.ryanstyle.com/alert/my/5/ms06\\_009\\_eng.html](http://www.ryanstyle.com/alert/my/5/ms06_009_eng.html)>

[http://www.ryanstyle.com/alert/my/5/ms06\\_009\\_eng.html](http://www.ryanstyle.com/alert/my/5/ms06_009_eng.html)

The original advisory can be found at:

<<http://www.securiteam.com/windowsntfocus/5ZP0C1FHPU.html>>

<http://www.securiteam.com/windowsntfocus/5ZP0C1FHPU.html>

=====

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:

[NT] ShellAbout() API Elevation of Privilege (MS06-009)

list-unsubscribe@xxxxxxxxxxxxxxxx

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

=====  
=====

**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.