

[NT] Vulnerability in Windows Could Allow Elevation of Privilege (MS06-075)

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2006-12/msg00014.html>

- *From:* SecuriTeam <support@xxxxxxxxxxxxxx>
 - *Date:* 13 Dec 2006 19:43:11 +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>

Vulnerability in Windows Could Allow Elevation of Privilege (MS06-075)

SUMMARY

A privilege elevation vulnerability exists in the way that Microsoft Windows starts applications with specially crafted file manifests. This vulnerability could allow a logged on user to take complete control of the system.

DETAILS

Affected Software:

* Microsoft Windows XP Service Pack 2 –

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=966704b5-1a7e-4110-9694-844706a52db7>>

Download the update

* Microsoft Windows Server 2003 –

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=5ea314a2-d76a-46f9-853b-15ff03f8ad95>>

Download the update

* Microsoft Windows Server 2003 for Itanium-based Systems –

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=7bceaa11-f655-4e3c-a588-5c49097e970b>>

Download the update

Non-Affected Software:

[NT] Vulnerability in Windows Could Allow Elevation of Privilege (MS06-075)

- * Microsoft Windows 2000 Service Pack 4
- * Microsoft Windows XP Professional x64 Edition
- * Microsoft Windows Server 2003 Service Pack 1
- * Microsoft Windows Server 2003 with Service Pack 1 for Itanium-based Systems
- * Microsoft Windows Server 2003 x64 Edition
- * Windows Vista

Mitigating Factors for File Manifest Corruption Vulnerability – CVE-2006-5585:

An attacker must have valid logon credentials and be able to log on locally to exploit this vulnerability. The vulnerability could not be exploited remotely or by anonymous users.

Workarounds for File Manifest Corruption Vulnerability – CVE-2006-5585:

No workarounds have been identified for this vulnerability.

FAQ for File Manifest Corruption Vulnerability – CVE-2006-5585:

What is the scope of the vulnerability?

This is a 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. To attempt to exploit the vulnerability, an attacker must be able to log on locally to the system and run a program.

What causes the vulnerability?

Improper processing and management of file manifests by the Client-Server Run-time Subsystem.

What is the Client Server Run-Time Subsystem?

Csrss is the user-mode portion of the Win32 subsystem (with Win32.sys being the kernel-mode portion). Csrss stands for client/server run-time subsystem and is an essential subsystem that must be running at all times. Csrss is responsible for console windows, creating and/or deleting threads.

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?

To try to exploit the vulnerability, an attacker must be able to log on locally to a system and run a program

How could an attacker exploit the vulnerability?

To exploit this vulnerability, an attacker would first have to log on to the system. An attacker could then run a specially crafted application that could exploit the vulnerability and gain complete control over the affected system.

[NT] Vulnerability in Windows Could Allow Elevation of Privilege (MS06-075)

What systems are primarily at risk from the vulnerability?

Workstations and terminal servers are primarily at risk. Servers could be at more risk if administrators allow users to log on to servers and to run programs. However, best practices strongly discourage allowing this.

Could the vulnerability be exploited over the Internet?

No. An attacker must be able to log on to the specific system that is targeted for attack. An attacker cannot load and run a program remotely by using this vulnerability.

What does the update do?

The update removes the vulnerability by modifying the way that Client Server Run-time Subsystem validates embedded file manifests before it passes data to the allocated buffer.

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

No this issue has not been previously publicly disclosed as a vulnerability.

How does this vulnerability relate to Microsoft Knowledge Base Article 921337?

<<http://support.microsoft.com/kb/921337/en-us>> Microsoft Knowledge Base Article 921337 discusses a related issue with file manifest that could potentially cause a system to reboot. In reviewing this issue Microsoft identified a potential security vulnerability that is addressed by the release of this security update.

ADDITIONAL INFORMATION

The original article can be found at:

<<http://www.microsoft.com/technet/security/Bulletin/MS06-075.msp>>
<http://www.microsoft.com/technet/security/Bulletin/MS06-075.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@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.

[NT] Vulnerability in Windows Could Allow Elevation of Privilege (MS06-075)

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