

[NT] Vulnerability in Windows Kernel Allows Elevation of Privilege (MS05-055)

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2005-12/msg00042.html>

- *From:* SecuriTeam <support@xxxxxxxxxxxxxx>
 - *Date:* 14 Dec 2005 18:46:44 +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 Kernel Allows Elevation of Privilege (MS05-055)

SUMMARY

A privilege elevation vulnerability exists in the way that asynchronous procedure calls are processed within the kernel.

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.

DETAILS

Vulnerable Systems:

- * Microsoft Windows 2000 Service Pack 4 (
<<http://www.microsoft.com/downloads/details.aspx?FamilyId=3832FF23-6B04-4CA2-80B9-D344B4CC98EA>>
Download the update)

Immune Systems:

- * Microsoft Windows XP Service Pack 1 and Microsoft Windows XP Service Pack 2
- * Microsoft Windows XP Professional x64 Edition

[NT] Vulnerability in Windows Kernel Allows Elevation of Privilege (MS05–055)

- * 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 Windows 98, Microsoft Windows 98 Second Edition (SE), and Microsoft Windows Millennium Edition (ME)

Windows Kernel Vulnerability:

A privilege elevation vulnerability exists in the way that asynchronous procedure calls are processed within the kernel. This vulnerability could allow a logged on user to take complete control of the system.

Mitigating Factors:

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:

Microsoft have not identified any workarounds for this vulnerability.

FAQ:

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. 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?

The method used to process items in the asynchronous procedure call (APC) queue list.

What is an asynchronous procedure call (APC)?

An asynchronous procedure call (APC) is a function that executes asynchronously in the context of a particular thread. For more information, please visit the following

<http://msdn.microsoft.com/library/default.asp?url=/library/en-us/dllproc/base/asynchronous_procedure_calls.asp> Microsoft web site.

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. 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

[NT] Vulnerability in Windows Kernel Allows Elevation of Privilege (MS05-055)

and gain complete control over the affected system.

What systems are primarily at risk from the vulnerability?

Workstations and terminal servers are primarily at risk. Servers could be at more risk if users who do not have sufficient administrative permissions are given the ability 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 addresses the vulnerability by modifying the way that Asynchronous Procedure Calls (APC) queues are processed.

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 and had not seen any examples of proof of concept code published when this security bulletin was originally issued.

CVE Information:

<<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-2827>>
CAN-2005-2827

ADDITIONAL INFORMATION

The original article can be found at:

<<http://www.microsoft.com/technet/security/bulletin/MS05-055.msp>>
<http://www.microsoft.com/technet/security/bulletin/MS05-055.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.

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

-
- Prev by Date: [*\[NT\] Cumulative Security Update for Internet Explorer \(MS05-054\)*](#)
 - Next by Date: [*\[NT\] Windows Kernel APC Data-Free Local Privilege Escalation \(MS05-055\)*](#)
 - Previous by thread: [*\[NT\] Cumulative Security Update for Internet Explorer \(MS05-054\)*](#)
 - Next by thread: [*\[NT\] Windows Kernel APC Data-Free Local Privilege Escalation \(MS05-055\)*](#)
 - Index(es):
 - ◆ [*Date*](#)
 - ◆ [*Thread*](#)