

[NT] Vulnerability in Plug and Play Allows Remote Code Execution and Elevation of Privilege (MS05-039)

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2005-08/0041.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 08/10/05

To: list@securiteam.com

Date: 10 Aug 2005 14:53:49 +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 Plug and Play Allows Remote Code Execution and Elevation of Privilege (MS05-039)

SUMMARY

A remote code execution vulnerability exists in Plug and Play (PnP) that allows an attacker who successfully exploited this vulnerability to take complete control of the affected system.

DETAILS

Vulnerable Systems:

* Microsoft Windows 2000 Service Pack 4

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=E39A3D96-1C37-47D2-82EF-0AC89905C88F>>

Download the update

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

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=9A3BFBDD-62EA-4DB2-88D2-415E095E207F>>

Download the update

* Microsoft Windows XP Professional x64 Edition

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=89D90E25-4773-4782-AD06-9B7517BAB3C8>>

Download the update

[NT] Vulnerability in Plug and Play Allows Remote Code Execution and Elevation of Privilege (MS05-039)

Securiteam: [NT] Vulnerability in Plug and Play Allows Remote Code Execution and Elevation of Privilege (MS05-039)

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

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=6275D7B7-DAB1-47C8-8745-533EB471072C>>

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=BE18D39D-3E4C-4C6F-B841-2CCD8D4C3F50>>

Download the update

* Microsoft Windows Server 2003 x64 Edition

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=D976316D-3B17-4AD4-9198-513FFDAC98E4>>

Download the update

Immune Systems:

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

Plug and Play Vulnerability – CAN-2005-1983:

A remote code execution and local elevation of privilege vulnerability exists in Plug and Play that could allow an attacker who successfully exploited this vulnerability to take complete control of the affected system.

Mitigating Factors for Plug and Play Vulnerability – CAN-2005-1983:

On Windows XP Service Pack 2 and Windows Server 2003 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 by anonymous users or by users who have standard user accounts. However, the affected component is available remotely to users who have administrative permissions.

On Windows XP Service Pack 1 an attacker must have valid logon credentials to try to exploit this vulnerability. The vulnerability could not be exploited remotely by anonymous users. However, the affected component is available remotely to users who have standard user accounts.

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.

Workarounds for Plug and Play Vulnerability – CAN-2005-1983:

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

Note Other protocols, such as Internetwork Packet Exchange (IPX) and Sequenced Packet Exchange (SPX), could be vulnerable to this issue. If you are using vulnerable protocols such as IPX and SPX, you should block the appropriate ports for those protocols. For more information about IPX and SPX, visit the following

[NT] Vulnerability in Plug and Play Allows Remote Code Execution and Elevation of Privilege (MS05-039)

<http://www.microsoft.com/resources/documentation/Windows/XP/all/reskit/en-us/prch_cnn_goue.asp>
Microsoft Web site.

Note As mentioned in the Mitigating Factors section, Windows XP Service Pack 2 and Windows Server 2003 are vulnerable to this issue primarily from locally logged on users. The following workarounds are designed primarily for earlier operating system versions that are vulnerable to anonymous network-based attacks.

Block TCP ports 139 and 445 at the firewall:

These ports are used to initiate a connection with the affected protocol. Blocking them at the firewall, both inbound and outbound, will help prevent systems that are behind that firewall from attempts to exploit this vulnerability. We recommend that you block all unsolicited inbound communication from the Internet to help prevent attacks that may use other ports. For more information about ports, visit the following <<http://go.microsoft.com/fwlink/?LinkId=21312>> Web site.

To help protect from network-based attempts to exploit this vulnerability, use a personal firewall, such as the <<http://go.microsoft.com/fwlink/?LinkId=33335>> Internet Connection Firewall, which is included with Windows XP Service Pack 1.

By default, the Internet Connection Firewall feature in Windows XP Service Pack 1 helps protect your Internet connection by blocking unsolicited incoming traffic. We recommend that you block all unsolicited incoming communication from the Internet.

To enable the Internet Connection Firewall feature by using the Network Setup Wizard, follow these steps:

1. Click Start, and then click Control Panel.
2. In the default Category View, click Network and Internet Connections, and then click Setup or change your home or small office network. The Internet Connection Firewall feature is enabled when you select a configuration in the Network Setup Wizard that indicates that your system is connected directly to the Internet.

To configure Internet Connection Firewall manually for a connection, follow these steps:

1. Click Start, and then click Control Panel.
2. In the default Category View, click Networking and Internet Connections, and then click Network Connections.
3. Right-click the connection on which you want to enable Internet Connection Firewall, and then click Properties.
4. Click the Advanced tab.
5. Click to select the Protect my computer or network by limiting or preventing access to this computer from the Internet check box, and then click OK.

Note If you want to enable certain programs and services to communicate through the firewall, click Settings on the Advanced tab, and then select

the programs, the protocols, and the services that are required.

To help protect from network-based attempts to exploit this vulnerability, enable advanced TCP/IP filtering on systems that support this feature.

You can enable advanced TCP/IP filtering to block all unsolicited inbound traffic. For more information about how to configure TCP/IP filtering, see <<http://support.microsoft.com/kb/309798>> Microsoft Knowledge Base Article 309798.

To help protect from network-based attempts to exploit this vulnerability, block the affected ports by using IPsec on the affected systems.

Use Internet Protocol security (IPsec) to help protect network communications. 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.

FAQ for Plug and Play Vulnerability – CAN-2005-1983:

What is the scope of the vulnerability?

This is a remote code execution and

<<http://go.microsoft.com/fwlink/?LinkId=21142>> local privilege elevation vulnerability. On Windows 2000, an anonymous attacker could remotely try to exploit this vulnerability. On Windows XP Service Pack 1, only an authenticated user could remotely try to exploit this vulnerability. On Windows XP Service Pack 2 and Windows Server 2003, only an administrator can remotely access the affected component. Therefore, on Windows XP Service Pack 2 and Windows Server 2003, this is strictly a local privilege elevation vulnerability. An anonymous user cannot remotely attempt to exploit this vulnerability on Windows XP Service Pack 2 and Windows Server 2003.

An attacker who successfully exploited this vulnerability 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?

An unchecked buffer in the Plug and Play service.

What is Plug and Play?

<<http://www.microsoft.com/technet/prodtechnol/windows2000pro/evaluate/featfunc/plugplay.mspx>> Plug and Play (PnP) allows the operating system to detect new hardware when you install it on a system. For example, when you install a new mouse on your system, PnP allows Windows to detect it, allows Windows to load the needed drivers, and allows Windows to begin using the new mouse.

What might an attacker use the vulnerability to do?

An attacker who successfully exploited this vulnerability could take

complete control of the affected system.

How could an attacker exploit the vulnerability?

On Windows 2000, an anonymous attacker could try to exploit the vulnerability by creating a specially crafted message and sending the message to an affected system. The message could then cause the affected system to execute code. This would be possible remotely on Windows XP Service Pack 1 from authenticated users only. On Windows XP Service Pack 2 and Windows Server 2003, to try to exploit the vulnerability, an attacker must be able to log on locally to a system and could then run a specially crafted application.

What systems are primarily at risk from the vulnerability?

Windows 2000 systems are primarily at risk from this vulnerability. On Windows XP Service Pack 1, Windows XP Service Pack 2, and Windows Server 2003 an attacker must have valid logon credentials to exploit this vulnerability. The vulnerability could not be exploited remotely by anonymous users on Windows XP Service Pack 1, Windows XP Service Pack 2, and Windows Server 2003.

Could the vulnerability be exploited over the Internet?

Yes, by anonymous users on Windows 2000 and by authenticated users on Windows XP Service Pack 1. 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. IT professionals can visit the <http://go.microsoft.com/fwlink/?LinkId=21171> Security Guidance Center Web site. On Windows XP Service Pack 2 and Windows Server 2003, an attacker must be able to log on to the specific system that is targeted for attack. An anonymous 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 the Plug and Play service validates the length of a message before it passes the message to the allocated buffer. Additionally, on Windows 2000, the update restricts anonymous access to the affected components, requiring users to authenticate with the affected component before attempting to use this functionality remotely. This change is consistent with the default settings of Windows XP Service Pack 1.

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.

Securiteam: [NT] Vulnerability in Plug and Play Allows Remote Code Execution and Elevation of Privilege (MS05-039)

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-2005-1983>>
CAN-2005-1983

ADDITIONAL INFORMATION

The information has been provided by Microsoft Product Security.

The original article can be found at:

<<http://www.microsoft.com/technet/security/Bulletin/MS05-039.msp>>
<http://www.microsoft.com/technet/security/Bulletin/MS05-039.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@securiteam.com

In order to subscribe to the mailing list, simply forward this email to: list-subscribe@securiteam.com

=====

=====

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.