

# [NT] Invalid Universal Plug and Play Request Can Disrupt System Operation

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2001-11/0000.html>

---

*From:* [support@securiteam.com](mailto:support@securiteam.com)

*Date:* 11/02/01

From: [support@securiteam.com](mailto:support@securiteam.com)

To: [list@securiteam.com](mailto:list@securiteam.com)

Subject: [NT] Invalid Universal Plug and Play Request Can Disrupt System Operation

Message-Id: <20011102212158.8D4C4138BF@mail.der-keiler.de>

Date: Fri, 2 Nov 2001 22:21:58 +0100 (CET)

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

When was the last time you checked your server's security?

How about a monthly report?

<http://www.AutomatedScanning.com> – Know that you're safe.

-----

## Invalid Universal Plug and Play Request Can Disrupt System Operation

---

### SUMMARY

The Universal Plug and Play (UPnP) service allows computers to discover and use network-based devices. Windows ME and XP include native UPnP services; Windows 98 and 98SE do not include a native UPnP service, but one can be installed via the Internet Connection Sharing client that ships with Windows XP.

A vulnerability results because the UPnP service does not correctly handle certain types of invalid UPnP requests. On Windows 98, 98SE, and ME systems, receiving such a request could cause a variety of effects ranging from slow performance to system failure. On Windows XP, the effect is less serious as the flaw consists of a memory leak. Each time a Windows XP system received such a request, a small amount of system memory would become unavailable; if repeated many times, it could deplete system resources to the point where performance slowed or stopped altogether.

### DETAILS

Affected Software:

## Securiteam: [NT] Invalid Universal Plug and Play Request Can Di

- \* Microsoft Windows 98
- \* Microsoft Windows 98SE
- \* Microsoft Windows ME
- \* Microsoft Windows XP

Note: Windows 98 and 98SE are only affected if the Internet Connection Sharing that ships with Windows XP has been installed on the machine.

Mitigating factors:

General:

- \* Standard firewalling practices (specifically, blocking ports 1900 and 5000) could be used to protect corporate networks from Internet-based attacks.

Windows 98 and 98SE:

- \* There is no native UPnP support for these systems. Windows 98 and 98SE systems would only be affected if the Internet Connection Sharing Client from Windows XP had been installed on the system.

Windows ME:

- \* Windows ME provides native UPnP support, but it is neither installed nor running by default. (However, some OEMs do configure pre-built systems with the service installed and running).

Windows XP:

- \* Internet Connection Firewall, which runs by default, would impede an attacker's ability to locate and attack the system.

Patch availability:

Download locations for this patch

- \* Microsoft 98 and 98SE:

<http://www.microsoft.com/Downloads/Release.asp?ReleaseID=33592>  
<http://www.microsoft.com/Downloads/Release.asp?ReleaseID=33592>

- \* Microsoft ME:

<http://www.microsoft.com/Windowsupdate>  
<http://www.microsoft.com/Windowsupdate>

- \* Microsoft XP:

This issue is eliminated via the update titled "Windows XP Update Package, October 25, 2001", at <http://www.microsoft.com/Windowsupdate>  
<http://www.microsoft.com/Windowsupdate>

What's the scope of the vulnerability?

This is a denial of service vulnerability. By sending a particular set of commands to an affected Windows 98, 98SE or ME machine, an attacker could cause a variety of effects, from slowing the machine's performance to causing it to fail altogether. The effect on a Windows XP machine would be less serious: at worst, the attacker could gradually deplete resources on the system to the point where performance could be slowed or stopped altogether.

There are a number of important restrictions affecting this vulnerability:

- \* On Windows 98 and 98SE, the service is only available if the user has installed an optional add-on package.
- \* On Windows ME, the affected component is available as part of the

## Securiteam: [NT] Invalid Universal Plug and Play Request Can Di

operating system but is not installed by default. (Some hardware manufacturers do, however, install it on the systems they sell)

\* Windows NT 4.0 and Windows 2000 are not affected at all by the vulnerability.

\* On Windows XP, the affected component is installed but not running by default. Even if it were running, Internet Connection Firewall would significantly reduce an attacker's ability to locate the machine.

What causes the vulnerability?

The vulnerability results because the Universal Plug and Play service that either ships with or can be installed on Windows 98, 98SE, ME and XP do not correctly handle certain requests. In Windows 98, 98SE and ME, these requests can cause an access violation and result in the system failing; in Windows XP, they cause a memory leak that, if exploited repeatedly, could deplete system resources to the point where the system performance was degraded.

What is Universal Plug and Play?

Universal Plug and Play (UPnP) is a capability that allows devices on a network to discover other devices and determine how to work with them. UPnP is most easily understood by comparison to plug-and-play (PnP) capability that most Windows users already are familiar with. PnP allows the operating system to detect new hardware when you install it on a system. For instance, if you install a new mouse onto your computer, PnP allows Windows to detect it, load the needed drivers, and begins using it.

UPnP extends this concept, and lets devices automatically recognize other devices on the network, rather than on the system. For instance, using UPnP, a computer that has been added to a network could detect whether there are printers on the network, and subsequently be able to control them.

What operating systems support UPnP?

\* Neither Windows 98 nor Windows 98SE include a native UPnP capability. It can only be added by installing the Internet Connection Sharing client provided in Windows XP.

\* Windows ME includes a native UPnP capability, but it is neither installed nor running by default.

\* Neither Windows NT 4.0 nor Windows 2000 support UPnP.

\* Windows XP includes a native UPnP capability. It is installed and running by default.

What's wrong with the UPnP service?

The service does not correctly handle certain types of invalid UPnP requests. The specific effects of receiving such a request vary, depending on which operating system is in use.

What's the effect of receiving such a request on a Windows 98, 98SE or ME system?

In these implementations, such a request could either degrade system performance or cause the system to fail altogether. The user could restore

## Securiteam: [NT] Invalid Universal Plug and Play Request Can Di

normal operation by rebooting the system.

What's the effect of receiving such a request on a Windows XP system?

On Windows XP, receiving such a request would deplete the system memory by a small amount. If the request were repeatedly sent over time, it could gradually deplete system memory to the point where it would slow or stop the system. The user could restore normal operation by rebooting the system.

What's the effect of receiving such a request on a Windows NT 4.0 or Windows 2000 system?

Neither Windows NT 4.0 nor Windows 2000 support UPnP, and as a result, neither is affected by the vulnerability.

How could an attack exploit this vulnerability?

An attacker could exploit the vulnerability by locating a system that has the UPnP service installed and running, and sending it the UPnP requests we have discussed above.

You said that the attacker would need to locate a vulnerable system first. Would this be difficult?

It would be, in the case of Windows XP. Windows XP ships with Internet Connection Firewall (ICF), the goal of which is to effectively make the system invisible on the network – that is, it causes the system to not respond to pings, port scans, and other measures that attackers might use to locate a system. ICF is installed and running by default.

Could an attacker exploit this vulnerability from the Internet against machines within a corporate network?

If proper firewalling were in place, Internet-based attacks would not be possible. The ports over which UPnP operates (ports 1900 and 5000) should be blocked at the firewall.

How can I determine whether the UPnP service is installed on my machine?

For Windows 98, 98SE, and ME:

- 1) Select Start, then Settings, then Control Panel
- 2) Select Add/Remove Programs
- 3) Select the Windows Setup tab.
- 4) Open the Communications sub-item
- 5) If the checkbox for Universal Plug and Play is checked, the service is installed and running.

For Windows XP:

- 1) Select Start, then right-click on My Computer and select Manage
- 2) Select Services and Applications, then select Services
- 3) Scan the list of services and locate the one named Universal Plug and Play Device Host.
- 4) Check the column titled Status. If it says Started, the service is installed and running.

## Securiteam: [NT] Invalid Universal Plug and Play Request Can Di

If UPnP is running on my machine, will turning it off protect me against the vulnerability?

Yes. If the service is not running, the vulnerability cannot be exploited.

How can I turn off the service?

For Windows 98, 98SE, and ME:

- 1) Select Start, then Settings, then Control Panel
- 2) Select Add/Remove Programs
- 3) Select the Windows Setup tab
- 4) Open the Communications sub-item
- 5) Uncheck the Universal Plug and Play selection

For Windows XP:

- 1) Select Start, then right-click on My Computer and select Manage
- 2) Select Services and Applications, then select Services
- 3) Scan the list of services and locate the one named Universal Plug and Plug Device Host.
- 4) Right-click on the service, and select Properties
- 5) In the section titled Service Status, click on Stop
- 6) In the pull-down box titled Startup Type, select Disabled

What does the patch do?

In Windows 98, 98SE and ME, the fix is delivered via an update to the UPnP service, which eliminates a number of eliminates this vulnerability as well as a number of other less serious bugs in the UPnP service. In Windows XP, the fix is delivered as part of the first Windows XP Critical Update, which corrects a number of other issues, some security-related, in addition to this one.

### ADDITIONAL INFORMATION

The information has been provided by <<mailto:secnotif@MICROSOFT.COM>>  
Microsoft Product Security.

=====

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](mailto:list-unsubscribe@securiteam.com)

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

---

• *Messages sorted by:* [\[ date \]](#) [\[ thread \]](#) [\[ subject \]](#) [\[ author \]](#) [\[ attachment \]](#)