

[NT] UPNP – Multiple Remote Windows XP/ME/98 Vulnerabilities

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2001-12/0103.html>

From: support@securiteam.com

Date: 12/24/01

From: support@securiteam.com

To: list@securiteam.com

Date: Mon, 24 Dec 2001 11:50:17 +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.

UPNP – Multiple Remote Windows XP/ME/98 Vulnerabilities

SUMMARY

Windows XP ships by default with a UPNP (Universal Plug and Play) service which can be used to detect and integrate with UPNP aware devices. Windows ME does not ship by default with the UPNP service; however, some OEM versions do provide the UPNP service by default. In addition, it is possible to install the Windows XP Internet Connection Sharing on top of Windows 98, therefore making it vulnerable.

As described on upnp.org: "UPNP architecture offers pervasive peer-to-peer network connectivity of PCs of all form factors, intelligent appliances, and wireless devices. UPNP architecture leverages TCP/IP and the Web to enable seamless proximity networking in addition to control and data transfer among networked devices in the home, office, and everywhere in between".

eEye believes that there are several security issues with the UPNP protocol itself; however, these more generic issues are out of the scope of this advisory. Expect a detailed paper to be released from eEye within the coming weeks.

Securiteam: [NT] UPNP – Multiple Remote Windows XP/ME/98 Vulnerabilities

This advisory covers three vulnerabilities within Microsoft's UPNP implementation. A remotely exploitable buffer overflow to gain SYSTEM level access to any default installation of Windows XP, a Denial-of-Service (DoS) attack, and a Distributed Denial-of-Service (DDoS) attack.

DETAILS

Vulnerable systems:

Microsoft Windows XP (All default systems)

Microsoft Windows 98 (Certain configurations)

Microsoft Windows 98SE (Certain configurations)

Microsoft Windows ME (Certain configurations)

1. The SYSTEM Remote Exploit

The first vulnerability within Microsoft's implementation of the UPNP protocol can result in an attacker gaining remote SYSTEM level access to any default installation of Windows XP. SYSTEM is the highest level of access within Windows XP.

During testing of the UPNP service, eEye discovered that by sending malformed advertisements at various speeds eEye could cause access violations on the target machine. Most of these violations were due to pointers being overwritten. The following describes one instance of our testing:

Example Session:

```
NOTIFY * HTTP/1.1
```

```
HOST: 239.255.255.250:1900
```

```
CACHE-CONTROL: max-age=10
```

```
LOCATION: http://IPADDRESS:PORT/.xml
```

```
NT: urn:schemas-upnp-org:device:InternetGatewayDevice:1
```

```
NTS: ssdp:alive
```

```
SERVER: EEYE/2001 UPnP/1.0 product/1.1
```

```
USN: uuid:EEYE
```

If a buffer is incremented in the protocol, port, and uri fields of the Location URL and send sessions with 10,000 microsecond intervals, access violations will begin to be observed. In one situation, The EAX and ECX registers will contain addresses that are pulled from the memory that was overwritten and the svchost.exe process will access an invalid memory address at a "mov" instruction. It throws an access violation because the destination address is an overwritten pointer, but there is nothing interesting at 0x41414141.

During our testing eEye discovered that there are multiple points of exploitation. eEye found instances of stack overflows and heap overflows, both of which were exploitable. In the case of the heap overflow, eEye saw pointers being overwritten for both buffers and functions.

Securiteam: [NT] UPNP – Multiple Remote Windows XP/ME/98 Vulnerabilities

The SSDP service also listens on Multicast and Broadcast addresses. Therefore gaining SYSTEM access to an entire network of XP machines is possible with only one anonymous UDP SSDP attack session.

2. The DoS and DDoS

UPNP consists of multiple protocols, one of which being the Simple Service Discovery Protocol (SSDP). When a UPNP enabled device is installed on a network, whether it be a computer, network device, or even a household appliance, the device sends out an advertisement to notify control points of its existence. On a default XP installation, no support is added for device control, as it would be the case in an installation of UPNP from "Network Services".

Although Microsoft added default support for an "InternetGatewayDevice", if a sniffer is run on a network with XP, XP can be observed searching for this device as XP is loading. This support was added to aid leading network hardware manufactures in making UPnP enabled "gateway devices".

By sending a malicious spoofed UDP packet containing an SSDP advertisement, an attacker can force the XP/ME client to connect back to a specified IP address and pass on a specified HTTP/HTTPS request.

An example session:

```
NOTIFY * HTTP/1.1
HOST: 239.255.255.250:1900
CACHE-CONTROL: max-age=1
LOCATION: URL
NT: urn:schemas-upnp-org:device:InternetGatewayDevice:1
NTS: ssdp:alive
SERVER: EEYE/2001 UPnP/1.0 PASSITON/1.1
USN: uuid:EEYE
```

The above packet data needs to be sent as a UDP packet to port 1900 of the XP/ME machine.

When the XP machine receives this request, it will interpret the URL following the LOCATION header entity. With no sanitizing of the URL, it is passed on to the functions in the Windows Internet Services API. The string is broken down and the new session is created.

For example:

```
LOCATION: http://xptest.example.com:19/himom.html
```

A malicious attacker could specify a chargen service on a remote machine causing the XP client to connect and be caught in a tight read/malloc loop. Doing this will throw the machine into an unstable state where CPU utilization is at %100 and memory is being allocated to the point that it is totally consumed. This makes the remote XP system completely unusable and requires a physical power-off shutdown.

Securiteam: [NT] UPNP – Multiple Remote Windows XP/ME/98 Vulnerabilities

Attackers could also use this exploit to control other XP machines, forcing such machines to perform Unicode attacks, double decode, or random CGI exploiting. Due to the insecure nature of UDP, an attacker can exploit security holes on a web server using UPNP with almost total anonymity.

One of the bigger problems, and why this can become a DDoS attack, is that this SSDP announcement can be sent to broadcast addresses and multicast. It is therefore possible to send one UDP packet causing all XP machines on the target network to be navigated to the URL of choice, performing an attack of choice.

Also since parts of the UPNP service are implemented as UDP (in our opinion, a bad idea), it makes all of these attacks completely untraceable.

Vendor status:

Microsoft has released a patch and security bulletin that is located at:
<<http://www.microsoft.com/technet/security/bulletin/MS01-059.asp>>
<http://www.microsoft.com/technet/security/bulletin/MS01-059.asp>

To verify that the patch has been installed on your system, do the following:

Windows 98 and 98SE:

Select Start, then Run, then run the QFECheck utility. If the patch is installed, "Windows 98 Q314941 Update" will be listed among the installed patches. To verify the individual files, use the file manifest provided in Knowledge Base article Q314941.

Windows ME:

Select Start, then Run, then run the QFECheck utility. If the patch is installed, "Windows Millennium Edition Q314757 Update" will be listed among the installed patches. To verify the individual files, use the file manifest provided in Knowledge Base article Q314757.

Windows XP:

Confirm that the following registry key has been created on the machine:
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Updates\Windows XP\SP1\Q315000. To verify the individual files, use the date/time and version information provided in the following registry key:
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Updates\Windows XP\SP1\Q315000\Filelist.

eEye would strongly suggest denying all UPNP traffic at your internet borders, as there is really no need to allow UPNP traffic across the Internet. In addition, it would be wise to completely turn off the UPNP services, as most users are probably not utilizing them. The less services running on your machine, the safer you will be. The SSDP Discovery Service and Universal Plug and Play Host service should both be set to manual load.

Securiteam: [NT] UPNP – Multiple Remote Windows XP/ME/98 Vulnerabilities

ADDITIONAL INFORMATION

The information has been provided by Riley Hassell of eEye.

=====

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.

-
- *Previous message:* support@securiteam.com: "[UNIX] PHPNuke module.php Vulnerability and PHP error reporting Issue"
 - *Messages sorted by:* [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#) [\[attachment \]](#)