

Multiple Remote Windows XP/ME/98 Vulnerabilities

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/bugtraq/2001-12/0219.html>

From: Marc Maiffret (marc@eeye.com)

Date: 12/20/01

From: "Marc Maiffret" <marc@eeye.com>
To: "BUGTRAQ" <BUGTRAQ@SECURITYFOCUS.COM>
Date: Thu, 20 Dec 2001 10:19:54 -0800

Multiple Remote Windows XP/ME/98 Vulnerabilities

Release Date:
12/20/01

Severity:
High

Systems Affected:
Microsoft Windows XP (All default systems)
Microsoft Windows 98 (Certain configurations)
Microsoft Windows 98SE (Certain configurations)
Microsoft Windows ME (Certain configurations)

Description:
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. Also its possible to install the Windows XP Internet Connection Sharing on top of Windows 98, therefore making it vulnerable.

"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." as described on upnp.org.

We believe that there are several 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.

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.

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

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 memory that was overwritten and the svchost.exe process will access an invalid memory address at a "mov" instruction. It throws an access violation due to the fact that the destination address is an overwritten pointer, and there's nothing interesting at 0x41414141.

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

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.

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, it 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".

SecurityFocus Bugtraq: Multiple Remote Windows XP/ME/98 Vulnerabilities

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 get 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 basically makes the remote XP system completely unusable and requires a physical power off shutdown.

Attackers could also use this exploit to control other XP machine's, 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.

SecurityFocus Bugtraq: Multiple Remote Windows XP/ME/98 Vulnerabilities

Vendor Status:

Microsoft has released a patch and security bulletin which is located at:

<http://www.microsoft.com/technet/security/bulletin/MS01-059.asp>

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

Windows 98 and 98SE:

To verify that the patch has been installed on the machine, 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:

To verify that the patch has been installed on the machine, 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:

To verify that the patch has been installed on the machine, 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.

The Common Vulnerabilities and Exposures (CVE) project has assigned the following two ID's:

The Buffer Overflow: CAN-2001-0876

The Denial of Service: CAN-2001-0877

This is a candidate for inclusion in the CVE list <http://cve.mitre.org>, which standardizes names for security problems.

We would strongly suggest denying all UPNP traffic at your internet borders as there is really no need to allow UPNP traffic across the Internet. Also it would be wise to completely turn off the UPNP service's as most users are probably not utilizing them anyways. 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.

Discovery:

Riley Hassell <riley@eeye.com>

With extra help from:

Ryan Permech – for technical advice and exploitation analysis for those difficult reverse engineering situations that Ryan has

SecurityFocus Bugtraq: Multiple Remote Windows XP/ME/98 Vulnerabilities

wet dreams about.

Marc Maiffret – as always with superb technical insight helping to discover and exploit the vulnerabilities in this advisory and once again proving that two heads are better than one.

Neothoth – "The typing machine", for camping out day and night in the eEye lab hammering vulnerabilities in URL handlers. Neo rocks :)

Greetings:

Mr. Patron and his tequila and the Three Wise Men(jim, jack and johnny).

Also Abraxas coffeeshop in Amsterdam.

eEye would like to offer thanks to all organizations supporting full disclosure, especially Securityfocus.com and NMRC. Don't let silly politics get in the way of what is right for everyone's security.

oh yeah, one more thing:

Four score and numerous advisories ago, a security company set off to tell the world about its love of Tequila. However, little did people know, the team was not even legal. Now that the youngin's Marc and Riley turned 21 this Nov. we are all officially legal. That means the next time the NSA buys us beer at a sec conference, they wont be breaking the law.

Copyright (c) 1998–2001 eEye Digital Security

Permission is hereby granted for the redistribution of this alert electronically. It is not to be edited in any way without express consent of eEye. If you wish to reprint the whole or any part of this alert in any other medium excluding electronic medium, please e-mail alert@eEye.com for permission.

Disclaimer

The information provided in this advisory may change without notice. Your reproduction or use of this information shall constitute your acceptance of the terms in this paragraph. This information is provided "AS IS" and eEye Digital Security disclaims all warranties, express and implied, with regard to this information. This information is provided only for legitimate security analysis purposes. eEye Digital Security does not condone the unauthorized access of systems or the writing or launching of worms, viruses or other software for malicious purposes, and specifically prohibits the use or reproduction of this information for such purposes. In no event shall eEye Digital Security or any author be liable for any damages whatsoever arising out of or in connection with the use or dissemination of this information. Any use of this information is at the user's own risk.

Feedback

Please send suggestions, updates, and comments to:

eEye Digital Security

<http://www.eEye.com>

info@eEye.com

- **Previous message:** [eNowak IGF remote: "Re: IRM Security Advisory 002: Netware Web Server Source Disclosure"](#)
- **Messages sorted by:** [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#) [\[attachment \]](#)