# Microsoft's Universal Plug and Play Does Not Play Securely

**Quana Bluford**

**January 26, 2002**

Quana Bluford
qjblufo001
Security Essentials/GSEC Certification
Version 1.2f
Original assignment
Conference course

*Table of Contents*

## Introduction

Knowing the vulnerabilities of a system and network is necessary to defend and protect it from malicious code, viruses, and hackers. Most hackers exploit known system vulnerabilities and continuously explore systems to find new entry methods to invade networks. By keeping current with virus and attack advisories, system administrators can receive notices on vulnerabilities and viruses, and how to provide protection.

Microsoft's Universal Plug and Play (UPnP) is a well-known service in various Microsoft operating systems. It provides a great service for interfacing new equipment without configuration. However, extensive research has discovered multiple vulnerabilities in its implementation. The first vulnerability is a remotely exploitable buffer overflow that can allow an attacker to gain system-level access. The second vulnerability allows a Denial of Service (DoS) attack and a Distributed Denial of Service (DDoS) attack because UPnP does not take adequate steps to limit how far the service goes to obtain information about a discovered service (eEye®, 2001). Providing information about UPnP's vulnerabilities will aid system administrators and users in protecting their systems and computers from attacks. This paper provides a clear, concise explanation of Microsoft's UPnP, its known vulnerabilities, and steps system administrators should take to secure their networks.

## What is Universal Plug and Play?

UPnP service allows computers to discover and use networked-based devices with no network configuration required by system administrators. A device can automatically join a network, acquire an IP address, share its capabilities, and learn about the existence and capabilities of other devices. This allows the devices to communicate with one another, permitting peer-to-peer networking. For example, a computer added to a network could determine if there are network printers that it can use and manage without requiring configuration from a system administrator.

In Windows XP, the UPnP service is installed as one of the default services. Windows ME includes the UPnP service, but it is not installed by default unless it's an OEM version. Neither Windows 98 nor Windows 98SE includes the UPnP service, but the Internet Connection Sharing (ICS) client provided in Windows XP can install it. Windows NT 4.0 and Windows 2000 do not support UPnP; therefore, they are not affected by the vulnerabilities.

| Operating System | Windows XP | Windows 98/ Windows 98 SE | Windows NT | Windows 2000 | Windows ME |
|---|---|---|---|---|---|
| Supports UPnP | X | X | | | X |
| Running by Default | X | | | | |

**Table 1. Microsoft's Operating Systems Supporting UPnP.**

## How UPnP Works

To further understand UPnP, let's take a look at how it works. There are six steps involved in UPnP networking: addressing, discovery, description, control, eventing, and presentation.

### Addressing

The first step involved in UPnP networking is **Addressing**. Each device has a Dynamic Host Configuration Protocol (DHCP) client and searches for a DHCP server when the device is initially connected to the network. If a DHCP server is available, the device will use the IP address assigned to it. If no DHCP server is available, the device must use Auto IP to get an address. Auto IP defines how a device intelligently chooses an IP address from a set of reserved private addresses; it allows a device easily move between managed and unmanaged networks. Once an IP address has been assigned to the device, it can communicate with other devices on the network using TCP/IP (Microsoft ®, 2001).

### Discovery

Now that a device can communicate on the network, it needs to make itself known to UPnP control points that exist on the network. When a device is added to the network, the UPnP **Discovery** protocol allows that device to advertise its services to control points on the network. When a new control point is added to the network, it multicasts a Simple Device Discovery Protocol (SSDP) message that allows the control point to search for devices of interest on the network. The discovery message contains important specifics about the device or one of its services. For example, a discovery message may give details such as the device type identifier and the pointer, or URL, to its description document (Microsoft ®, 2001).

### Description

The next step in UPnP networking is **Description**. After a control point has discovered a device, the control point still needs to know more information about the device. In order for the control point to learn more about the device and its capabilities, or to interact with the device, the control point must retrieve the device's description from the URL provided by the device in the discovery message. Devices may in fact contain other logical devices and services. The UPnP description for a device is expressed in Extensible Markup Language (XML) and includes vendor-specific, manufacturer information including the model name and number, serial number, manufacturer name, URLs to vendor-specific Web sites, etc. XML is used throughout the UPnP implementation. The description contains a list of any embedded devices or services, as well as URLs for control, eventing, and presentation (Microsoft ®, 2001).

### Control

After a control point has retrieved a description of the device, the control point has the fundamentals for device **Control**, which is the next step involved in UPnP networking. To learn more about the service, a control point must retrieve a detailed UPnP description for each service. The description for a service is also expressed in XML and includes a list of commands and actions the service responds to, and parameters or arguments for each action. The description for a service also includes a list of variables that model the state of the service at run time, and are described in terms of their data type, range, and event characteristics. To control a device, the control point sends a control message to the control URL for the device's service. In response to the control message, the service returns action-specific values or fault codes (Microsoft ®, 2001).

Eventing

An UPnP description for a service includes a list of actions the service responds to and a list of variables that model the state of the service at run time. The service publishes updates when these variables change, and a control point may subscribe to receive this information. The service publishes updates by **Eventing** or sending event messages. Event messages contain the names of one or more state variables and the current value of those variables. A special event message contains the names and values for all evented variables and allows the subscriber to initialize its model of the state of service when a control point first subscribes (Microsoft ®, 2001).

Presentation

Finally, in the **Presentation** step, the URL for the presentation page is contained in the device description. Retrieving this page requires the control point to issue an HTTP GET request to the presentation URL. The device will then return a presentation page where a user can control the device and view its status (Microsoft ®, 2001).

**Vulnerabilities**

eEye Digital reported multiple vulnerabilities that exist in Microsoft's implementation of UPnP. There is a remotely exploitable buffer overflow that allows an attacker to gain system-level access to any default installation of Windows XP. The other two vulnerabilities are types of DoS attacks that affect all UPnP implementations. In the DoS attack the hacker can remotely crash the Windows XP system only in the Windows XP implementations of UPnP. The second DoS attack is a DDoS, which allows a hacker to remotely command many Windows XP systems at once in an effort to flood a single host (eEye ®, 2001).

Remotely Exploitable Buffer Overflow

A buffer is a storage place for bits or information. Computer programmers usually create sections in memory for information storage within their code. A buffer overflow occurs when more data is put into a buffer than it can hold. In actuality, the program writes past the bounds of the buffer, thus creating a buffer overflow. As this happens, the adjacent memory is overwritten, and critical information is replaced with garbage code, unintelligent code, or malicious code causing programs to execute incorrectly or fail completely. In some cases, which Gary McGraw and John Vieta of Reliable Software Technologies (2000) describe, "The program can proceed without any noticeable difference in execution." This means that malicious code, such as a virus or a worm, can be placed into a program without its presence being detected.

Problems caused by buffer overflows have plagued system administrators for many years, yet buffer overflows continue to create critical vulnerabilities. "Buffer overflows have been causing serious security problems for decades, and are far from ancient history. Buffer overflows accounted for over 50 percent of all major security bugs leading to CERT/CC advisories last year" (John Vieta and Gary McGraw, 2000).

Microsoft's implementation of UPnP allows a remotely exploitable buffer overflow that can result in system-level access to the vulnerable host. There is an unchecked buffer in one of the services' components that handles messages in the Discovery step of UPnP networking. By sending a particularly malformed discovery message produced at different segments, it would be possible for a hacker to write or develop code that will allow them to carry out commands at the highest level of access within Windows XP. This system level access includes the ability to delete files, change users' settings, and download malicious software. This is definitely, an attractive hacker attack. Since UPnP service runs with system privileges, a hacker who successfully exploited this vulnerability could gain complete control over the system.

DoS

Another common vulnerability in UPnP is the DoS attack. During a connection, the device sends a message asking the server to authenticate it. The server returns the approved authenticated message to the device. The device acknowledges the approval and then is given permission to access the server. In a DoS attack, the device sends several authenticated requests to the server, filling it up. All requests have false return addresses, so the server can't locate the originator when it tries to send the authenticated approval. The server waits, usually longer than a minute, before closing the connection. Once it closes the connection, the attacker sends a new batch of fake requests, and the process starts all over again. This repetition leads to a DoS because the server is occupied dealing with these requests. (CNET News.com Staff, 2000).

The DoS attack can occur in Microsoft's UPnP because it does not take sufficient steps to limit how far the service goes to obtain information about a discovered service. Within the description step of UPnP networking, a new UPnP device sends information telling the other computers where to get its device description. The device description lists the services the device offers and procedures for using them. The device description could in fact be located on a third-party server instead of the device itself. Nevertheless, the UPnP implementations do not sufficiently control how it performs this task and, as a result, two DoS vulnerabilities exist.

In the first situation a hacker could send a discovery message to a susceptible host and loop the request. This loop would ultimately devour all system resources on the susceptible system. The U.S. Department of Energy's Computer Incident Advisory Capability (CIAC) illustrates an example where a hacker could send a discovery message to an UPnP-capable computer, specifying that the device description should be downloaded from a particular port on a particular server. If the server was configured to simply echo the downloaded request back to the UPnP, the computer could be made to enter an endless download cycle that could consume some or all of the system's availability. An attacker could craft and send this directive to a victim's machine directly, by using the machine's IP address. Or, an attacker could send this same directive to a broadcast and multicast domain, and attack all affected machines nearby, consuming some or all of those systems' availability. The DoS vulnerability could delay, or prohibit performance on a single machine (U.S. Department of Energy, 2001).

The second DoS vulnerability, the DDoS, occurs when an attacker uses multiple machines to flood a computer with data. As the UPnP service responds to a flood of fake requests, it gets too many responses from the machines, resulting in a distributed attack. The hacker could not gain administrative privileges over the system by using this vulnerability, but he could use it to render the system useless.

**Countermeasures**

Microsoft has released a patch and is recommending all Windows XP users and system administrators apply it immediately. The patch provides a fix for both vulnerabilities. The patch eliminates the buffer overflow vulnerability by instituting proper buffer handling in the Windows XP UPnP implementation. The patch introduces a new functionality that enables system administrators to alter how patched systems undertake device discovery.

Microsoft's patch prevents the DoS attack by changing how the UPnP services in the affected system handle device descriptions. It sets a maximum size on device descriptions and ensures the system does not accept any that exceed that size. The patch also causes the service to validate the information in the device description, and reject any invalid information. To combat the distributed DoS vulnerability, the patch institutes checking to confirm that the downloaded location is valid and that the system does not continually try to download device descriptions from it. It also provides the ability for the administrator to regulate which machines the system will attempt to download such information from.

As described earlier, Windows 98 and Windows ME machines can inherit this vulnerability from Windows XP through the use of ICS. The patch prevents further infection by updating netsetup on Windows XP. Once the patch is applied to a Windows XP machine, any Windows 98 or Windows ME machines that are subsequently configured to use ICS from the patched Windows XP machine will not be affected by the vulnerability (Microsoft ®, 2001). If a Windows 98 or Windows ME is already affected, Microsoft's website has a patch to fix these operating systems.

After installing all necessary patches, system administrators should make an evaluation to determine if UPnP is needed. They should make a decision based on what they're willing to risk. If the system administrators conclude that the service is not needed, it should be turned off.

In addition, the CIAC suggests that a corporate firewall would protect against attacks from the Internet. Most firewalls block unsolicited messages. Blocking ports 1900 and 5000 helps protect against Internet-based attacks. Additionally, using an Internet Connection Firewall (ICF) should provide some protection against an attack via unsolicited messages because, to carry out such an attack, the hacker would need to know the IP address of the target system. Since ICF causes the machine not to respond to port scans and other common methods of obtaining the IP address, the hacker will be unable to send a message to the target system (US Department of Energy, 2001).

**Conclusion**

Microsoft's UPnP is a powerful tool that can potentially reduce the workload for system administrators. However, the recent discovery of critical vulnerabilities should remind system administrators of the importance of essential security practices. First, system administrators must understand the services being configured under default installations. An evaluation must be done to determine if the product or service is necessary. Then a risk analysis must be done to determine what the system administrator is willing to risk. Additionally, it is imperative for system administrators to stay abreast of vulnerabilities and alerts. System administrators should load patches as they are provided. If no patches are immediately available from the vendor, ideas for alternative solutions may be found by looking at approaches other system administrators have taken.

## References

CNET News.com Staff, "How a denial of service attack works". February 9, 2000. http://news.com.com/2100-1017-236728.html Accessed: January 25, 2002

eEye® Digital Security, "eEye® Digital Security Announces Major Vulnerabilities in Default Installations of Windows XP and Certain Installations of Windows ME and 98." December 20, 2001. http://www.eeye.com/html/Research/Advisories/AD20011220.html Accessed: December 21, 2001.

Internet Security System Security Alert. "Multiple Vulnerabilities in Universal Plug and Play Service." December 20, 2001. http://xforce.iss.net/alerts/advise106.php Accessed: January 25, 2002.

McGraw, Gary, Vieta John. "Making your software behave. Learning the Basics of Buffer." Overflow." Reliable Software Technologies. March 2001. http://www-106.ibm.com/developerworks/library/overflows/index.html?e Accessed: January 25, 2002.

Microsoft® Corporation. "How UPnP Works." June 29, 2001. http://www.microsoft.com/windowsxp/pro/techinfo/planning/upnp/howitworks.asp Accessed: January 10, 2002.

Microsoft® Corporation. "Universal Plug and Play in Windows XP." June 29, 2001. http://www.microsoft.com/windowsxp/pro/techinfo/planning/upnp/howitworks.asp Accessed: January 10, 2002.

Pfeil, Ken. "Denial of Service in Microsoft Universal Plug and Play Service." November 2, 2001. http://www.secadministrator.com/Articles/Index.cfm?ArticleID=23110 Accessed: January 4, 2002.

Pfeil, Ken. "Multiple Vulnerabilities in Microsoft Universal Plug and Play." December 21, 2001. http://www.secadministrator.com/Articles/Index.cfm?ArticleID=23594 Accessed: January 4, 2002.

U.S. Department of Energy. "Computer Incident Advisory Capability: M-030: Multiple Remote Windows XP/ME/98 Universal Plug and Play Vulnerabilities [Microsoft Security Bulletin MS01-059]." December 21, 2001. http://ciac.llnl.gov/ciac/bulletins/m-030.shtml Accessed: January 4, 2002.

**Questions**

1. Why is the remotely exploitable buffer overflow the most critical vulnerability associated with UPnP?
    a. Buffer overflows have been causing serious security problems for decades
    b. Buffer overflow is a common vulnerability
    c. It can result in system level access
    d. A buffer is storage place for bits

    *The correct answer is **C**. The most critical vulnerability is the remotely exploitable buffer overflow that can result in system level access. Since UPnP runs with system privileges, hacker who successfully exploited this vulnerability could gain complete control over the system .

2. Why does the denial of service vulnerability exist in UPnP?
    a. It does not take sufficient steps to limit how far the service goes to obtain information about a discovered service
    b. By using this vulnerability the hacker could not gain administrative over the system
    c. Denial of service attack is a common vulnerability
    d. Because your system has a backdoor

    *The correct answer is **A**. The denial of service can occur in UPnP because it does not take sufficient steps to limit how far the service goes to obtain information about a discovered service. The device description could in fact be located on a third party server instead of the device itself. Nevertheless, the UPnP implementations do not sufficiently control how it performs this task.

3. How would you defend your system against a remotely exploitable buffer overflow if the patch were not available.
    a. Using a virus program such as McAfee
    b. Ordering software from Microsoft
    c. Installing additional hardware
    d. A corporate firewall

    *The correct answer is **D**. CIAC suggests that, a corporate firewall would protect against attacks from the Internet. Most firewalls block unsolicited messages. An Internet Connection Firewall (ICF) should also provide some protection against an attack via unsolicited messages because, to carry out such an attack the hacker would need to know the IP address of the target system.. The ICF causes the machine not to respond to port scans and other common methods of obtaining the IP address, and hence unable to send a message to it.

4. What is one way that the patch that Microsoft released prevents a denial of service attack?
    a. It sets a maximum size on device descriptions
    b. It denies the hacker access to your system
    c. It will not allow your IP address to be viewed by outsiders
    d. It makes sure everyone can access your services without ever being denied

    *The correct answer is **A**. The patch changes how the UPnP services in the affected system handle device description. It sets a maximum size on descriptions, and ensures that the system does not accept any that exceed that size.

5. During which step of UPnP networking does the device need to make themselves known to UPnP control points that are already up and running on the network.
    a. Addressing
    b. Discovery
    c. Control
    d. Presentation

    *The correct answer is **B**. When a device is added to the network, the UPnP discovery protocol allows that device to advertise its services to control point on the network. When a new control point is added to the network, it multicasts a Simple Device Discovery Protocol (SSDP) message that allows the control point to search for devices of interest on the network. The discovery message contains a few important specifics about the device or one of its services.

**True/False**

6. Windows NT and Windows 2000 both support UPnP and the service is installed and one of the default services.

    *The correct answer is **False**. Neither Windows NT nor Windows 2000 support UPnP therefore, they are not affected by the vulnerabilities. In Windows XP the service is installed and running by default. In Windows ME, includes the service, but the user must install it. Neither Windows 98 nor Windows 98 SE includes the service, but the Internet Connection Sharing client provided in XP can install it.

7. Universal Plug and Play (UPnP) service allows computers to discover and use networked based devices.

    *The correct answer is **True**. With UPnP, a device can automatically join a network, acquire an IP address, share its capabilities, and learn about the existence and capabilities of other devices without any network configuration. This allows the devices to communicate with one another permitting peer-to-peer networking.

8. There are eight steps involved in the UPnP networking.

    *The correct answer is **False**. To further understand how UPnP works, let's take a look at the six steps. There are six steps involved in UPnP networking, which are addressing, discovery, description, control, eventing, and presentation.

9. Each device must have a Dynamic Host Configuration Protocol (DHCP) client and search for a DHCP server when the device is initially connected to the network.

*The correct answer is **True**. In order for the devices to communicate with one another on the network they must have an IP address assigned to them.

10. A buffer overflow occurs when you do not put enough data in the buffer.
    *The correct answer is **False**. A buffer overflow occurs when you put more data in a buffer than it can hold. In actuality, the program writes past the bounds of the buffer creating a buffer overflow.