

Multiple Remote Windows XP/ME/98 Vulnerabilities

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/focus-ms/2001-12/0299.html>

From: Marc Maiffret (marc@eeye.com)

Date: 12/20/01

From: "Marc Maiffret" <marc@eeye.com>
To: "FOCUS-MS" <FOCUS-MS@SECURITYFOCUS.COM>
Date: Thu, 20 Dec 2001 10:19:55 -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.

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

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 w