

[NT] IrDA Semi-Remote Vulnerability

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2001-08/0090.html>

From: support@securiteam.com

Date: 08/23/01

From: support@securiteam.com

To: list@securiteam.com

Subject: [NT] IrDA Semi-Remote Vulnerability

Message-Id: <20010823142959.A7FF4138BF@mail.der-keiler.de>

Date: Thu, 23 Aug 2001 16:29:59 +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.

IrDA Semi-Remote Vulnerability

SUMMARY

Windows machines suffer from a 'semi remote' vulnerability that can be exploited via the infrared port. As result of exploiting this vulnerability the computer will crash, displaying a "Blue Screen of Death" (BSOD), shortly followed by a reboot.

As IrDA ports are mostly found on laptops, these machines are more likely to be exploitable. Limited test data suggests this attack is successful against Windows 2000 Professional machines, but not against machines running Windows 98. Other OS versions have not been tested.

DETAILS

Systems tested that were vulnerable:

- [] OEM laptop, Windows 2000 Professional service pack 2 v5.00.2195, National Semiconductor IrDA.

Options:

Infrared Trans. A: HP HSDL-1100/2100,

Infrared Trans. B SIR Transceiver,

Max Con. Rate: 4Mbps.

Driver National Semiconductor 9/8/1999 v1.0.0.0 (signed MS 2000 Publisher)

Securiteam: [NT] IrDA Semi-Remote Vulnerability

[] Toshiba Satellite Pro 4000, Windows 2000 Professional service pack 2 v5.00.2195, SMC IrCC IrDA.

Options:

Fast Infrared Port: Infrared

Transceiver Type: auto,

Min. Turn-Around Time: 1.0mS,

Speed Limit: 4 Mbps,

Driver: SMC 22/10/2000 v4.10.1999.5 (signed MS comp).

[] Acer TravelMate 527TE P3-700MHz, Windows 2000 Professional

Systems tested that were not vulnerable:

[] Dell Inspiron 3200 D233XT TS30H, Windows 98 SE 4.10.1998 32Mb P2, IrDA driver (Microsoft 5-11-1998)

[Thanks Jen!]

[] IBM ThinkPad T21, Windows 98 SE 4.10.2222 A 128Mb P3, IrDA driver (Microsoft 4-23-1999)

Workaround:

Disable the IrDA port under the Device Manager. The truly paranoid can place Insulation/PVC tape over the port to prevent abuse.

Recreate:

1. Startup laptops. In the test setup, the victim was running Windows, and the attacker was running GNU/Linux. The Linux kernel must have IrDA support compiled in.
2. Under GNU/Linux, make sure `irda-utils-0.9.10-9` is installed, other versions are untested, but will probably work too.
3. Do `"irattach /dev/ttyS1 -s"` or equivalent to activate the IrDA port.
4. Check the GNU/Linux side is working correctly by running the `"irdadump"` command. You should see repetitive output similar to:

```
07:28:17.790903 xid:cmd 4d274896 > ffffffff S=6 s=0 (14)
07:28:17.880849 xid:cmd 4d274896 > ffffffff S=6 s=1 (14)
07:28:17.970845 xid:cmd 4d274896 > ffffffff S=6 s=2 (14)
07:28:18.060858 xid:cmd 4d274896 > ffffffff S=6 s=3 (14)
07:28:18.150840 xid:cmd 4d274896 > ffffffff S=6 s=4 (14)
07:28:18.240861 xid:cmd 4d274896 > ffffffff S=6 s=5 (14)
07:28:18.330859 xid:cmd 4d274896 > ffffffff S=6 s=* rattusrattus hint=0400
[ Computer ] (28)
```

5. Place laptops so the infrared ports are aligned and within IrDA distance, `irdadump` should reflect new machine. The Windows machine should also respond, usually by making a sound.
6. Run `irdaping`. The destination address ("`0x4d274896`" for above example) is required, but actual value does not matter.
7. Victim machine should display the BSOD at this point and reboot.

Solution:

Microsoft has released a patch to address this issue:

Securiteam: [NT] IrDA Semi-Remote Vulnerability

<<http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS01-046.asp>>
<http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS01-046.asp>

ADDITIONAL INFORMATION

The information has been provided by <<mailto:paulm@astro.gla.ac.uk>> Paul Millar.

=====

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: "[NT] BadBlue File Viewing Vulnerability"
 - *Messages sorted by:* [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#) [\[attachment \]](#)