

[NEWS] Seti@home information leakage and remote compromise

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2003-04/0008.html>

From: support@securiteam.com

Date: 04/09/03

From: support@securiteam.com

To: list@securiteam.com

Date: 9 Apr 2003 22:51:31 +0200

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

In the US?

Contact Beyond Security at our new California office
housewarming rates on automated network vulnerability
scanning. We also welcome ISPs and other resellers!

Please contact us at: 323-882-8286 or ussales@beyondsecurity.com

Seti@home information leakage and remote compromise

SUMMARY

<<http://setiathome.berkeley.edu/>> SETI@home is a scientific experiment that uses Internet-connected computers in the Search for Extraterrestrial Intelligence (SETI). You can participate by running a free program that downloads and analyzes radio telescope data.

The SETI@home program is a special kind of screensaver. Like other screensavers it starts up when you leave your computer unattended, and it shuts down as soon as you return to work. What it does in the interim is unique.

There are currently over four million registered users of seti@home. Over half a million of these users are "active"; they have returned at least one result within the last four weeks.

Security vulnerabilities in the Seti@home application leak potentially sensitive information and also enable remote root compromise of the machines running seti@home.

DETAILS

Securiteam: [NEWS] Seti@home information leakage and remote compromise

Vulnerable versions:

All versions under 3.08

The seti@home clients use the HTTP protocol to download new work units, user information and to register new users. The implementation leaves two security vulnerabilities:

1) All information is sent in plaintext across the network. This information includes the processor type and the operating system of the machine seti@home is running on.

Sniffing the information exposed by the seti@home client is trivial and very useful to a malicious person planning an attack on a network. A passive scan of machines on a network can be made using any packet sniffer to grab the information from the network.

2) There is a buffer overflow in the server responds handler. Sending an overly large string followed by a newline ('\n') character to the client will trigger this overflow. This has been tested with various versions of the client. All versions are presumed to have this flaw in some form.

All tested clients have similar buffer overflows, which allowed setting eip to an arbitrary value which can lead to remote code execution. An attacker would have to reroute the connection the client tries to make to the seti@home webserver to a machine he or she controls. This can be done using various widely available spoofing tools. Seti@home also has the ability to use a HTTP-proxy, and an attacker could also use the machine the PROXY runs on as a base for this attack. Routers can also be used as a base for this attack.

3) A similar buffer overflow seems to affect the main seti@home server at shserver2.ssl.berkeley.edu. It closes the connection after receiving a too large string of bytes followed by a '\n'.

Exploitation of the bug in the server has not been tested. It should be note that a successful exploitation of the bug in the server would offer a platform from which all seti@home clients can be exploited.

Vendor status:

Vendor notified.

Several patches were released.

ADDITIONAL INFORMATION

Information provided by: Berend-Jan Wever

<mailto:SkyLined@edup.tudelft.nl> SkyLined@edup.tudelft.nl.

=====

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:

[NEWS] Seti@home information leakage and remote compromise

Securiteam: [NEWS] Seti@home information leakage and remote compromise

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.