

[NT] Buffer Overflow in AnalogX Proxy and NEC Socks5

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2002-07/0084.html>

From: support@securiteam.com

Date: 07/18/02

From: support@securiteam.com

To: list@securiteam.com

Date: Thu, 18 Jul 2002 22:44:13 +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.

Buffer Overflow in AnalogX Proxy and NEC Socks5

SUMMARY

A buffer overflow exists in AnalogX's Proxy and NEC's Socks5 software. Exploitation of this vulnerability allows remote execution of arbitrary code with the privileges of the Proxy daemon.

DETAILS

Vulnerable systems:

- * AnalogX Proxy v4.07 and previous version
- * NEC Socks5 version 1.0r11

Web Proxy Overflow

Sending a HTTP proxy request to the target system on TCP port 6588 consisting of a single space character followed by 320 or more non-space characters followed by 2 carriage-return linefeeds causes a read access violation in the application. Manually dismissing the application error message box that is displayed on the affected system at this point will terminate the process. If the message box is not manually dismissed then repeated sending of the request causes repeated access violation message boxes to appear on the affected system up to the point where the service no longer responds.

Securiteam: [NT] Buffer Overflow in AnalogX Proxy and NEC Socks5

Different number of bytes sent cause different error conditions to occur, such as write access violations and Watcom memory error dialogs to appear.

Socks4a Buffer Overflow

Sending a Sock4a request to the target system on TCP port 1080 consisting of a hostname section of 140 or more characters will cause a write access violation application error. Manually dismissing the application error message box that is displayed on the affected system at this point will terminate the process. If the message box is not manually dismissed then repeated sending of the request causes repeated access violation message boxes to appear on the affected system up to the point where the service no longer responds.

An example TCP packet to send is

```
\x04\x01\x04\x38\x00\x00\x00abcd\x00#\x00
```

Where the '\xxx' characters signify their corresponding HEX binary values and the '#' is substituted with the DNS name of 140 or more characters.

Note:

A similar problem affects NEC's Socks5 implementation.

Solution:

Refer to the vendor's web site for further details:

<<http://www.analogx.com>> <http://www.analogx.com>

ADDITIONAL INFORMATION

The information has been provided by <<mailto:robin.keir@foundstone.com>>
Robin Keir and <<mailto:3APA3A@SECURITY.NNOV.RU>> 3APA3A.

=====

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: "[EXPL] TrendMicro's VirusWall Space Gap (Exploit)"
 - **Messages sorted by:** [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#) [\[attachment \]](#)