

[VulnWatch] SRT2003-06-12-0853 – ike-scan local root format string issue

Source: <http://www.derkeiler.com/Mailing-Lists/VulnWatch/2003-06/0005.html>

From: KF (dotslash_at_snosoft.com)

Date: 06/13/03

Date: Thu, 12 Jun 2003 20:40:59 -0700

To: bugtraq@securityfocus.com

<http://www.secnetops.biz/research>

Secure Network Operations, Inc. <http://www.secnetops.com>

Strategic Reconnaissance Team research@secnetops.com

Team Lead Contact kf@secnetops.com

Our Mission:

Secure Network Operations offers expertise in Networking, Intrusion Detection Systems (IDS), Software Security Validation, and Corporate/Private Network Security. Our mission is to facilitate a secure and reliable Internet and inter-enterprise communications infrastructure through the products and services we offer.

Quick Summary:

Advisory Number : SRT2003-06-12-0853

Product : ike-scan

Version : 1.0 & 1.1

Vendor : <http://www.nta-monitor.com/ike-scan/>

Class : Local

Criticality : Low

Operating System(s) : *nix, cygwin

High Level Explanation

High Level Description : Local format string issue in logging functions

What to do : Please upgrade ike-scan to version 1.2

Technical Details

Proof Of Concept Status : Secure Network Operations does have PoC code

Low Level Description :

In the course of performing security assessments and penetration tests for their customers, <http://www.nta-monitor.com> has found that VPN systems often provide full access to the internal network which makes them tempting targets to an attacker.

In addition, many people assume that their VPN servers are invisible and impenetrable which is a dangerous assumption given that research at NTA shows that IPsec VPN systems can be discovered and the manufacturer identified.

When this potential for discovery and identification is combined with the fact that several VPN vulnerabilities have been reported in the past few months, it would seem to be only a matter of time before hackers start to target VPN systems.

With this in mind, NTA took the decision to raise awareness of this serious industry problem by producing a white paper on how VPN servers can be detected and identified, combined with the development of a security-auditing program "ike-scan."

The concepts behind ike-scan can be located in the following pdf. <http://www.nta-monitor.com/ike-scan/whitepaper.pdf>

In a default configuration ike-scan is not suid root. The suid bit is not set during the install. As an admin you may have been tricked by a user that was perhaps higher on the food chain than you and he really wanted to use ike-scan so you had to chmod +s /usr/local/bin/ike-scan for him. In other words there is potential for this to be exploited.

```
[root@Immunity root]# su - nobody
sh-2.05$ /usr/local/bin/ike-scan 127.0.0.1
ERROR: Could not bind UDP socket to local port 500
You need to be root, or ike-scan must be suid root to bind to ports below
1024.
Only one process may bind to a given port at any one time.
bind: Permission denied
```

Recently I started using (<http://www.wirex.com/shop/index.php/cPath/25>) Immunix 7+ from the Wirex folks and lets just say my night has been ruined a few times due to their products protection measures. As an example after compiling the new version of ike-scan to show how it was no longer exploitable, I found that I was unable to pop items off the stack as an example. If I were at work rather than home I would show the example however... FormatGuard kinda threw a wrench into that idea. =].

```
[root@Immunity ike-scan-1.1]# ./ike-scan %x
ike-scan[7372]: ImmunixOS format error – mismatch of 0 in syslog() called
by err_print
```

Even though I am the one finding the vulnerabilities, I certainly enjoy having Immunix tell me about the exact function being exploited when I run

the PoC code that was created for a non protected machine.

After ike-scan is updated to version 1.2 you should see the following in your system logs if someone were to attempt to exploit ike-scan.

```
Jun 12 20:32:11 Immunity ike-scan[8827]: Starting: /usr/local/bin/ike-scan %x
[root@Immunity ike-scan-1.2]# /usr/local/bin/ike-scan %x
gethostbyname: No such file or directory
```

If you were on a regular redhat 7.0 machine exploitation would be as follows.

```
[root@Immunity ike-scan-1.1]# head 0x82-eat_ike-scan.c
```

```
/*
**
** ike-scan local root exploit
** exploit by "you dong-hun"(Xpl017Elz), <szoahc@hotmail.com>.
** [x82@xpl017elz bin]$ ls -al ike-scan
** -rwsr-xr-x 1 root root 100554 Jun 2 06:23 ike-scan
** [x82@xpl017elz bin]$ ./0x82-eat_ike-scan
** [+] make /tmp/x82 code.
** [+] Auto Brute-force mode: gethostbyname: Success
** [+] Ok, exploited successfully.
** [+] It's shell !
** bash#
**
*/
```

Vendor Status : This issue was promptly addressed by the vendor fixes are available at <http://www.nta-monitor.com/ike-scan/download.htm>
Please upgrade to ike-scan 1.2.

Bugtraq URL : to be assigned

This advisory was released by Secure Network Operations, Inc. as a matter of notification to help administrators protect their networks against the described vulnerability. Exploit source code is no longer released in our advisories. Contact research@secnetops.com for information on how to obtain exploit information.