

[VulnWatch] Sustworks Unauthorized Network Monitoring and tcpflow format string attack

Source: <http://www.derkeiler.com/Mailing-Lists/VulnWatch/2003-08/0010.html>

From: _at_stake Advisories (_at_stake)

Date: 08/07/03

Date: Thu, 07 Aug 2003 15:35:53 -0400

To: vulnwatch@vulnwatch.org

-----BEGIN PGP SIGNED MESSAGE-----

Hash: SHA1

@stake, Inc.
www.atstake.com

Security Advisory

Advisory Name: Sustworks Unauthorized Network Monitoring and
tcpflow format string attack

Release Date: 08/07/2003

Application: IPNetMonitorX and IPNetSentryX

Platform: Mac OS X

Severity: Local users can sniff network traffic

Local users can become root

Author: Dave G. <daveg@atstake.com>

Vendor Status: Fix available

CVE Candidate: CVE candidate number applied for

Reference: www.atstake.com/research/advisories/2003/a080703-1.txt

Overview:

IPNetSentryX and IPNetMonitorX are network tools that provide firewalling and general network monitoring respectively. Both of these tools come with three helper tools that each have security issues associated with them. The first two tools: RunTCPDump and RunTCPFlow allow arbitrary users to monitor the network without requiring any form of authentication or privilege. The third tool, tcpflow (executed by RunTCPFlow), contains a format string vulnerability, allowing arbitrary commands to be run as the user calling the program. Since RunTCPFlow is setuid root and will pass arguments to tcpflow, we can execute arbitrary commands as root.

Details:

VulnWatch: [VulnWatch] Sustworks Unauthorized Network Monitoring and tcpflow format string attack

RunTCPDump and RunTCPFlow are setuid root helper applications that simply execute `/usr/sbin/tcpdump` and `/usr/local/bin/tcpflow`. These helper applications pass all arguments to the commands they are executing, allowing users to execute `tcpdump` and `tcpflow` however they choose. Unfortunately, any user with interactive access to a Mac OS X system with IPNetSentryX or IPNetMonitorX can run these commands. This allows any user on the system to be able to view all network traffic that pass through the vulnerable system.

For example:

```
bash-2.05a$ id
uid=503(dummy) gid=20(staff) groups=20(staff)
bash-2.05a$ pwd
/Applications/IPNetSentryX.app/Contents/Resources
bash-2.05a$ ./RunTCPDump -i en1 -x -v -s 4096
RunTCPDump: listening on en1
18:02:55.726143 arp who-has 192.168.0.1 tell 192.168.0.1
                0001 0800 0604 0001 XXXX XXXX XXXX XXXX
                0001 0000 0000 0000 c0a8 0001 0000 0000
                0000 0000 0000 0000 0000 0000 0000
```

Additionally, `tcpflow` is vulnerable to a format string vulnerability, which normally would not be a serious security vulnerability. However, since any user on a system that has IPNetSentryX or IPNetMonitorX and `tcpflow` installed can cause `tcpflow` to be executed as root via `RunTCPFlow`, an attacker can use this vulnerability to become root. A corresponding @stake advisory (a080703-2) has been released on the `tcpflow` format string attack.

Vendor Response:

These vulnerabilities are mitigated in the latest version of IPNetSentryX and IPNetMonitorX available from <http://www.sustworks.com>. Mitigation strategies include stronger input validation and access control to `RunTCPDump` and `RunTCPFlow`.

Recommendation:

Upgrade to the latest version of IPNetSentryX and `tcpflow`.

Common Vulnerabilities and Exposures (CVE) Information:

The Common Vulnerabilities and Exposures (CVE) project has assigned the following names to these issues. These are candidates for inclusion in the CVE list (<http://cve.mitre.org>), which standardizes names for security problems.

CVE candidate number applied for

VulnWatch: [VulnWatch] Sustworks Unauthorized Network Monitoring and tcpflow format string attack

@stake Vulnerability Reporting Policy:
<http://www.atstake.com/research/policy/>

@stake Advisory Archive:
<http://www.atstake.com/research/advisories/>

PGP Key:
http://www.atstake.com/research/pgp_key.asc

@stake is currently seeking application security experts to fill several consulting positions. Applicants should have strong application development skills and be able to perform application security design reviews, code reviews, and application penetration testing. Please send resumes to jobs@atstake.com.

Copyright 2003 @stake, Inc. All rights reserved.

-----BEGIN PGP SIGNATURE-----

Version: PGP 8.0

iQA/AwUBPzKp50e9kNifAm4yEQLzUACg8NWt5xklZb72A+1x9b/a9FVC7YcAn0qp
+za7wOpXnQ6cmqlu3gEkm5ae
=sYTv

-----END PGP SIGNATURE-----