Alpine Linux - Bug #6812

Bug # 6811 (Closed): tcpdump: Multiple vulnerabilities (Various CVEs)

[3.5] tcpdump: Multiple vulnerabilities (Various CVEs)

02/05/2017 08:51 AM - Alicha CH

Status:	Closed	**Start date:**	02/05/2017
Priority:	Normal	**Due date:**	
Assignee:	Natanael Copa	**% Done:**	100%
Category:	Security	**Estimated time:**	0.00 hour
Target version:	3.5.2		
Affected versions:		**Security IDs:**	

Description

CVE-2016-7922 (arbitrary code execution)

The AH parser in tcpdump before 4.9.0 has a buffer overflow in print-ah.c:ah_print().

CVE-2016-7923 (arbitrary code execution)

The ARP parser in tcpdump before 4.9.0 has a buffer overflow in print-arp.c:arp_print().

CVE-2016-7924 (arbitrary code execution)

The ATM parser in tcpdump before 4.9.0 has a buffer overflow in print-atm.c:oam_print().

CVE-2016-7925 (arbitrary code execution)

The compressed SLIP parser in tcpdump before 4.9.0 has a buffer overflow in print-sl.c:sl_if_print().

CVE-2016-7926 (arbitrary code execution)

The Ethernet parser in tcpdump before 4.9.0 has a buffer overflow in print-ether.c:ethertype_print().

CVE-2016-7927 (arbitrary code execution)

The IEEE 802.11 parser in tcpdump before 4.9.0 has a buffer overflow in print-802_11.c:ieee802_11_radio_print().

CVE-2016-7928 (arbitrary code execution)

The IPComp parser in tcpdump before 4.9.0 has a buffer overflow in print-ipcomp.c:ipcomp_print().

CVE-2016-7929 (arbitrary code execution)

The Juniper PPPoE ATM parser in tcpdump before 4.9.0 has a buffer overflow in print-juniper.c:juniper_parse_header().

CVE-2016-7930 (arbitrary code execution)

The LLC/SNAP parser in tcpdump before 4.9.0 has a buffer overflow in print-llc.c:llc_print().

CVE-2016-7931 (arbitrary code execution)

The MPLS parser in tcpdump before 4.9.0 has a buffer overflow in print-mpls.c:mpls_print().

CVE-2016-7932 (arbitrary code execution)

The PIM parser in tcpdump before 4.9.0 has a buffer overflow in print-pim.c:pimv2_check_checksum().

CVE-2016-7933 (arbitrary code execution)

The PPP parser in tcpdump before 4.9.0 has a buffer overflow in print-ppp.c:ppp_hdlc_if_print().

CVE-2016-7934 (arbitrary code execution)

The RTCP parser in tcpdump before 4.9.0 has a buffer overflow in print-udp.c:rtcp_print().

CVE-2016-7935 (arbitrary code execution)

The RTP parser in tcpdump before 4.9.0 has a buffer overflow in print-udp.c:rtp_print().

CVE-2016-7936 (arbitrary code execution)

The UDP parser in tcpdump before 4.9.0 has a buffer overflow in print-udp.c:udp_print().

CVE-2016-7937 (arbitrary code execution)

The VAT parser in tcpdump before 4.9.0 has a buffer overflow in print-udp.c:vat_print().

CVE-2016-7938 (arbitrary code execution)

The ZeroMQ parser in tcpdump before 4.9.0 has an integer overflow in print-zeromq.c:zmtp1_print_frame().

CVE-2016-7939 (arbitrary code execution)

The GRE parser in tcpdump before 4.9.0 has a buffer overflow in print-gre.c, multiple functions.

CVE-2016-7940 (arbitrary code execution)

The STP parser in tcpdump before 4.9.0 has a buffer overflow in print-stp.c, multiple functions.

CVE-2016-7973 (arbitrary code execution)

The AppleTalk parser in tcpdump before 4.9.0 has a buffer overflow in print-atalk.c, multiple functions.

CVE-2016-7974 (arbitrary code execution)

The IP parser in tcpdump before 4.9.0 has a buffer overflow in print-ip.c, multiple functions.

CVE-2016-7975 (arbitrary code execution)

The TCP parser in tcpdump before 4.9.0 has a buffer overflow in print-tcp.c:tcp_print().

CVE-2016-7983 (arbitrary code execution)

The BOOTP parser in tcpdump before 4.9.0 has a buffer overflow in print-bootp.c:bootp_print().

CVE-2016-7984 (arbitrary code execution)

The TFTP parser in tcpdump before 4.9.0 has a buffer overflow in print-tftp.c:tftp_print().

CVE-2016-7985 (arbitrary code execution)

The CALM FAST parser in tcpdump before 4.9.0 has a buffer overflow in print-calm-fast.c:calm_fast_print().

CVE-2016-7986 (arbitrary code execution)

The GeoNetworking parser in tcpdump before 4.9.0 has a buffer overflow in print-geonet.c, multiple functions.

CVE-2016-7992 (arbitrary code execution)

The Classical IP over ATM parser in tcpdump before 4.9.0 has a buffer overflow in print-cip.c:cip_if_print().

CVE-2016-7993 (arbitrary code execution)

A bug in util-print.c:relts_print() in tcpdump before 4.9.0 could cause a buffer overflow in multiple protocol parsers (DNS, DVMRP, HSRP, IGMP, lightweight resolver protocol, PIM).

CVE-2016-8574 (arbitrary code execution)

The FRF.15 parser in tcpdump before 4.9.0 has a buffer overflow in print-fr.c:frf15_print().

CVE-2016-8575 (arbitrary code execution)

The Q.933 parser in tcpdump before 4.9.0 has a buffer overflow in print-fr.c:q933_print(), a different vulnerability than CVE-2017-5482.

CVE-2017-5202 (arbitrary code execution)

The ISO CLNS parser in tcpdump before 4.9.0 has a buffer overflow in print-isoclns.c:clnp_print().

CVE-2017-5203 (arbitrary code execution)

The BOOTP parser in tcpdump before 4.9.0 has a buffer overflow in print-bootp.c:bootp_print().

CVE-2017-5204 (arbitrary code execution)

The IPv6 parser in tcpdump before 4.9.0 has a buffer overflow in print-ip6.c:ip6_print().

CVE-2017-5205 (arbitrary code execution)

The ISAKMP parser in tcpdump before 4.9.0 has a buffer overflow in print-isakmp.c:ikev2_e_print().

CVE-2017-5341 (arbitrary code execution)

The OTV parser in tcpdump before 4.9.0 has a buffer overflow in print-otv.c:otv_print().

CVE-2017-5342 (arbitrary code execution)

In tcpdump before 4.9.0, a bug in multiple protocol parsers (Geneve, GRE, NSH, OTV, VXLAN and VXLAN GPE) could cause a buffer overflow in print-ether.c:ether_print().

CVE-2017-5482 (arbitrary code execution)

The Q.933 parser in tcpdump before 4.9.0 has a buffer overflow in print-fr.c:q933_print(), a different vulnerability than CVE-2016-8575.

CVE-2017-5483 (arbitrary code execution)

The SNMP parser in tcpdump before 4.9.0 has a buffer overflow in print-snmp.c:asn1_parse().

CVE-2017-5484 (arbitrary code execution)

The ATM parser in tcpdump before 4.9.0 has a buffer overflow in print-atm.c:sig_print().

CVE-2017-5485 (arbitrary code execution)

The ISO CLNS parser in tcpdump before 4.9.0 has a buffer overflow in addrtoname.c:lookup_nsap().

CVE-2017-5486 (arbitrary code execution)

The ISO CLNS parser in tcpdump before 4.9.0 has a buffer overflow in print-isoclns.c:clnp_print().

References:

http://www.tcpdump.org/tcpdump-changes.txt
https://marc.info/?l=oss-security&m=148576949320709&w=2

Associated revisions

Revision 889fe674 - 02/07/2017 08:06 AM - Sergei Lukin

main/tcpdump: security upgrade to 4.9.0 - fixes #6812

CVE-2016-7922 (arbitrary code execution)
CVE-2016-7923 (arbitrary code execution)
CVE-2016-7924 (arbitrary code execution)
CVE-2016-7925 (arbitrary code execution)
CVE-2016-7926 (arbitrary code execution)
CVE-2016-7927 (arbitrary code execution)
CVE-2016-7928 (arbitrary code execution)
CVE-2016-7929 (arbitrary code execution)
CVE-2016-7930 (arbitrary code execution)
CVE-2016-7931 (arbitrary code execution)
CVE-2016-7932 (arbitrary code execution)
CVE-2016-7933 (arbitrary code execution)
CVE-2016-7934 (arbitrary code execution)
CVE-2016-7935 (arbitrary code execution)
CVE-2016-7936 (arbitrary code execution)
CVE-2016-7937 (arbitrary code execution)
CVE-2016-7938 (arbitrary code execution)
CVE-2016-7939 (arbitrary code execution)
CVE-2016-7940 (arbitrary code execution)
CVE-2016-7973 (arbitrary code execution)
CVE-2016-7974 (arbitrary code execution)
CVE-2016-7975 (arbitrary code execution)
CVE-2016-7983 (arbitrary code execution)
CVE-2016-7984 (arbitrary code execution)
CVE-2016-7985 (arbitrary code execution)
CVE-2016-7986 (arbitrary code execution)
CVE-2016-7992 (arbitrary code execution)

CVE-2016-7993 (arbitrary code execution)
CVE-2016-8574 (arbitrary code execution)
CVE-2016-8575 (arbitrary code execution)
CVE-2017-5202 (arbitrary code execution)
CVE-2017-5203 (arbitrary code execution)
CVE-2017-5204 (arbitrary code execution)
CVE-2017-5205 (arbitrary code execution)
CVE-2017-5341 (arbitrary code execution)
CVE-2017-5342 (arbitrary code execution)
CVE-2017-5482 (arbitrary code execution)
CVE-2017-5483 (arbitrary code execution)
CVE-2017-5484 (arbitrary code execution)
CVE-2017-5485 (arbitrary code execution)
CVE-2017-5486 (arbitrary code execution)

History

#1 - 02/07/2017 08:06 AM - Sergei Lukin

- Status changed from New to Resolved

- % Done changed from 0 to 100

Applied in changeset alpine:889fe674354b8ffbce03fdbfb24f5b03f1520291.

#2 - 02/09/2017 10:58 AM - Alicha CH

- Category set to Security

- Status changed from Resolved to Closed