Multiple TCPdump vulnerabilities in HiOS, Classic and OWL products

Date: July 27, 2018
Version: 1.0

Summary

The following vulnerabilities affect the TCPdump functionality in one or more versions of the products listed in the next section:

ID	Title / Description	Severity
CVE-2017-12894	Several protocol parsers in tcpdump before 4.9.2 could cause a buffer over-read in addrtoname.c:lookup_bytestring().	CVSSv3.0: 7.5 (*)
CVE-2017-12988	The telnet parser in tcpdump before 4.9.2 has a buffer over-read in print-telnet.c:telnet_parse().	
CVE-2017-12996	The PIMv2 parser in tcpdump before 4.9.2 has a buffer over-read in print-pim.c:pimv2_print().	
CVE-2017-13012	The ICMP parser in tcpdump before 4.9.2 has a buffer over-read in print-icmp.c:icmp_print().	
CVE-2017-13013	The ARP parser in tcpdump before 4.9.2 has a buffer over-read in print-arp.c, several functions.	
CVE-2017-13022	The IP parser in tcpdump before 4.9.2 has a buffer over-read in print-ip.c:ip_printroute().	
CVE-2017-13030	The PIM parser in tcpdump before 4.9.2 has a buffer over-read in print-pim.c, several functions.	
CVE-2017-13037	The IP parser in tcpdump before 4.9.2 has a buffer over-read in print-ip.c:ip_printts().	
CVE-2016-7923	The ARP parser in tcpdump before 4.9.0 has a buffer overflow in print-arp.c:arp_print().	
CVE-2016-7926	The Ethernet parser in tcpdump before 4.9.0 has a buffer overflow in print-ether.c:ethertype_print().	
CVE-2016-7932	The PIM parser in tcpdump before 4.9.0 has a buffer overflow in print-pim.c:pimv2_check_checksum().	
CVE-2016-7936	The UDP parser in tcpdump before 4.9.0 has a buffer overflow in print-udp.c:udp_print().	
CVE-2016-7974	The IP parser in tcpdump before 4.9.0 has a buffer overflow in print-ip.c, multiple functions.	
CVE-2016-7975	The TCP parser in tcpdump before 4.9.0 has a buffer overflow in print-tcp.c:tcp_print().	
CVE-2016-7983	The BOOTP parser in tcpdump before 4.9.0 has a buffer overflow in print-bootp.c:bootp_print().	
CVE-2016-7984	The TFTP parser in tcpdump before 4.9.0 has a buffer overflow in print-tftp.c:tftp_print().	

(*) The CVSS score deviates from the official CVE score because all vulnerabilities can only be exploited during an active user initiated TCPdump session and for network traffic that is directed to the management of the device. The TCPdump functionality is inactive per default.

Impact

These vulnerabilities might result in denial of service or the execution of arbitrary code.

Affected Products

Brand	Product Line / Platform	Product	Version
Hirschmann	HiOS	RSP, RSPE, RSPS, RSPL, MSP, EES, EESX, GRS, OS, RED	07.0.00 and lower
	Classic	RS, RSR, RSB, MACH100, MACH1000, MACH4000, MS, OCTOPUS	All
	Cellular Router	OWL	01.2.02 and lower

Solution

Customers are advised to update their products or to follow the workaround instructions.

Available Updates:

Brand	Product Line / Platform	Product	Version
Hirschmann	HiOS	RSP, RSPE, RSPS, RSPL, MSP, EES, EESX, GRS, OS, RED	07.0.01
	Classic	RS, RSR, RSB, MACH100, MACH1000, MACH4000, MS, OCTOPUS	No fix planned
	Cellular Router	OWL LTE M12	01.2.03
		OWL LTE, OWL 3G	Fix planned for 02.0.00

Available workaround:
Use the "-w" option (“debug tcpdump start cpu parms -w” command for HiOS and Classic) to write raw packets into a PCAP file and analyze the file with a PCAP file viewer. For this use case the protocol decoding subsystem will not be used and the vulnerable source code is not executed.

For Help or Feedback

To view all Belden Security Advisories and Bulletins or to report suspected security vulnerabilities, go to https://www.belden.com/security.
For technical support and other requests, please visit https://hirschmann-support.belden.com.

Disclaimer

Revisions

V1.0 (July 27, 2018): Bulletin created.