20675 Manhattan Place
Torrance, CA 90501. USA
www.trendnet.com

Tel: (310) 961-5500
Fax: (310) 961-5511
support@trendnet.com

SUPPORT TICKET # 238145

Submitted: 3/2/2020 7:12:05 AM

Contact Information			
Company:		**Customer ID:**	
Name:		**Email:**	kuc822@psu.edu
Address:		**City:**	
State:		**Country:**	
Zipcode:		**Phone:**	

Support Ticket Status

Status:	Closed — Your Helpdesk Request has been closed due to no response after 2 weeks
Assigned to:	Albert M.
Submitted on:	3/2/2020 7:12:05 AM
Last Updated:	3/23/2020 8:39:06 AM

Support Ticket Info

Model Number:	TEW-827DRU
Version:	v2.0R
Operating System:	Linux
Serial Number:	
Firmware Version:	2.06B04
Issue Category:	Issue Category: Other

Issue:	Hi Trendnet support team, We have found multiple unknown vulnerabilities in the Trendnet product and we inform you as soon as possible by email. The following is the detail information about these vulnerabilities. Vulnerability-1: (command injection) TRENDnet TEW-827DRU with firmware up to and including 2.06B04 contains a command injection in apply.cgi via the action kick_ban_wifi_mac_allow with the key qcawifi.wifi0_vap0.maclist, allowing an authenticated user to run arbitrary commands on the device. Vulnerability-2: (stack overflow) TRENDnet TEW-827DRU with firmware up to and including 2.06B04 contains a stack-based buffer overflow in the ssi binary. The overflow allows an authenticated user to execute arbitrary code by POSTing to apply.cgi via the action kick_ban_wifi_mac_allow with a sufficiently long key qcawifi.wifi0_vap0.maclist. Vulnerability-3: (command injection) TRENDnet TEW-827DRU with firmware up to and including 2.06B04 contains a command injection in apply.cgi via the action kick_ban_wifi_mac_deny with the key qcawifi.wifi0_vap0.maclist, allowing an authenticated user to run arbitrary commands on the device. Vulnerability-4: (stack overflow) TRENDnet TEW-827DRU with firmware up to and including 2.06B04 contains a stack-based buffer overflow in the ssi binary. The overflow allows an authenticated user to execute arbitrary code by POSTing to apply.cgi via the action kick_ban_wifi_mac_deny with a sufficiently long key qcawifi.wifi0_vap0.maclist. Thanks and look forward to your reply. There are no attachments
Notes:	3/2/2020 11:56:59 AM - Albert M. (Technical Support Rep) Hi, Thank you for your feedback. I will forward this to our product management team for further review and i will follow up with you as soon as i get an update. 3/8/2020 3:13:16 PM - Hi Trendnet support team, I have attached detail information about the issue. Attachments View kick_ban_wifi_mac_deny_overflow.pdf View kick_ban_wifi_mac_deny_command.pdf View kick_ban_wifi_mac_allow_overflow.pdf View kick_ban_wifi_mac_allow_command.pdf
Resolution:	Helpdesk Request closed because there has been no response for over 2 weeks

Print Close