

SUPPORT TICKET # 238144

Submitted: 3/2/2020 7:08:49 AM

Contact Information			
Company:		Customer ID:	
Name:		Email:	<a href="mailto:kuc822@psu.edu">kuc822@psu.edu</a>
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 7:08:49 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

<b>Issue:</b>	<p>Hi Trendnet support team,</p> <p>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.</p> <p>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 st_dev_connect with the key "wan_type", allowing an authenticated user to run arbitrary commands on the device.</p> <p>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 st_dev_connect with a sufficiently long key "wan_type".</p> <p>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 st_dev_disconnect with the key "wan_type", allowing an authenticated user to run arbitrary commands on the device.</p> <p>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 st_dev_disconnect with a sufficiently long key "wan_type".</p> <p>Vulnerability-5: (command injection) TRENDnet TEW-827DRU with firmware up to and including 2.06B04 contains multiple command injections in apply.cgi via the action st_dev_rconnect with the key "wan_type", allowing an authenticated user to run arbitrary commands on the device.</p> <p>Vulnerability-6: (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 st_dev_rconnect with a sufficiently long key "wan_type".</p> <p>Thanks and look forward to your reply.</p> <p>There are no attachments</p>
<b>Notes:</b>	<p>3/2/2020 11:56:18 AM - Albert M. (Technical Support Rep) Hi,</p> <p>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.</p> <p>3/8/2020 3:14:33 PM - Hi Trendnet support team,</p> <p>I have attached detail information about the issue.</p> <p><u>Attachments</u> <a href="#">View</a> st_dev_rconnect_overflow.pdf <a href="#">View</a> st_dev_rconnect_command.pdf <a href="#">View</a> st_dev_disconnect_overflow.pdf <a href="#">View</a> st_dev_disconnect_command.pdf <a href="#">View</a> st_dev_connect_overflow.pdf <a href="#">View</a> st_dev_connect_command.pdf</p>

Resolution:	Helpdesk Request closed because there has been no response for over 2 weeks
-------------	---

Print

Close