20675 Manhattan Place
Torrance, CA 90501. USA
www.trendnet.com
Tel: (310) 961-5500
Fax: (310) 961-5511
support@trendnet.com

SUPPORT TICKET # 251187

Submitted: 9/11/2022 5:24:15 AM

Contact Information			
Company:		**Customer ID:**	
Name:		**Email:**	cyeaa@connect.ust.hk
Address:		**City:**	
State:		**Country:**	
Zipcode:		**Phone:**	

Support Ticket Status

Status:	Worked On — Your Helpdesk Request is being worked on
Assigned to:	Sonny S
Submitted on:	9/11/2022 5:24:15 AM
Last Updated:	9/29/2022 11:19:28 AM

Support Ticket Info

Model Number:	TEW-755AP
Version:	v1.0R
Operating System:	Linux
Serial Number:	
Firmware Version:	TEW755AP-FW113B01.bin
Issue Category:	Issue Category: Other
Issue:	Hi, We have found 3 vulnerabilities in TEW-755AP router (firmware version: 1.13B01) and at the first time we email to you. The detailed information is put in the attachment. Vulnerability 1: The www/cgi/ssi in the TEW-755AP router (firmware version: 1.13B01) has several NULL Pointer Dereference vulnerabilities in function 0x424AE4 . It can be triggered by sending POST request to secmark1524.cgi without some required keys in post data. Vulnerability 2: The www/cgi/ssi in the TEW-755AP router (firmware version: 1.13B01) has a possible logical bug at address

	0x43DA28. A null pointer is assign to a variable again in the null check branch. If exploited could result in NULL Pointer Dereference and crash. Vulnerability 3: The www/cgi/ssi in the TEW-755AP router (firmware version: 1.13B01) has several NULL Pointer Dereference vulnerabilities in function do_get_trx, null pointer argument is directly passed to function strtok and strcmp, if exploited can crash the program. We have constructed PoC and tested some of them on the latest firmware. Looking forward to your reply. View Vul1.pdf View Vul2.pdf View Vul3.pdf
Notes:	9/15/2022 3:59:02 PM - Sonny S (Technical Support Rep) Tech Support Rep Change: Mukilan G. ⇒ Sonny S Dear Customer, We are reviewing your report and expect to have the result by September 22. regards, Sonny 9/23/2022 9:19:24 AM - Sonny S (Technical Support Rep) Hi Ye, We are still working on this and expect to have the result 9/26. regards, Sonny 9/26/2022 3:21:54 PM - Sonny S (Technical Support Rep) Hi Ye, We have confirmed the three vulnerabilities and are working on the firmware. The fix is not an easy one, we estimate to have the new firmware toward the end of December 2022. If you are planning on publishing these vulnerabilities before our firmware fix, please let me know. regards, Sonny 9/29/2022 11:19:28 AM - Sonny S (Technical Support Rep) Hi Ye, We currently do not have a procedure to apply CVE, so if you are familiar with the CVE application, please apply one for each vulnerability and let me know the ID numbers. If possible, please use my name, today's date, and TRENDnet helpdesk as the confirmation instead of the ticket number. But, if it is easier for you to track, it is okay to use the ticket number. I will push the Engineer to try to release the firmware early and post the status here. regards, Sonny 9/12/2022 4:15:49 PM - Mukilan G. (Technical Support Rep) Dear Customer,

Thank you for notifying us with your detailed update. We will check with our resources to isolate it and will update you ASAP.

Regards,
TRENDnet Customer Service

9/13/2022 9:17:10 AM - Mukilan G. (Technical Support Rep)
Dear Customer,

Thank you for your feedback, we have forwarded it our team for review and and will update you ASAP.

Regards,
TRENDnet Customer Service

9/23/2022 8:47:54 AM -
If you need any further help please let me know.

Regards,
Ye

9/29/2022 1:08:45 AM -
Thanks so much for the confirmation! We would like to apply CVE ID for these bugs in these days, may I ask could I use this ticket as the confirmation? We will not disclose the detail of these bugs (like poc) until it's fixed.

Thanks again,
Ye

Print Close