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

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

SUPPORT TICKET # 243638

Submitted: 1/4/2021 8:46:19 AM

Contact Information

Company:		**Customer ID:**	
Name:		**Email:**	1096290054@qq.com
Address:		**City:**	
State:		**Country:**	
Zipcode:		**Phone:**	

Support Ticket Status

Status:	Closed — Your Helpdesk Request has been closed with a resolution
Assigned to:	Johnny H.
Submitted on:	1/4/2021 8:46:19 AM
Last Updated:	3/2/2021 9:27:25 AM

Support Ticket Info

Model Number:	TEW-755AP2KAC
Version:	v1.0R
Operating System:	Linux
Serial Number:	
Firmware Version:	
Issue Category:	Issue Category: Other

Issue:

Hi,

We have found six vulnerabilities in several Trendnet products and at the first time we email to you. The detail information and PoCs are put in the attachment.

Vulnerability 1:

The www/cgi/ssi in the TEW-755AP router (firmware version: 1.11B03) has a logic bug at address 0x40dcd0 when calling fprintf with "%s: key len = %d, too long\n" format. The two variables seem to be put in the wrong order. The vulnerability could be triggered by sending the POST request to apply_cgi with a long and unknown key in the request body.

Vulnerability 2:

The www/cgi/ssi in TEW-755AP router (firmware version: 1.11B03) has a NULL pointer dereference vulnerability. It could be triggered by sending the POST request to apply_cgi with unknown action name.

Vulnerability 3:

The www/cgi/ssi in TEW-755AP router (firmware version: 1.11B03) has a NULL pointer dereference vulnerability. It could be triggered by sending the POST request to apply_cgi via action ping_test without ping_ipaddr key.

Vulnerability 4:

The www/cgi/ssi in TEW-755AP router (firmware version: 1.11B03) has a NULL pointer dereference vulnerability. It could be triggered by sending the POST request to apply_cgi via action 'lang' without language key.

Vulnerability 5:

The www/cgi/ssi in TEW-755AP router (firmware version: 1.11B03) has a NULL pointer dereference vulnerability. It could be triggered by sending the POST request to apply_cgi via action 'do_graph_auth' without session_id key.

Vulnerability 6:

The www/cgi/ssi in TEW-755AP router (firmware version: 1.11B03) has a NULL pointer dereference vulnerability. It could be triggered by sending the POST request to apply_cgi via action 'do_graph_auth' without login_name key.

We have tested them successfully on latest firmware version 1.11B03 of TEW-755AP2KAC, TEW-821DAP2KAC and TEW-825DAP. We did not test latest version of TEW-827DRU, but we think the issue may exists in it.

Looking forward to your reply.

Thanks,

Yaowen

View vulnerability report-3.pdf

Notes:

1/8/2021 8:03:49 AM - Johnny H. (Technical Support Rep)
Hello,

I received the following update.

The engineer checked and claims these vulnerabilities do not exist in the GUI based on their testing. The are claiming that the GUI will defend against abnormal POST as noted in the customer report. See attached screen shot.

Attachments
View 755dap.png
1/4/2021 3:39:25 PM - Johnny H. (Technical Support Rep)
Hello,

Thank you for the information. I have forwarded this to our product management team for further review. I will follow up with you as soon as i get an update.

1/11/2021 9:53:01 AM - Johnny H. (Technical Support Rep)
Hello,

Thank yo for your feedback. I will pass this along to our product management team for further review.

2/10/2021 1:16:58 PM - Johnny H. (Technical Support Rep)
Hello,

We apologize for the inconvenience. We should have a Beta firmware available by the end of the month, first week of March. Once i get another update i will follow up with you.

3/1/2021 8:37:34 AM - Johnny H. (Technical Support Rep)
Hello,

Below is the link to the beta firmware.

http://Hytekcloud.quickconnect.to/d/f/606581498813921874

Please let me know if it helps resolve your issue.

3/2/2021 9:27:25 AM - Johnny H. (Technical Support Rep)
Hello,

Thank you and we appreciate the feedback. I will update our product management team.

1/8/2021 7:50:54 PM -
Hello,

Thanks for your response.

According to the feedback, I have tried them again in the GUI based testing, but it seems that these problems still exist.

As the screenshot shows, the server indeed works well since the long strings are put in the 'Value' part. (Shown in 755ap_normal.png)

However, it may incur the crash if we put the long strings in the 'Name' part. (Shown in 755ap_crash.png)

Attachments
View 755ap_crash.png
View 755ap_normal.png
2/9/2021 11:24:03 PM -
Hello,

Is there any update for the reported vulnerabilities.

Thanks

3/1/2021 8:44:07 PM -
Yes, the beta firmware has solved these issues.

Print Close