发件人: TRENDnet Support <helpdesk@trendnet.com>
发送时间: 2020年2月24日星期一 12:48
收件人:
主题: TRENDnet Helpdesk Ticket #238052 Updated

Your Helpdesk Ticket needs attention. A TRENDnet Support Rep has requested additional information in order to resolve your Helpdesk Ticket . The latest information is highlighted in yellow. Note, Helpdesk Ticket with no response for over 2 weeks will be automatically closed.

Note: Please do not reply to this email, this is an autoresponse. Replies to this email will not be addressed. Update your Helpdesk Ticket at https://www.trendnet.com/support/helpdesk/view-helpdesk-ticket.asp?id=238052. You may need to login to your Helpdesk Ticket account.

TRENDnet Helpdesk Ticket

Helpdesk Ticket # 238052
Submitted: 2/24/2020 8:19:08 AM

Contact Info

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

Helpdesk Ticket Status

Status:	Worked On — Your Helpdesk Request is being worked on
Assigned to:	Albert M.
Submitted on:	2/24/2020 8:19:08 AM
Last Updated:	2/24/2020 9:46:48 AM

Helpdesk Ticket Info

Model Number:	TEW-632BRP
Version:	A1.0R
Operating System:	Linux
Serial Number:	N/A
Firmware Version:	1.010B32
Issue Category:	Other
Issue:	Hi Trendnet support team, We have found three unknown vulnerabilities in Trendnet product and we inform you as soon as possible by email. The following are the detail information about these vulnerabilities. Vulnerability 1: Description: TRENDnet TEW-632BRP v1.010B32 devices have an OS command injection vulnerability in the CGI interface "dns_query.cgi", which allows remote attackers to execute arbitrary commands via parameter "dns_query_name" passed to the "dns_query.cgi" binary through a POST request. Vulnerability 2: Description: TRENDnet TEW-632BRP v1.010B32 devices have an OS command injection vulnerability in the CGI interface "system_time.cgi", which allows remote attackers to execute arbitrary commands

	via parameter "date" passed to the "system_time.cgi" binary through a POST request. Vulnerability 3: Description: TRENDnet TEW-632BRP v1.010B32 dev ices have an OS command injection vulnerability in the CGI interface "set_sta_enrollee_pin.cgi", which allows remote attackers to execute arbitrary commands via parameter "wps_sta_enrollee_pin" passed to the "set_sta_enrollee_pin.cgi" binary through a POST request. Thanks and look forward to your reply. Attachments There are no attachments
Notes:	**2/24/2020 9:46:48 AM** **Albert M.** **(Technical Support Rep)** Hi, Thank you for your feedback. Unfortunately, this product has been discontinued since 2008 and there will no longer be any firmware updates for this product.