TrendNet 823 dru 漏洞分析

Stack Buffer Overflow

0x1 sbo in function ping_test

Affected components

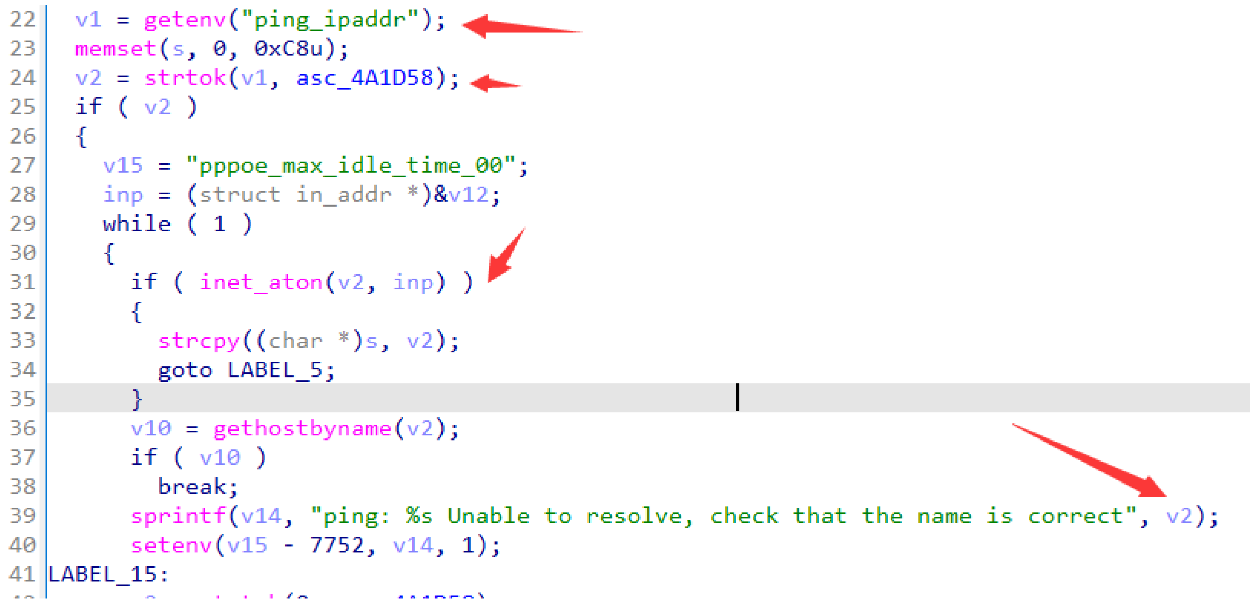
binary ssi in firmware

Attack vector

A user in the router's network can exploit the device by sending malicious http requests

Description

TRENDnet TEW-823DRU with firmware up to and including 1.02B01 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 ping_test with a sufficiently long key ping_ipaddr.



```
  v1 = getenv("ping_ipaddr");
  memset(s, 0, 0xC8u);
  v2 = strtok(v1, asc_4A1D58);
  if ( v2 )
  {
    v15 = "pppoe_max_idle_time_00";
    inp = (struct in_addr *)&v12;
    while ( 1 )
    {
      if ( inet_aton(v2, inp) )
      {
        strcpy((char *)s, v2);
        goto LABEL_5;
      }
      v10 = gethostbyname(v2);
      if ( v10 )
        break;
      sprintf(v14, "ping: %s Unable to resolve, check that the name is correct", v2);
      setenv(v15 - 7752, v14, 1);
LABEL_15:
```

0x2 sbo in function ping6_test

Affected components

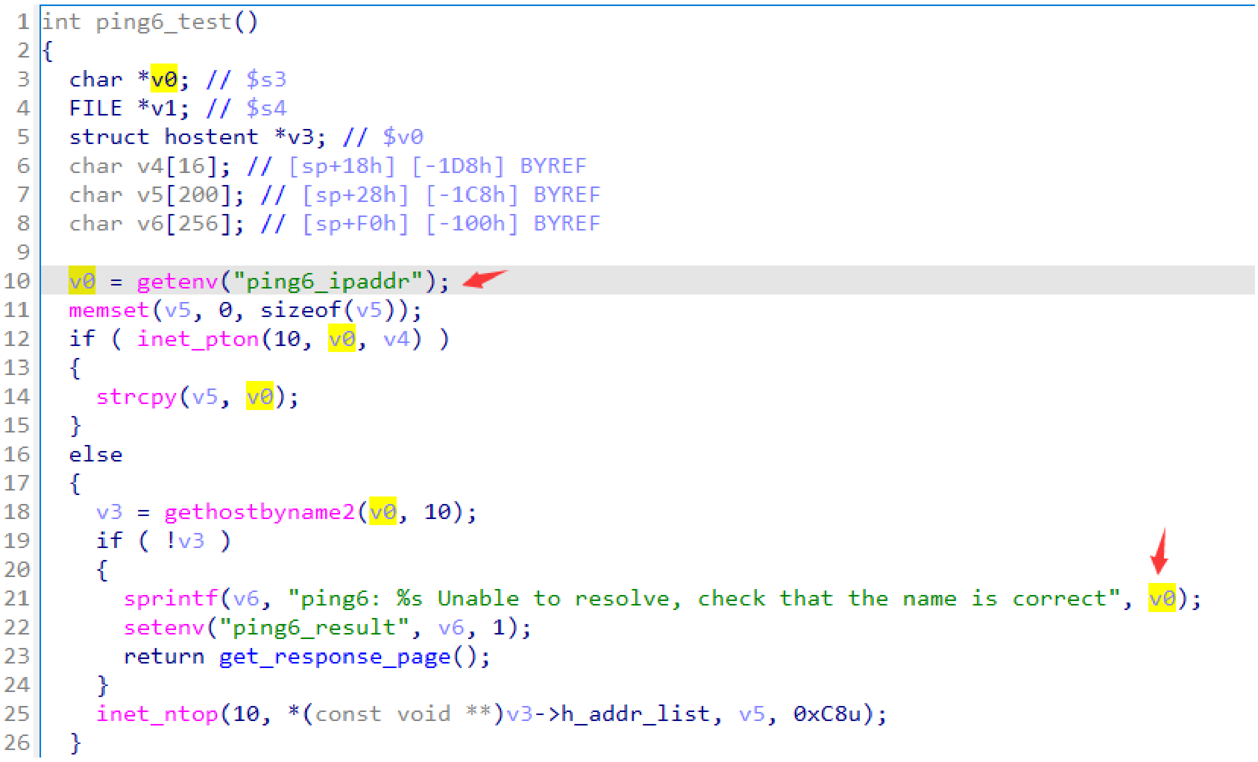
binary ssi in firmware

Attack vector

A user in the router's network can exploit the device by sending malicious http requests

Description

TRENDnet TEW-823DRU with firmware up to and including 1.02B01 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 ping6_test with a sufficiently long key ping6_ipaddr.



```
int ping6_test()
{
  char *v0; // $s3
  FILE *v1; // $s4
  struct hostent *v3; // $v0
  char v4[16]; // [sp+18h] [-1D8h] BYREF
  char v5[200]; // [sp+28h] [-1C8h] BYREF
  char v6[256]; // [sp+F0h] [-100h] BYREF

  v0 = getenv("ping6_ipaddr");
  memset(v5, 0, sizeof(v5));
  if ( inet_pton(10, v0, v4) )
  {
    strcpy(v5, v0);
  }
  else
  {
    v3 = gethostbyname2(v0, 10);
    if ( !v3 )
    {
      sprintf(v6, "ping6: %s Unable to resolve, check that the name is correct", v0);
      setenv("ping6_result", v6, 1);
      return get_response_page();
    }
    inet_ntop(10, *(const void **)v3->h_addr_list, v5, 0xC8u);
  }
```

0x3 sbo in function auto_up_lp

Affected components

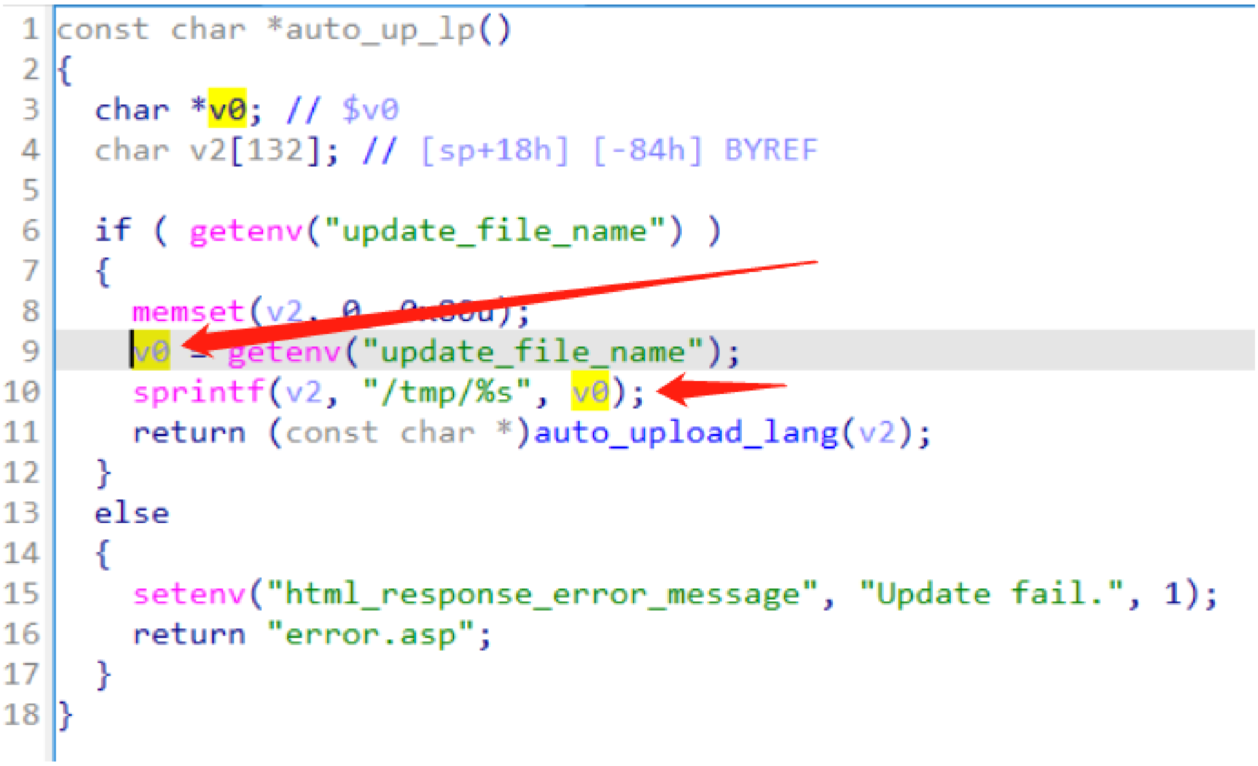
binary ssi in firmware

Attack vector

A user in the router's network can exploit the device by sending malicious http requests

Description

TRENDnet TEW-823DRU with firmware up to and including 1.02B01 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 auto_up_lp with a sufficiently long key update_file_name.



```
const char *auto_up_lp()
{
  char *v0; // $v0
  char v2[132]; // [sp+18h] [-84h] BYREF

  if ( getenv("update_file_name") )
  {
    memset(v2, 0, 0x80u);
    v0 = getenv("update_file_name");
    sprintf(v2, "/tmp/%s", v0);
    return (const char *)auto_upload_lang(v2);
  }
  else
  {
    setenv("html_response_error_message", "Update fail.", 1);
    return "error.asp";
  }
}
```

0x4 sbo in function do_graph_auth

Affected components

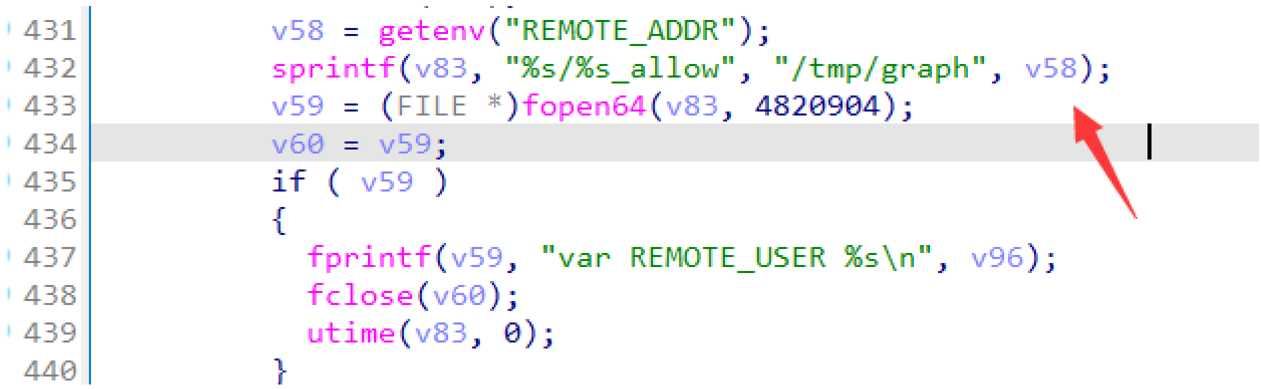
binary ssi in firmware

Attack vector

A user in the router's network can exploit the device by sending malicious http requests

Description

TRENDnet TEW-823DRU with firmware up to and including 1.02B01 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 do_graph_auth with a sufficiently long key REMOTE_ADDR.



```
        v58 = getenv("REMOTE_ADDR");
        sprintf(v83, "%s/%s_allow", "/tmp/graph", v58);
        v59 = (FILE *)fopen64(v83, 4820904);
        v60 = v59;
        if ( v59 )
        {
          fprintf(v59, "var REMOTE_USER %s\n", v96);
          fclose(v60);
          utime(v83, 0);
        }
```

0x5 sbo in function set_sta_enrollee_pin_5g and set_sta_enrollee_pin_24g

Affected components

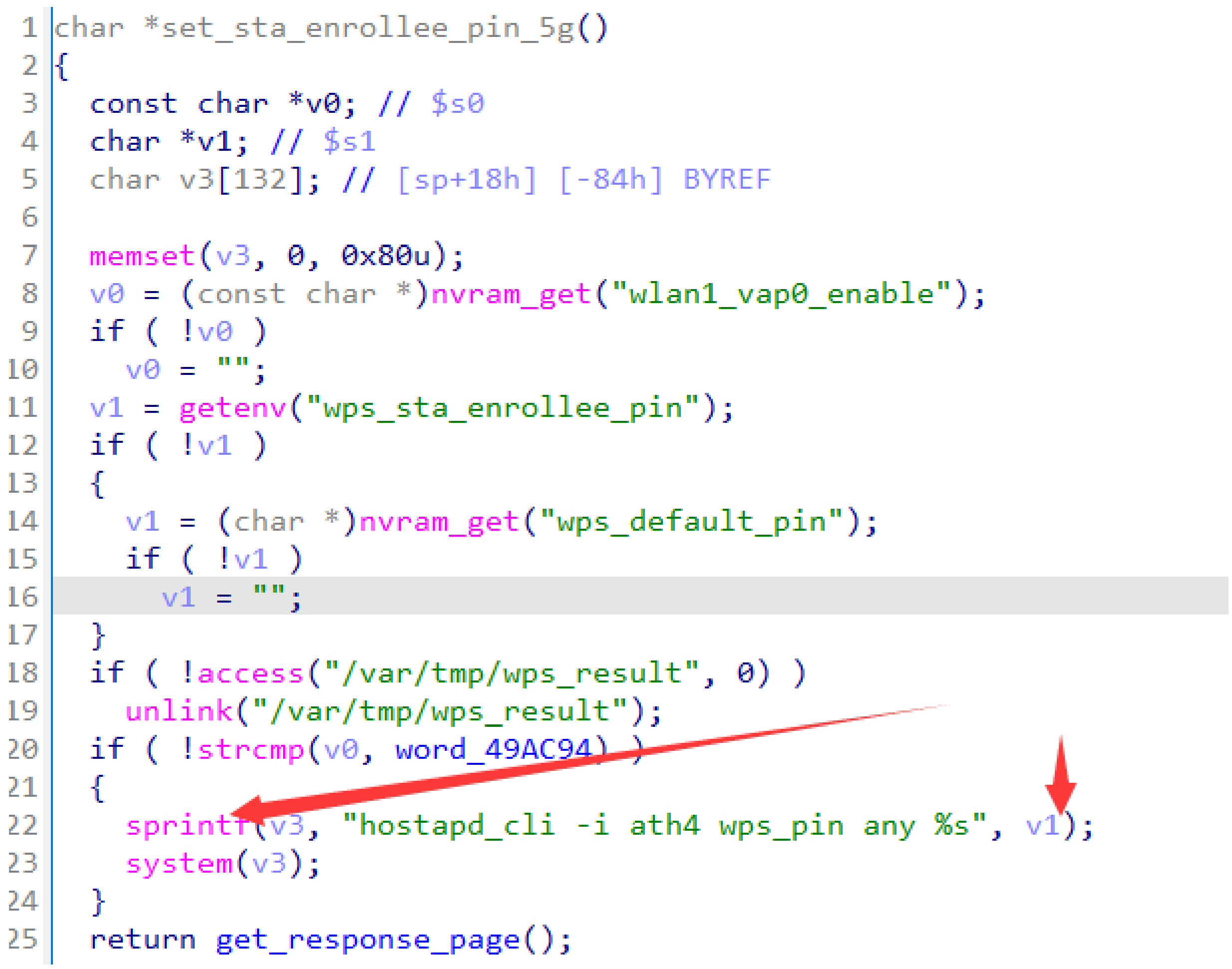
binary ssi in firmware

Attack vector

A user in the router's network can exploit the device by sending malicious http requests

Description

TRENDnet TEW-823DRU with firmware up to and including 1.02B01 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 set_sta_enrollee_pin_5g or set_sta_enrollee_pin_24g with a sufficiently long key wps_sta_enrollee_pin.



```
char *set_sta_enrollee_pin_5g()
{
  const char *v0; // $s0
  char *v1; // $s1
  char v3[132]; // [sp+18h] [-84h] BYREF

  memset(v3, 0, 0x80u);
  v0 = (const char *)nvram_get("wlan1_vap0_enable");
  if ( !v0 )
    v0 = "";
  v1 = getenv("wps_sta_enrollee_pin");
  if ( !v1 )
  {
    v1 = (char *)nvram_get("wps_default_pin");
    if ( !v1 )
      v1 = "";
  }
  if ( !access("/var/tmp/wps_result", 0) )
    unlink("/var/tmp/wps_result");
  if ( !strcmp(v0, word_49AC94) )
  {
    sprintf(v3, "hostapd_cli -i ath4 wps_pin any %s", v1);
    system(v3);
  }
  return get_response_page();
```

0x6 sbo in function reject

Affected components

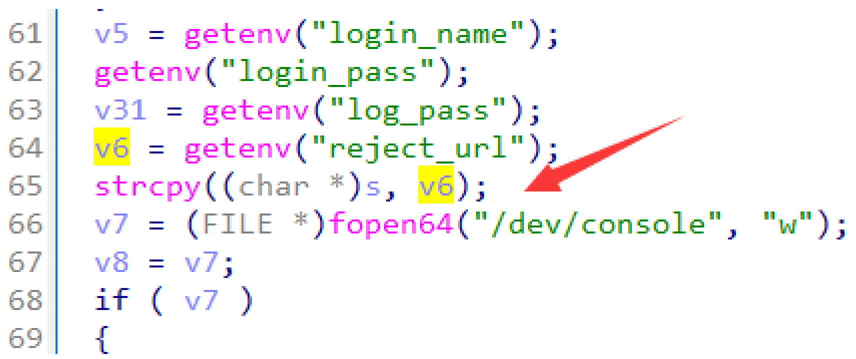
binary ssi in firmware

Attack vector

A user in the router's network can exploit the device by sending malicious http requests

Description

TRENDnet TEW-823DRU with firmware up to and including 1.02B01 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 reject with a sufficiently long key reject_url.



```
v5 = getenv("login_name");
getenv("login_pass");
v31 = getenv("log_pass");
v6 = getenv("reject_url");
strcpy((char *)s, v6);
v7 = (FILE *)fopen64("/dev/console", "w");
v8 = v7;
if ( v7 )
{
```

0x7 sbo in function main

Affected components

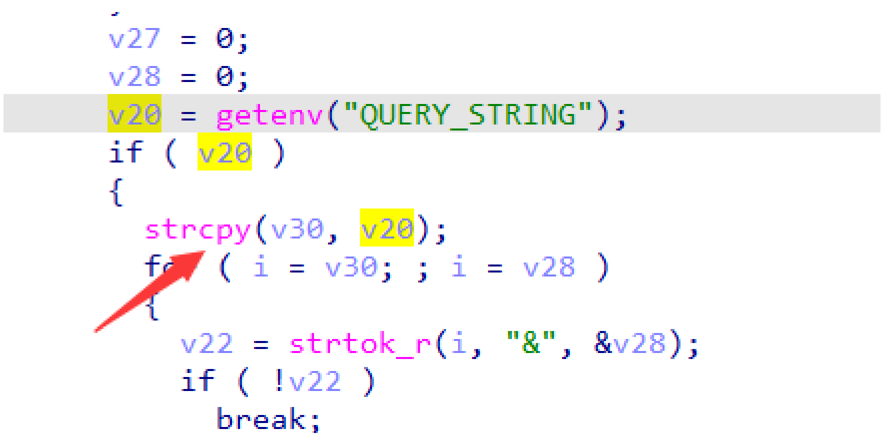
binary ssi in firmware

Attack vector

The user can exploit the device by sending malicious http requests remotely.

Description

TRENDnet TEW-823DRU with firmware up to and including 1.02B01 contains a stack-based buffer overflow in the ssi binary. The overflow allows an unauthenticated user to execute arbitrary code by providing a sufficiently long query string when posting to any valid cgi, txt, asp, or js file. The vulnerability can be exercised on the local intranet or remotely if remote administration is enabled.



```
v27 = 0;
v28 = 0;
v20 = getenv("QUERY_STRING");
if ( v20 )
{
  strcpy(v30, v20);
  for ( i = v30; ; i = v28 )
  {
    v22 = strtok_r(i, "&", &v28);
    if ( !v22 )
      break;
```

0x8 sbo in function st_dev_connect/st_dev_disconnect/st_dev_rconnect

Affected components

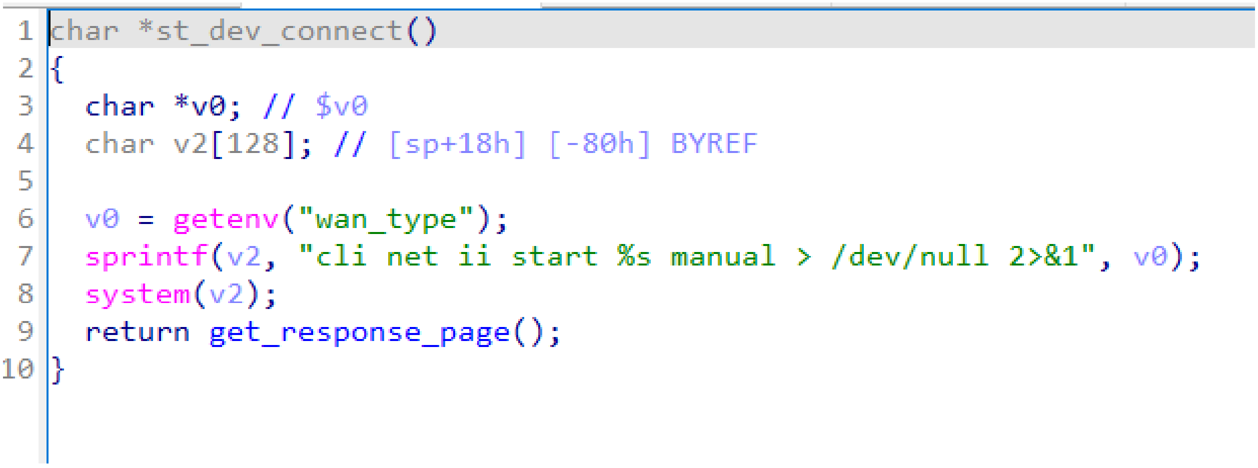
binary ssi in firmware

Attack vector

A user in the router's network can exploit the device by sending malicious http requests

Description

TRENDnet TEW-823DRU with firmware up to and including 1.02B01 contains multi stack-based buffer overflows 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, st_dev_disconnect, or st_dev_rconnect with a sufficiently long wan_type key.



```c
char *st_dev_connect()
{
  char *v0; // $v0
  char v2[128]; // [sp+18h] [-80h] BYREF

  v0 = getenv("wan_type");
  sprintf(v2, "cli net ii start %s manual > /dev/null 2>&1", v0);
  system(v2);
  return get_response_page();
}
```

0x9 sbo in function wizard_ipv6

Affected components

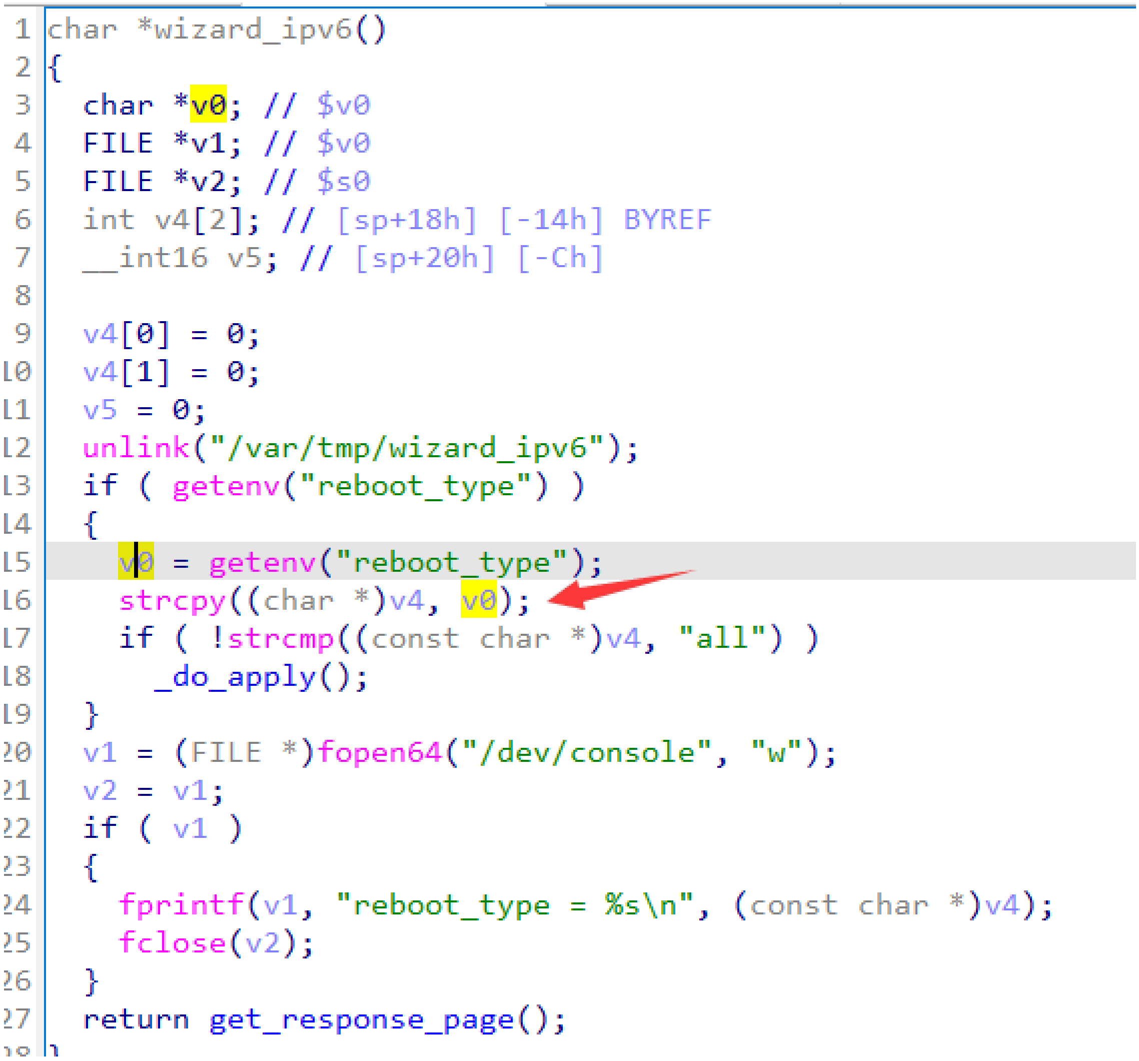
binary ssi in firmware

Attack vector

A user in the router's network can exploit the device by sending malicious http requests

Description

TRENDnet TEW-823DRU with firmware up to and including 1.02B01 contains a stack-based buffer overflows in the ssi binary. The overflow allows an authenticated user to execute arbitrary code by POSTing to apply.cgi via the action wizard_ipv6 with a sufficiently long reboot_type key.



```
char *wizard_ipv6()
{
  char *v0; // $v0
  FILE *v1; // $v0
  FILE *v2; // $s0
  int v4[2]; // [sp+18h] [-14h] BYREF
  __int16 v5; // [sp+20h] [-Ch]

  v4[0] = 0;
  v4[1] = 0;
  v5 = 0;
  unlink("/var/tmp/wizard_ipv6");
  if ( getenv("reboot_type") )
  {
    v0 = getenv("reboot_type");
    strcpy((char *)v4, v0);
    if ( !strcmp((const char *)v4, "all") )
      _do_apply();
  }
  v1 = (FILE *)fopen64("/dev/console", "w");
  v2 = v1;
  if ( v1 )
  {
    fprintf(v1, "reboot_type = %s\n", (const char *)v4);
    fclose(v2);
  }
  return get_response_page();
}
```

0x10 sbo in function setup_wizard_mydlink

Affected components

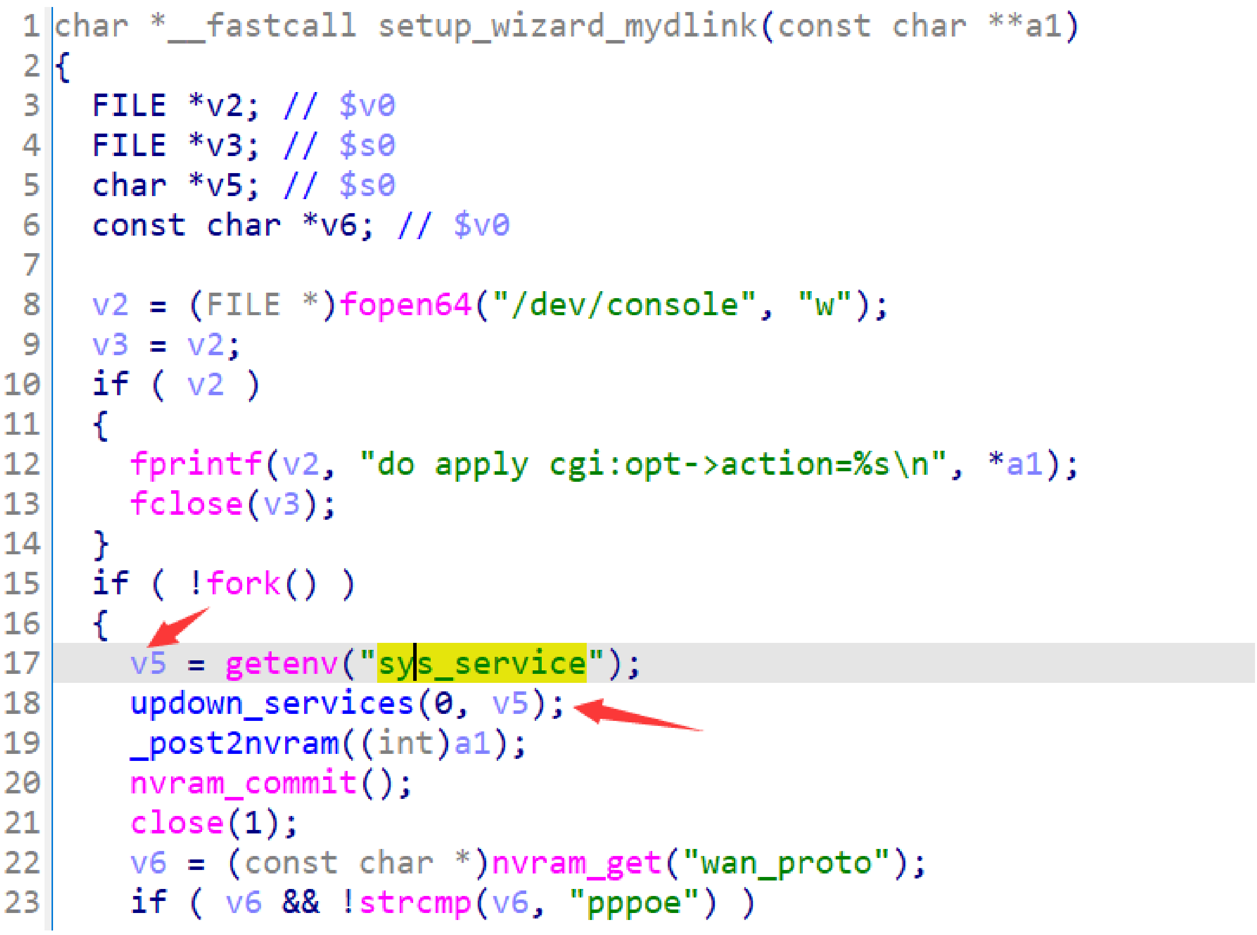
binary ssi in firmware

Attack vector

A user in the router's network can exploit the device by sending malicious http requests

Description

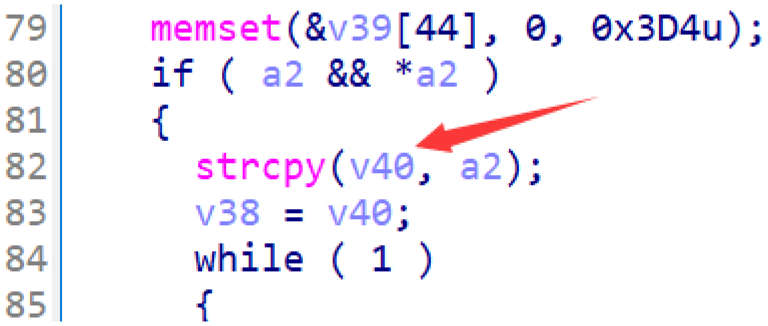
TRENDnet TEW-823DRU with firmware up to and including 1.02B01 contains a stack-based buffer overflows in the ssi binary. The overflow allows an authenticated user to execute arbitrary code by POSTing to apply.cgi via the action setup_wizard_mydlink with a sufficiently long sys_service key.



```
char *__fastcall setup_wizard_mydlink(const char **a1)
{
  FILE *v2; // $v0
  FILE *v3; // $s0
  char *v5; // $s0
  const char *v6; // $v0

  v2 = (FILE *)fopen64("/dev/console", "w");
  v3 = v2;
  if ( v2 )
  {
    fprintf(v2, "do apply cgi:opt->action=%s\n", *a1);
    fclose(v3);
  }
  if ( !fork() )
  {
    v5 = getenv("sys_service");
    updown_services(0, v5);
    _post2nvram((int)a1);
    nvram_commit();
    close(1);
    v6 = (const char *)nvram_get("wan_proto");
    if ( v6 && !strcmp(v6, "pppoe") )
```

The value of "sys_service" will be called as the a2 parameter in function updown_services, which leads to a buffer overflow in strcpy



```
  memset(&v39[44], 0, 0x3D4u);
  if ( a2 && *a2 )
  {
    strcpy(v40, a2);
    v38 = v40;
    while ( 1 )
    {
```

OS Command Injection

0x1 OCI in function set_sta_enrollee_pin_5g

Affected components

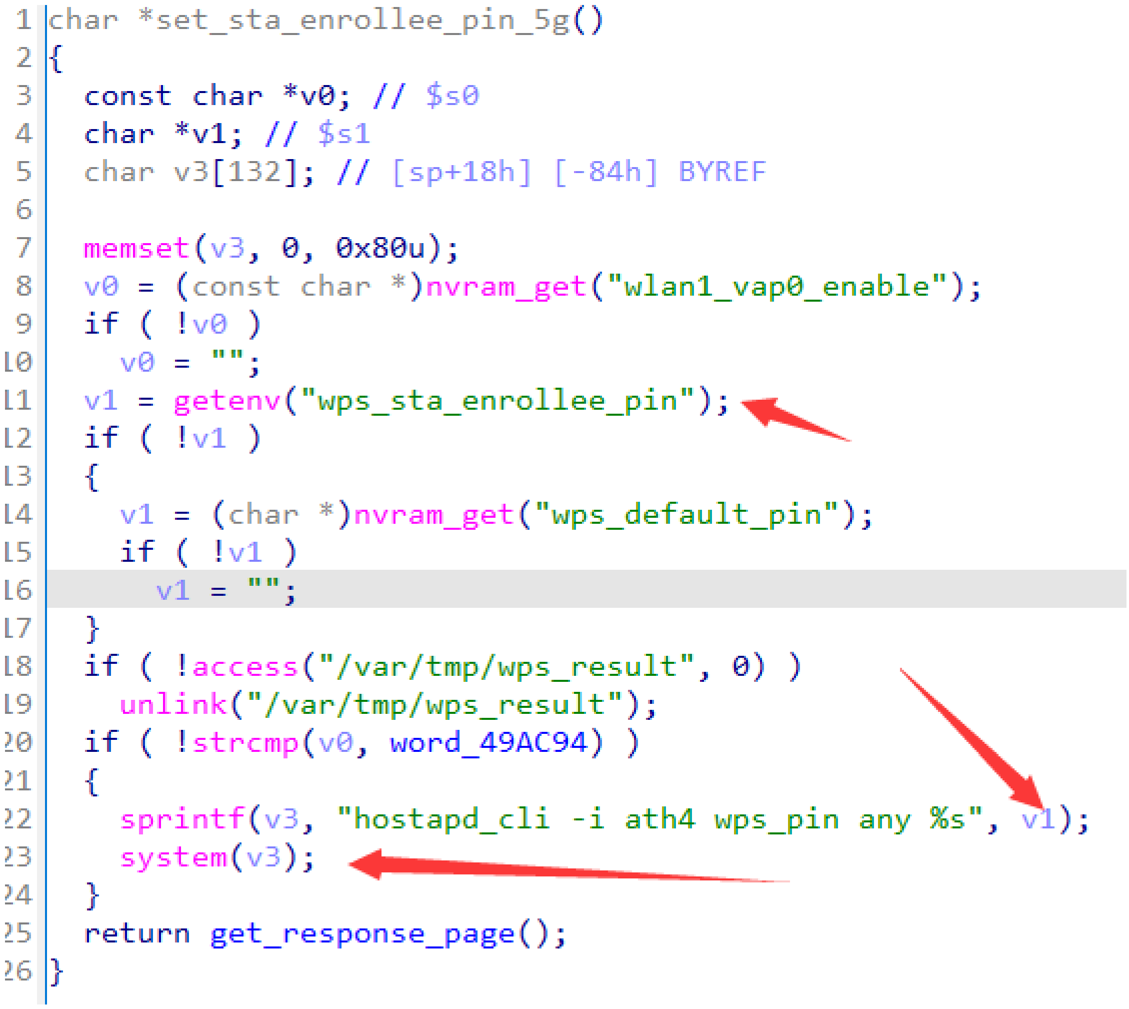
binary ssi in firmware

Attack vector

A user in the router's network can exploit the device by sending malicious http requests

Description

TRENDnet TEW-823DRU devices through 1.02B01 contain a command injection in apply.cgi via the action set_sta_enrollee_pin_5g with the key wps_sta_enrollee_pin, allowing an authenticated user to run arbitrary commands on the device.



```
char *set_sta_enrollee_pin_5g()
{
  const char *v0; // $s0
  char *v1; // $s1
  char v3[132]; // [sp+18h] [-84h] BYREF

  memset(v3, 0, 0x80u);
  v0 = (const char *)nvram_get("wlan1_vap0_enable");
  if ( !v0 )
    v0 = "";
  v1 = getenv("wps_sta_enrollee_pin");
  if ( !v1 )
  {
    v1 = (char *)nvram_get("wps_default_pin");
    if ( !v1 )
      v1 = "";
  }
  if ( !access("/var/tmp/wps_result", 0) )
    unlink("/var/tmp/wps_result");
  if ( !strcmp(v0, word_49AC94) )
  {
    sprintf(v3, "hostapd_cli -i ath4 wps_pin any %s", v1);
    system(v3);
  }
  return get_response_page();
}
```

0x2 OCI in function send_log_email

Affected components

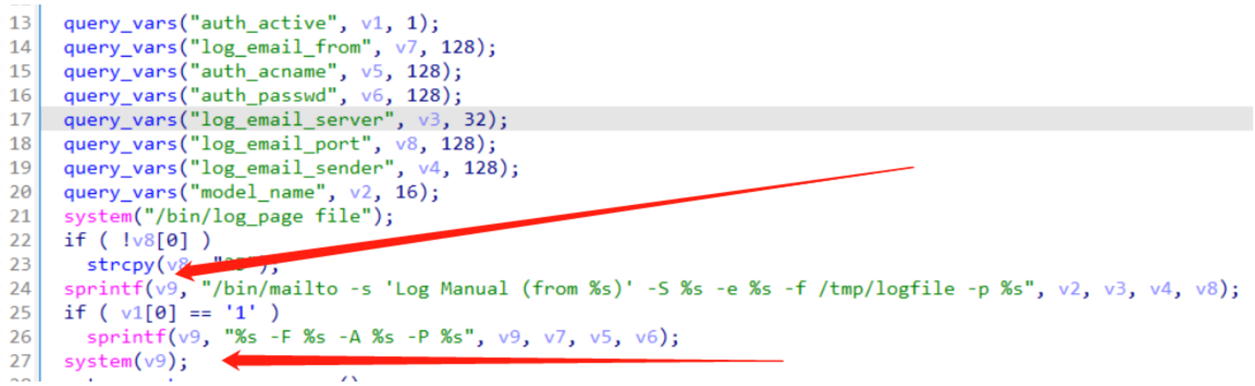
binary ssi in firmware

Attack vector

A user in the router's network can exploit the device by sending malicious http requests

Description

TRENDnet TEW-823DRU devices through 1.02B01 contain multi command injections in apply.cgi via the action send_log_email with the keys log_email_from or auth_acname or auth_acpasswd or log_email_port..., allowing an authenticated user to run arbitrary commands on the device.



```
query_vars("auth_active", v1, 1);
query_vars("log_email_from", v7, 128);
query_vars("auth_acname", v5, 128);
query_vars("auth_passwd", v6, 128);
query_vars("log_email_server", v3, 32);
query_vars("log_email_port", v8, 128);
query_vars("log_email_sender", v4, 128);
query_vars("model_name", v2, 16);
system("/bin/log_page file");
if ( !v8[0] )
  strcpy(v8, "25");
sprintf(v9, "/bin/mailto -s 'Log Manual (from %s)' -S %s -e %s -f /tmp/logfile -p %s", v2, v3, v4, v8);
if ( v1[0] == '1' )
  sprintf(v9, "%s -F %s -A %s -P %s", v9, v7, v5, v6);
system(v9);
```

0x3 OCI in function pppoe_connect

Affected components

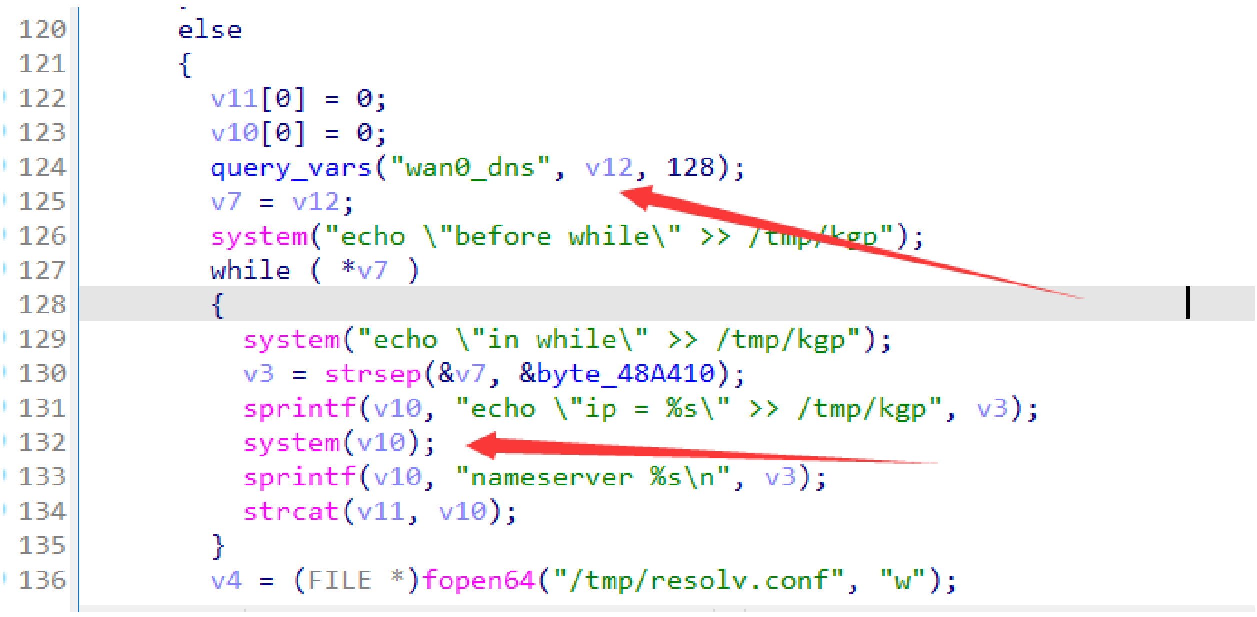
binary ssi in firmware

Attack vector

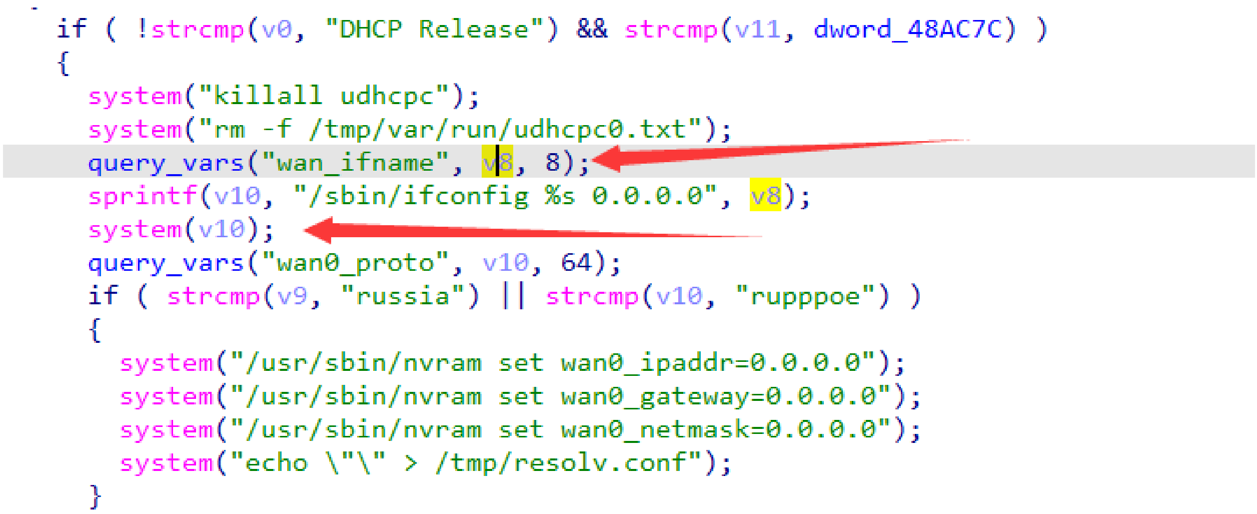
A user in the router's network can exploit the device by sending malicious http requests

Description

TRENDnet TEW-823DRU devices through 1.02B01 contain multi command injections in apply.cgi via the action pppoe_connect or ru_pppoe_connect or dhcp_connect with the key wan0_devs or wan_ifname, allowing an authenticated user to run arbitrary commands on the device.



```
else
{
  v11[0] = 0;
  v10[0] = 0;
  query_vars("wan0_dns", v12, 128);
  v7 = v12;
  system("echo \"before while\" >> /tmp/kgp");
  while ( *v7 )
  {
    system("echo \"in while\" >> /tmp/kgp");
    v3 = strsep(&v7, &byte_48A410);
    sprintf(v10, "echo \"ip = %s\" >> /tmp/kgp", v3);
    system(v10);
    sprintf(v10, "nameserver %s\n", v3);
    strcat(v11, v10);
  }
  v4 = (FILE *)fopen64("/tmp/resolv.conf", "w");
```



```
if ( !strcmp(v0, "DHCP Release") && strcmp(v11, dword_48AC7C) )
{
  system("killall udhcpc");
  system("rm -f /tmp/var/run/udhcpc0.txt");
  query_vars("wan_ifname", v8, 8);
  sprintf(v10, "/sbin/ifconfig %s 0.0.0.0", v8);
  system(v10);
  query_vars("wan0_proto", v10, 64);
  if ( strcmp(v9, "russia") || strcmp(v10, "rupppoe") )
  {
    system("/usr/sbin/nvram set wan0_ipaddr=0.0.0.0");
    system("/usr/sbin/nvram set wan0_gateway=0.0.0.0");
    system("/usr/sbin/nvram set wan0_netmask=0.0.0.0");
    system("echo \"\" > /tmp/resolv.conf");
  }
```

0x4 OCI in function st_dev_connect/st_dev_disconnect/st_dev_rconnect

Affected components

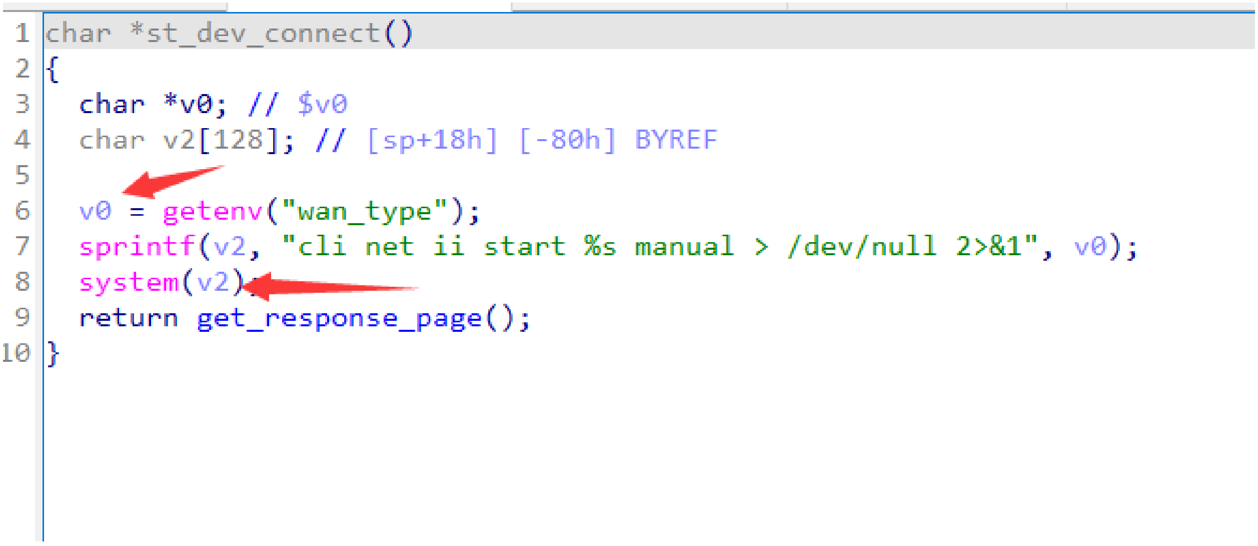
binary ssi in firmware

Attack vector

A user in the router's network can exploit the device by sending malicious http requests

Description

TRENDnet TEW-823DRU devices through 1.02B01 contain multi command injections in apply.cgi via the action st_dev_connect or st_dev_disconnect or st_dev_rconnect with the key wan_type, allowing an authenticated user to run arbitrary commands on the device.



```
char *st_dev_connect()
{
  char *v0; // $v0
  char v2[128]; // [sp+18h] [-80h] BYREF

  v0 = getenv("wan_type");
  sprintf(v2, "cli net ii start %s manual > /dev/null 2>&1", v0);
  system(v2);
  return get_response_page();
}
```

0x5 OCI in function delete_vpn

Affected components

binary ssi in firmware

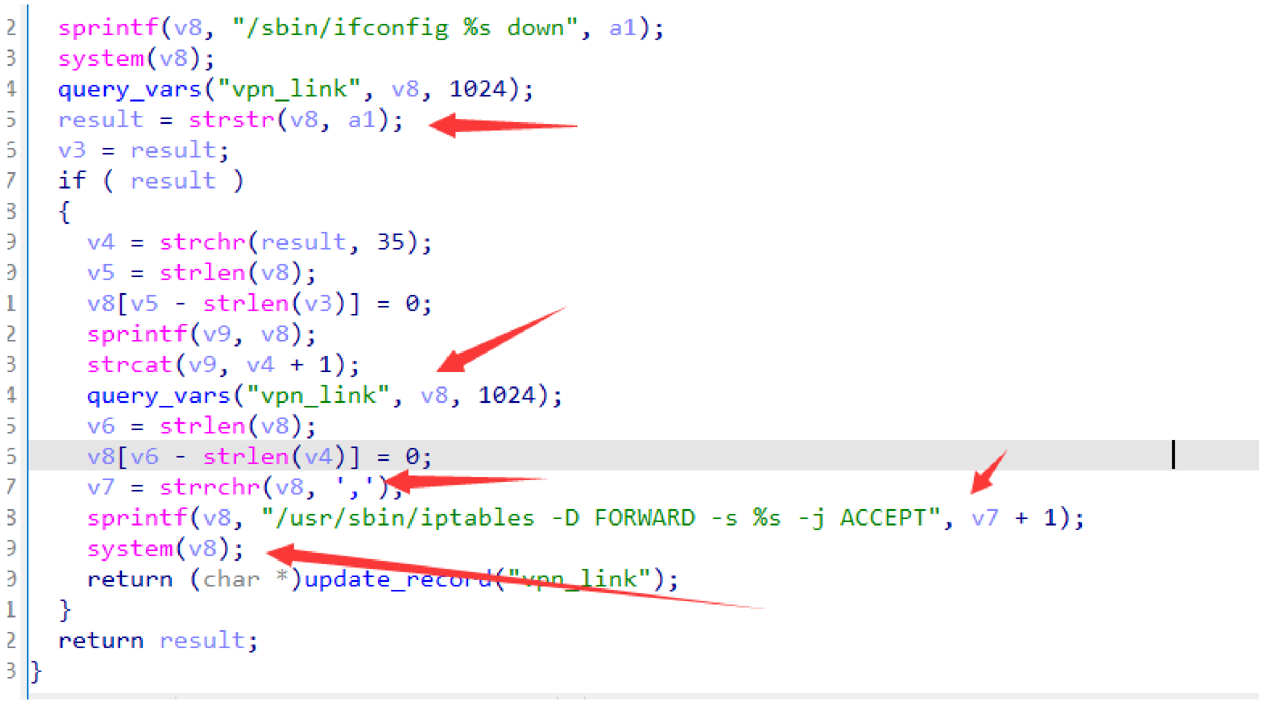
Attack vector

A user in the router's network can exploit the device by sending malicious http requests

Description

TRENDnet TEW-823DRU devices through 1.02B01 contain a command injections in apply.cgi via the action delete_vpn with the key vpn_link, allowing an authenticated user to run arbitrary commands on the device.

Once the value of vpn_link contains "/sbin/ifconfig 0 down,", the arbitrrary command can be executed by system()



```
  sprintf(v8, "/sbin/ifconfig %s down", a1);
  system(v8);
  query_vars("vpn_link", v8, 1024);
  result = strstr(v8, a1);
  v3 = result;
  if ( result )
  {
    v4 = strchr(result, 35);
    v5 = strlen(v8);
    v8[v5 - strlen(v3)] = 0;
    sprintf(v9, v8);
    strcat(v9, v4 + 1);
    query_vars("vpn_link", v8, 1024);
    v6 = strlen(v8);
    v8[v6 - strlen(v4)] = 0;
    v7 = strrchr(v8, ',');
    sprintf(v8, "/usr/sbin/iptables -D FORWARD -s %s -j ACCEPT", v7 + 1);
    system(v8);
    return (char *)update_record("vpn_link");
  }
  return result;
}
```

0x6 OCI in function hnt_udp

Affected components

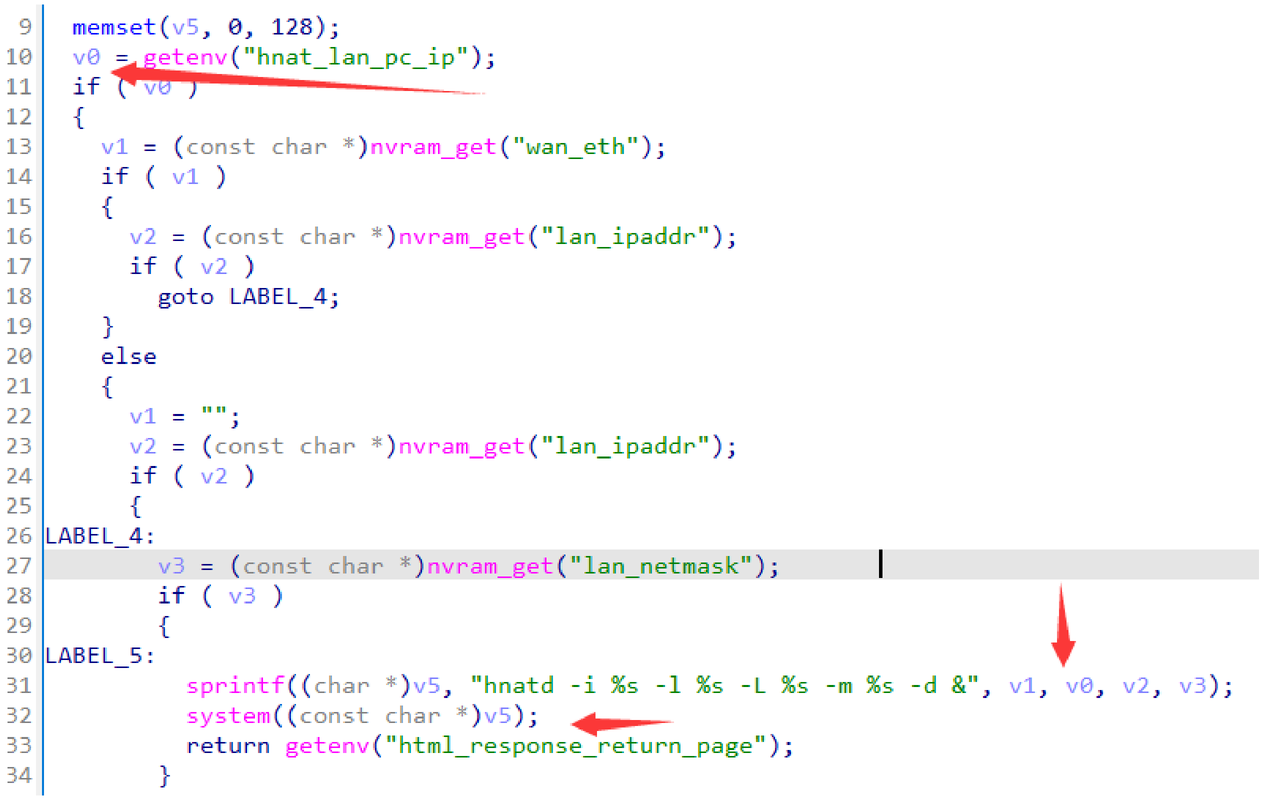
binary ssi in firmware

Attack vector

A user in the router's network can exploit the device by sending malicious http requests

Description

TRENDnet TEW-823DRU devices through 1.02B01 contain a command injections in apply.cgi via the action hnt_udp with the key hnat_lan_pc_ip, allowing an authenticated user to run arbitrary commands on the device.



```
  memset(v5, 0, 128);
  v0 = getenv("hnat_lan_pc_ip");
  if ( v0 )
  {
    v1 = (const char *)nvram_get("wan_eth");
    if ( v1 )
    {
      v2 = (const char *)nvram_get("lan_ipaddr");
      if ( v2 )
        goto LABEL_4;
    }
    else
    {
      v1 = "";
      v2 = (const char *)nvram_get("lan_ipaddr");
      if ( v2 )
      {
LABEL_4:
        v3 = (const char *)nvram_get("lan_netmask");
        if ( v3 )
        {
LABEL_5:
          sprintf((char *)v5, "hnatd -i %s -l %s -L %s -m %s -d &", v1, v0, v2, v3);
          system((const char *)v5);
          return getenv("html_response_return_page");
        }
```

0x7 OS command injection in function timeout and fail

Affected components

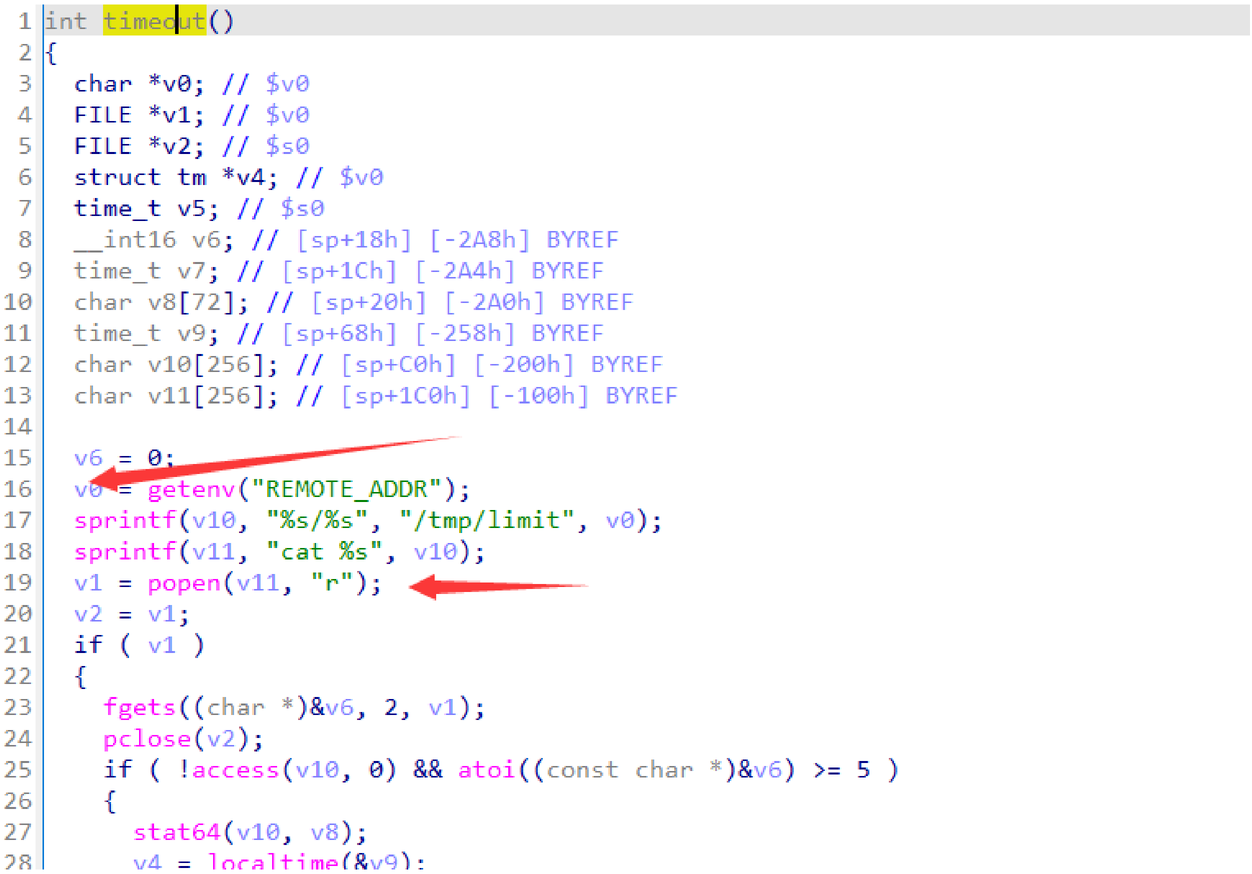
binary ssi in firmware

Attack vector

A user in the router's network can exploit the device by sending malicious http requests

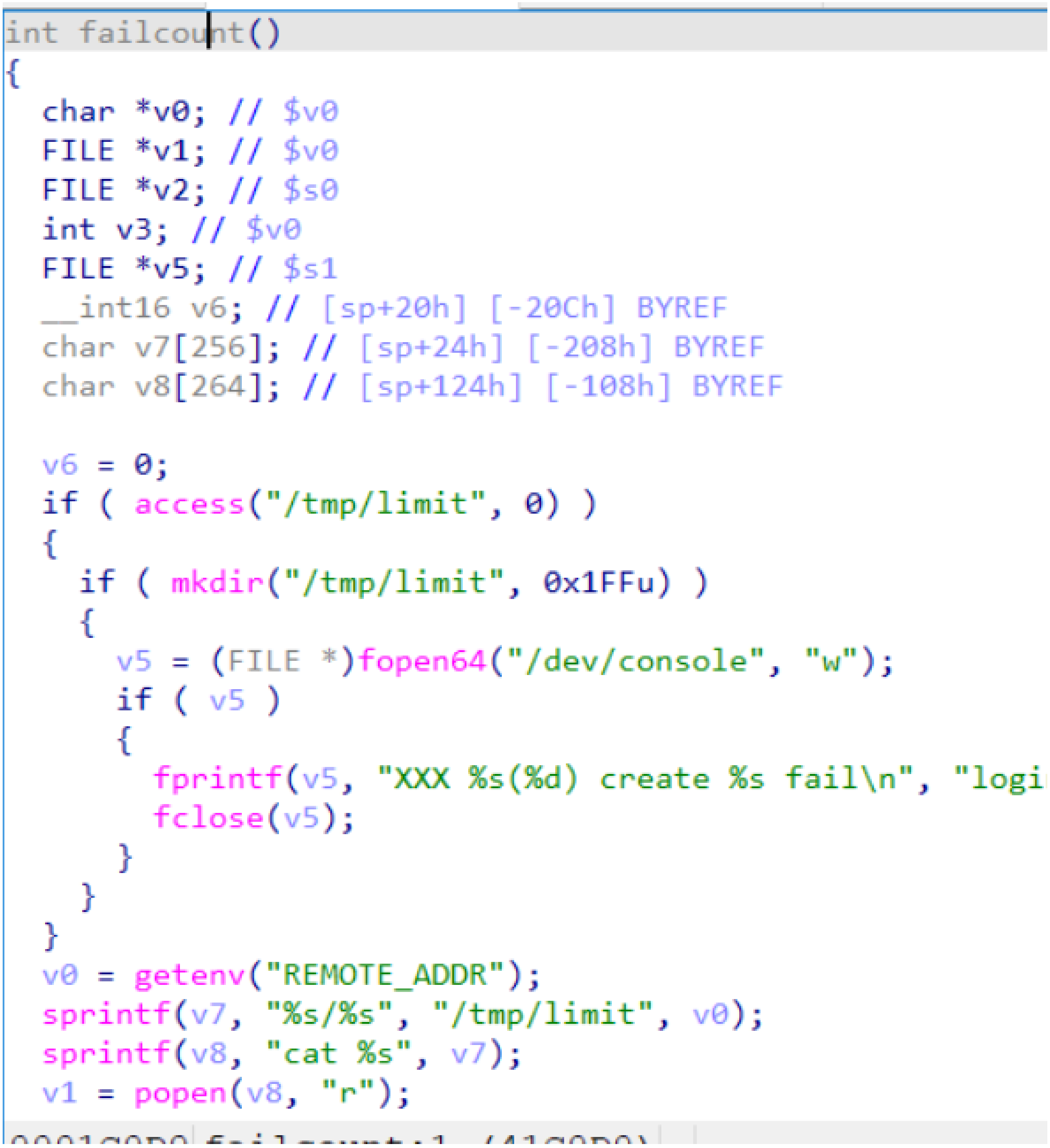
Description

TRENDnet TEW-823DRU devices through 1.02B01 contain command injections in apply.cgi via the action timeout or fail with the key REMOTE_ADDR, allowing an authenticated user to run arbitrary commands on the device.



```
int timeout()
{
  char *v0; // $v0
  FILE *v1; // $v0
  FILE *v2; // $s0
  struct tm *v4; // $v0
  time_t v5; // $s0
  __int16 v6; // [sp+18h] [-2A8h] BYREF
  time_t v7; // [sp+1Ch] [-2A4h] BYREF
  char v8[72]; // [sp+20h] [-2A0h] BYREF
  time_t v9; // [sp+68h] [-258h] BYREF
  char v10[256]; // [sp+C0h] [-200h] BYREF
  char v11[256]; // [sp+1C0h] [-100h] BYREF

  v6 = 0;
  v0 = getenv("REMOTE_ADDR");
  sprintf(v10, "%s/%s", "/tmp/limit", v0);
  sprintf(v11, "cat %s", v10);
  v1 = popen(v11, "r");
  v2 = v1;
  if ( v1 )
  {
    fgets((char *)&v6, 2, v1);
    pclose(v2);
    if ( !access(v10, 0) && atoi((const char *)&v6) >= 5 )
    {
      stat64(v10, v8);
      v4 = localtime(&v9);
```



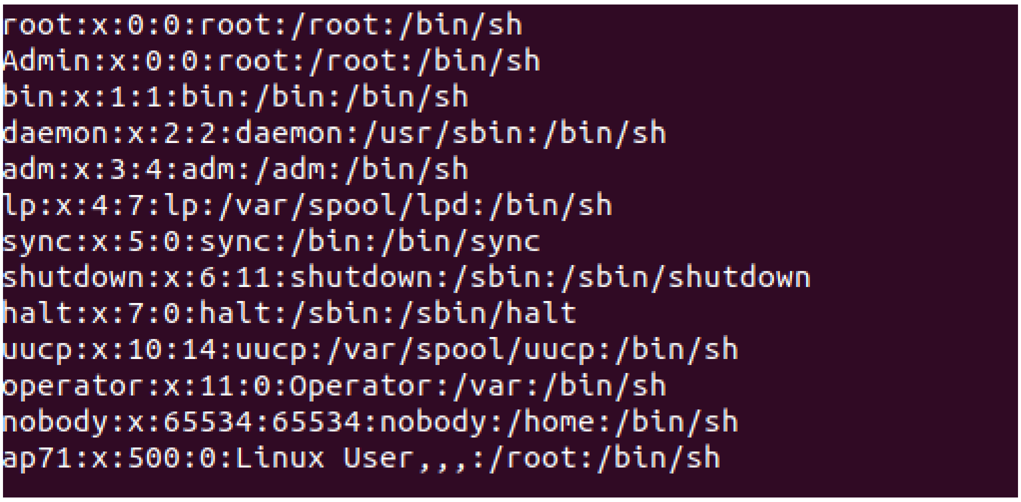
```
int failcount()
{
  char *v0; // $v0
  FILE *v1; // $v0
  FILE *v2; // $s0
  int v3; // $v0
  FILE *v5; // $s1
  __int16 v6; // [sp+20h] [-20Ch] BYREF
  char v7[256]; // [sp+24h] [-208h] BYREF
  char v8[264]; // [sp+124h] [-108h] BYREF

  v6 = 0;
  if ( access("/tmp/limit", 0) )
  {
    if ( mkdir("/tmp/limit", 0x1FFu) )
    {
      v5 = (FILE *)fopen64("/dev/console", "w");
      if ( v5 )
      {
        fprintf(v5, "XXX %s(%d) create %s fail\n", "logi
        fclose(v5);
      }
    }
  }
  v0 = getenv("REMOTE_ADDR");
  sprintf(v7, "%s/%s", "/tmp/limit", v0);
  sprintf(v8, "cat %s", v7);
  v1 = popen(v8, "r");
0001C0D0 failcount:1 (41C0D0)
```

Plaintext Storage

0x1 config information stored in plaintext

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



```
root:x:0:0:root:/root:/bin/sh
Admin:x:0:0:root:/root:/bin/sh
bin:x:1:1:bin:/bin:/bin/sh
daemon:x:2:2:daemon:/usr/sbin:/bin/sh
adm:x:3:4:adm:/adm:/bin/sh
lp:x:4:7:lp:/var/spool/lpd:/bin/sh
sync:x:5:0:sync:/bin:/bin/sync
shutdown:x:6:11:shutdown:/sbin:/sbin/shutdown
halt:x:7:0:halt:/sbin:/sbin/halt
uucp:x:10:14:uucp:/var/spool/uucp:/bin/sh
operator:x:11:0:Operator:/var:/bin/sh
nobody:x:65534:65534:nobody:/home:/bin/sh
ap71:x:500:0:Linux User,,,:/root:/bin/sh
```

0x2 sensitive information used by HTTP

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