peanuts62 / **bug_poc** Public

bug_poc

☆ 2 stars 1 fork

☆ Star | Notifications

Code | Issues 1 | Pull requests | Actions | Projects | Security | ···

master ▾ | Go to file

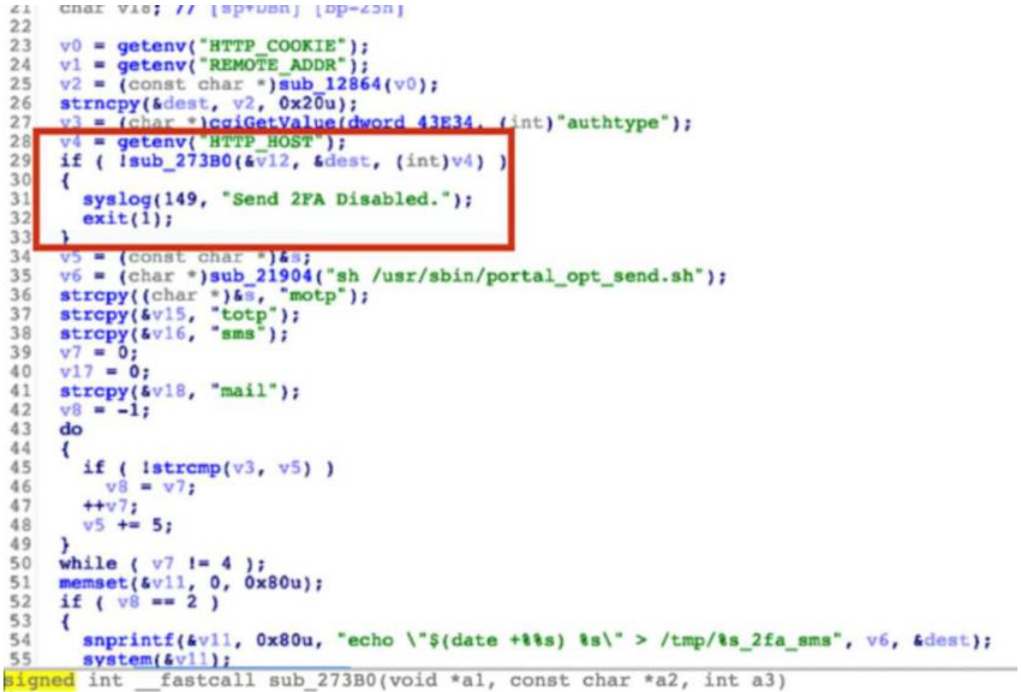
peanuts and **peanuts** add ··· on Dec 18, 2020 9

View code

README.md

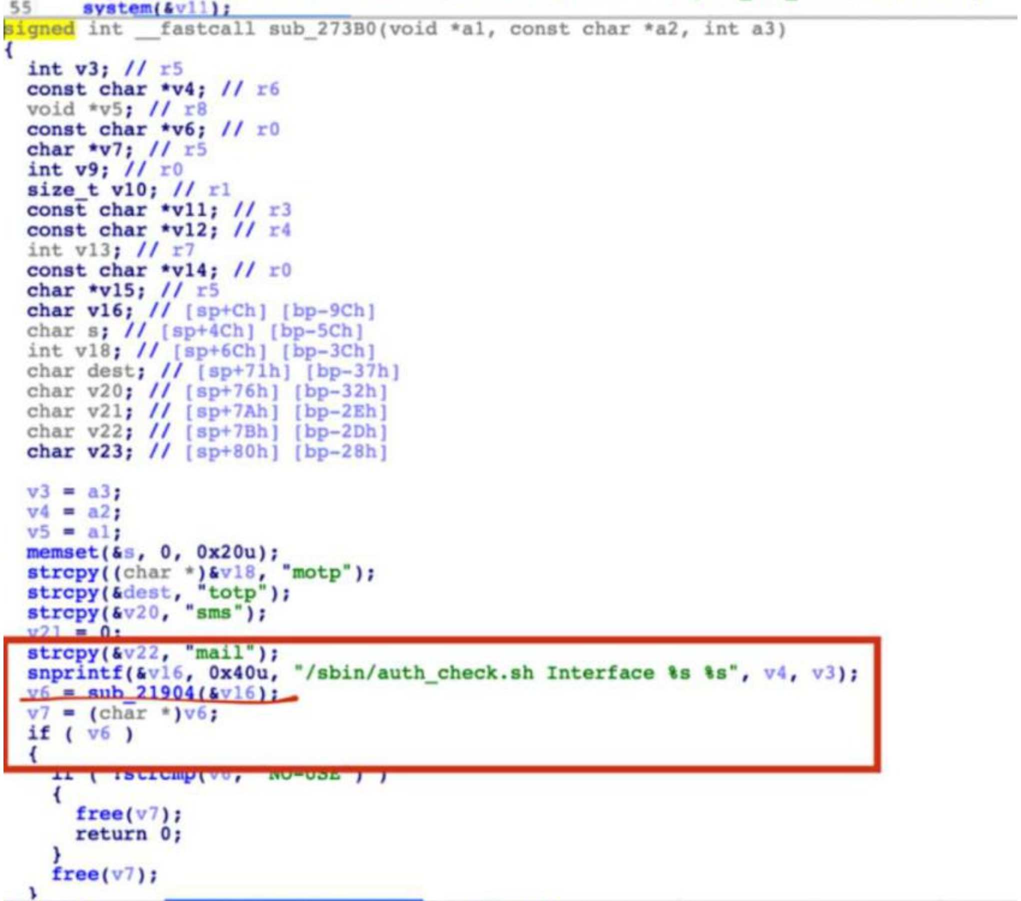
bug_poc

in the mainfunction.cgi use ida could find the bug.



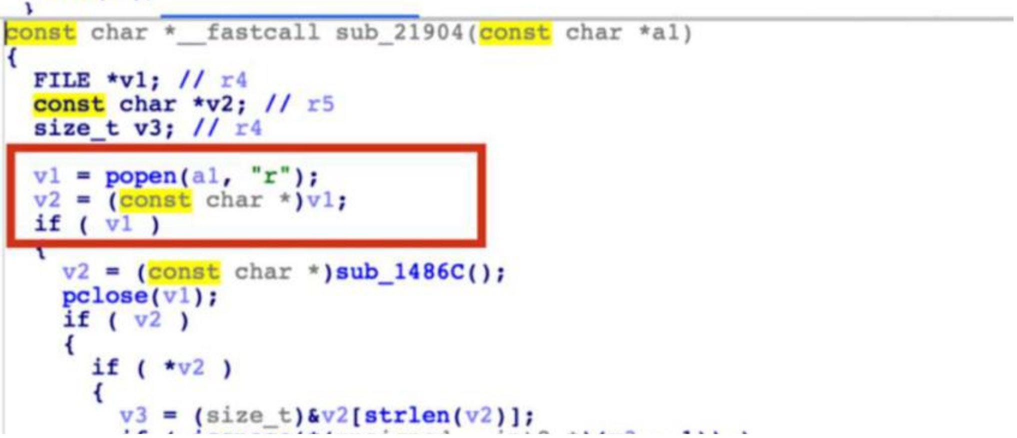
```
  char v18; // [sp+DBh] [bp-25h]

  v0 = getenv("HTTP_COOKIE");
  v1 = getenv("REMOTE_ADDR");
  v2 = (const char *)sub_12864(v0);
  strncpy(&dest, v2, 0x20u);
  v3 = (char *)cgiGetValue(dword_43E34, (int)"authtype");
  v4 = getenv("HTTP_HOST");
  if ( !sub_273B0(&v12, &dest, (int)v4) )
  {
    syslog(149, "Send 2FA Disabled.");
    exit(1);
  }
  v5 = (const char *)&s;
  v6 = (char *)sub_21904("sh /usr/sbin/portal_opt_send.sh");
  strcpy((char *)&s, "motp");
  strcpy(&v15, "totp");
  strcpy(&v16, "sms");
  v7 = 0;
  v17 = 0;
  strcpy(&v18, "mail");
  v8 = -1;
  do
  {
    if ( !strcmp(v3, v5) )
      v8 = v7;
    ++v7;
    v5 += 5;
  }
  while ( v7 != 4 );
  memset(&v11, 0, 0x80u);
  if ( v8 == 2 )
  {
    snprintf(&v11, 0x80u, "echo \"$(date +%%s) %s\" > /tmp/%s_2fa_sms", v6, &dest);
    system(&v11);
```



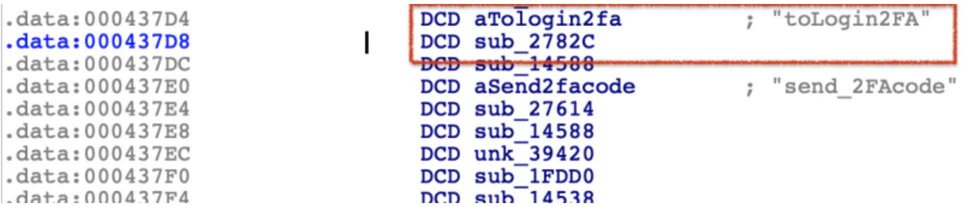
```
signed int __fastcall sub_273B0(void *a1, const char *a2, int a3)
{
  int v3; // r5
  const char *v4; // r6
  void *v5; // r8
  const char *v6; // r0
  char *v7; // r5
  int v9; // r0
  size_t v10; // r1
  const char *v11; // r3
  const char *v12; // r4
  int v13; // r7
  const char *v14; // r0
  char *v15; // r5
  char v16; // [sp+Ch] [bp-9Ch]
  char s; // [sp+4Ch] [bp-5Ch]
  int v18; // [sp+6Ch] [bp-3Ch]
  char dest; // [sp+71h] [bp-37h]
  char v20; // [sp+76h] [bp-32h]
  char v21; // [sp+7Ah] [bp-2Eh]
  char v22; // [sp+7Bh] [bp-2Dh]
  char v23; // [sp+80h] [bp-28h]

  v3 = a3;
  v4 = a2;
  v5 = a1;
  memset(&s, 0, 0x20u);
  strcpy((char *)&v18, "motp");
  strcpy(&dest, "totp");
  strcpy(&v20, "sms");
  v21 = 0;
  strcpy(&v22, "mail");
  snprintf(&v16, 0x40u, "/sbin/auth_check.sh Interface %s %s", v4, v3);
  v6 = sub_21904(&v16);
  v7 = (char *)v6;
  if ( v6 )
  {
    if ( !strcmp(v6, "NO-USE") )
    {
      free(v7);
      return 0;
    }
    free(v7);
  }
```



```
const char *__fastcall sub_21904(const char *a1)
{
  FILE *v1; // r4
  const char *v2; // r5
  size_t v3; // r4

  v1 = popen(a1, "r");
  v2 = (const char *)v1;
  if ( v1 )
  {
    v2 = (const char *)sub_1486C();
    pclose(v1);
    if ( v2 )
    {
      if ( *v2 )
      {
        v3 = (size_t)&v2[strlen(v2)];
```



```
.data:000437D4                 DCD aTologin2fa         ; "toLogin2FA"
.data:000437D8                 DCD sub_2782C
.data:000437DC                 DCD sub_14588
.data:000437E0                 DCD aSend2facode        ; "send_2FAcode"
.data:000437E4                 DCD sub_27614
.data:000437E8                 DCD sub_14588
.data:000437EC                 DCD unk_39420
.data:000437F0                 DCD sub_1FDD0
.data:000437F4                 DCD sub_14538
```

when http aciton=toLogin2FA can hacked

assign CVE-2020-19664

Releases

No releases published

Packages

No packages published