TEW-690AP backdoor vulnerability

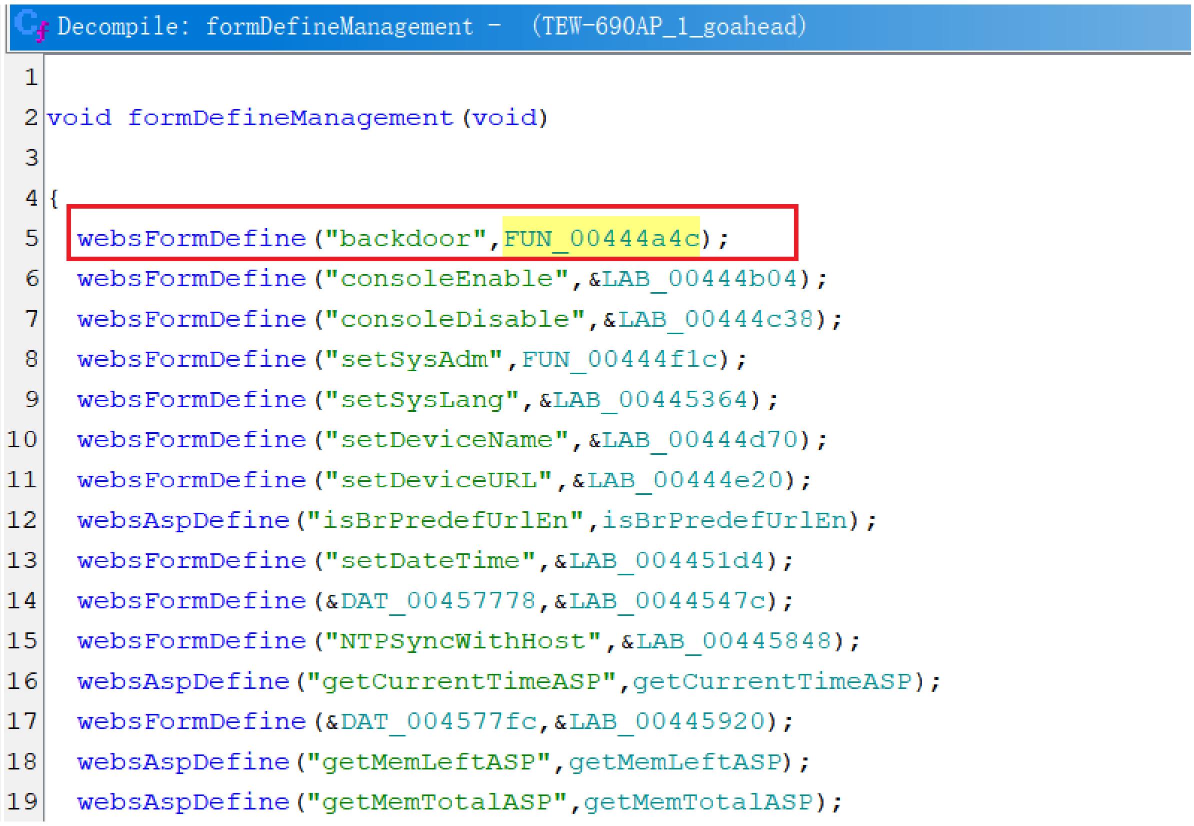
Affected firmware

Undocumented TELNET service in TRENDnet TEW-690AP when a web page named backdoor contains an HTML parameter of password and a value of j78G¬DFdg_24Mhw3.

Affected Version: TEW-690AP Version v3.0R

Details

There is an undocumented service called `backdoor` in the backend HTTP service binary `goahead`



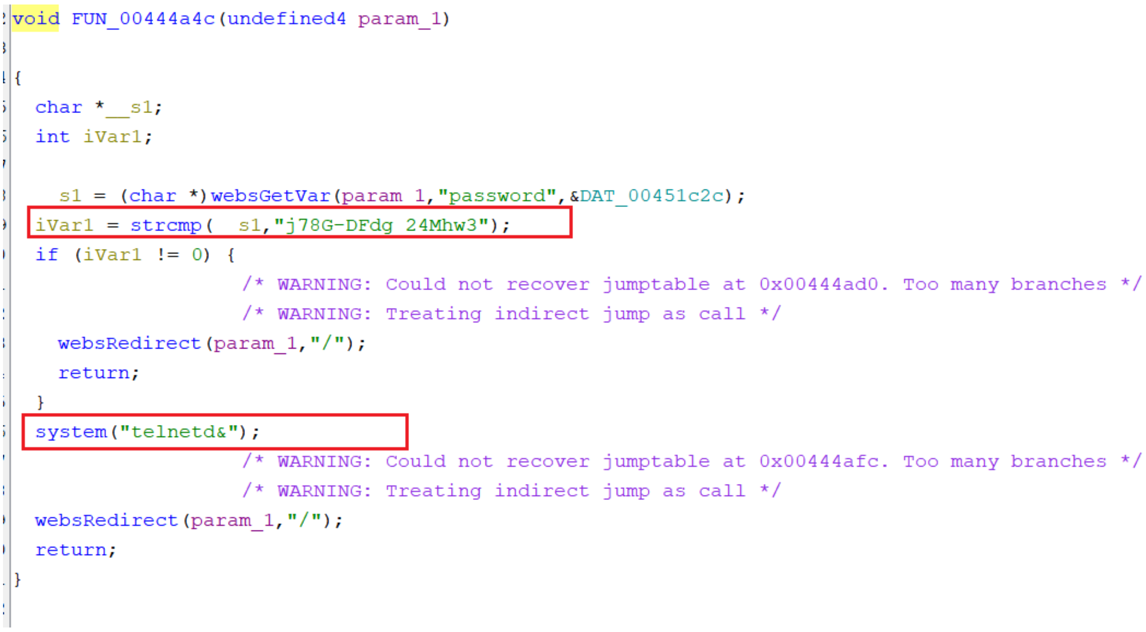
Decompile: formDefineManagement - (TEW-690AP_1_goahead)

```

void formDefineManagement(void)

{
  websFormDefine("backdoor",FUN_00444a4c);
  websFormDefine("consoleEnable",&LAB_00444b04);
  websFormDefine("consoleDisable",&LAB_00444c38);
  websFormDefine("setSysAdm",FUN_00444f1c);
  websFormDefine("setSysLang",&LAB_00445364);
  websFormDefine("setDeviceName",&LAB_00444d70);
  websFormDefine("setDeviceURL",&LAB_00444e20);
  websAspDefine("isBrPredefUrlEn",isBrPredefUrlEn);
  websFormDefine("setDateTime",&LAB_004451d4);
  websFormDefine(&DAT_00457778,&LAB_0044547c);
  websFormDefine("NTPSyncWithHost",&LAB_00445848);
  websAspDefine("getCurrentTimeASP",getCurrentTimeASP);
  websFormDefine(&DAT_004577fc,&LAB_00445920);
  websAspDefine("getMemLeftASP",getMemLeftASP);
  websAspDefine("getMemTotalASP",getMemTotalASP);
```

The handler of this backdoor service compares user input with a hard-coded string j78G-DFdg_24Mhw3, and opens telnet service if it passes authentication.



```
void FUN_00444a4c(undefined4 param_1)

{
  char *__s1;
  int iVar1;

    s1 = (char *)websGetVar(param 1,"password",&DAT_00451c2c);
  iVar1 = strcmp(  s1,"j78G-DFdg 24Mhw3");
  if (iVar1 != 0) {
                    /* WARNING: Could not recover jumptable at 0x00444ad0. Too many branches */
                    /* WARNING: Treating indirect jump as call */
    websRedirect(param_1,"/");
    return;
  }
  system("telnetd&");
                    /* WARNING: Could not recover jumptable at 0x00444afc. Too many branches */
                    /* WARNING: Treating indirect jump as call */
  websRedirect(param_1,"/");
  return;
}
```

This vulnerability is a recurring vulnerability of CVE-2013-3367. But this product has not been tagged with this vulnerability. So it should be assigned with another CVE id.