FinjectRoute

Report on 'httpd_20220819_190545'

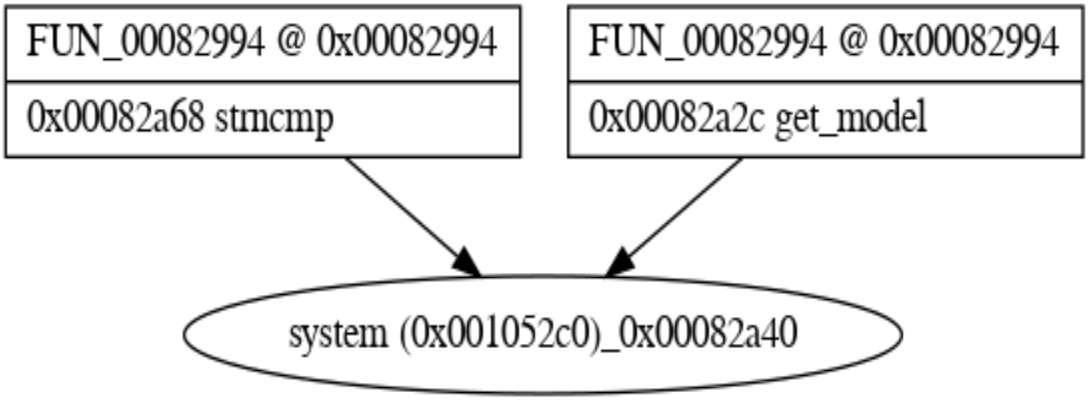
Date: 19-Aug-2022

Table of contents

Taint graphs on vulnerabilities

Vulnerable Graph #1 [system (0x001052c0) @ 0x00082a40]

Sink Name: system (0x001052c0)
Sink Address: 0x00082a40
Comments: *no comments*



Taint path details on vulnerabilities

Vulnerable Sink #1 [@ 0x00082a40]

Sink Name: system (0x001052c0)
Sink Address: 0x00082a40

Path #1 [system (0x001052c0)]

FUN_00082994 @ 0x00082994
`0x00082a68  strncmp`

Path #2 [system (0x001052c0)]

FUN_00082994 @ 0x00082994
`0x00082a2c  get_model`

Path #3 [system (0x001052c0)]

Appendix

FUN_00082994

```
void FUN_00082994(char *param_1)

{
    int iVar1;
    undefined4 uVar2;
    size_t sVar3;
    int iVar4;
    int *piVar5;
    int *piVar6;
    int *piVar7;
    char *pcVar8;
    char *__src;
    char acStack52 [8];
    char local_2c [6];
    undefined local_26;
    int local_24;

    local_24 = __stack_chk_guard;
    if ((*param_1 != '\0') && (iVar1 = FUN_0001a2d8(), iVar1 != 0)) {
        uVar2 = FUN_0007a854("rc_support");
        iVar1 = find_word(uVar2,"tcode");
        if (iVar1 != 0) {
            uVar2 = FUN_0007a854("territory_code");
            iVar1 = snprintf(acStack52,7,"%s",uVar2);
            if (0 < iVar1) {
                iVar1 = get_model();
                piVar5 = &tcode;_langcode_list;
                do {
                    piVar7 = piVar5;
                    iVar4 = *piVar7;
                    if (iVar4 == 0) goto LAB_00082a24;
                    piVar5 = piVar7 + 4;
                } while ((iVar4 != -1 && iVar1 != iVar4) ||
                                (iVar4 = strncmp((char *)piVar7[1],acStack52,2), iVar4 !=
0));
                pcVar8 = (char *)piVar7[2];
                sVar3 = strspn(pcVar8," ");
                pcVar8 = pcVar8 + sVar3;
                strncpy(local_2c,pcVar8,7);
                sVar3 = strcspn(local_2c," ");
                local_2c[sVar3] = '\0';
                local_26 = 0;
                pcVar8 = strchr(pcVar8,0x20);
                while (local_2c[0] != '\0') {
                    iVar4 = strcmp(local_2c,param_1);
                    if (iVar4 == 0) {
                        piVar5 = &tcode;_location_list;
                        goto LAB_00082b20;
                    }
                    __src = "";
```

```
                    if (pcVar8 != (char *)0x0) {
                        sVar3 = strspn(pcVar8," ");
                        __src = pcVar8 + sVar3;
                    }
                    strncpy(local_2c,__src,7);
                    sVar3 = strcspn(local_2c," ");
                    local_2c[sVar3] = '\0';
                    local_26 = 0;
                    pcVar8 = strchr(__src,0x20);
                }
            }
        }
    }
LAB_00082a24:
    uVar2 = 0;
    goto LAB_00082c44;
    while( true ) {
        pcVar8 = (char *)piVar7[3];
        iVar4 = strncmp((char *)piVar6[1],pcVar8,2);
        if (iVar4 == 0) break;
LAB_00082b20:
        do {
            piVar6 = piVar5;
            if (*piVar6 == 0) goto LAB_00082a24;
            piVar5 = piVar6 + 10;
        } while (iVar1 != *piVar6);
    }
    nvram_set("location_code",pcVar8);
    piVar5 = &location;_init_nvram_list;
    while( true ) {
        piVar6 = piVar5;
        piVar5 = piVar6 + 5;
        iVar4 = *piVar6;
        if (iVar4 == 0) break;
        if ((iVar4 == -1 || iVar1 == iVar4) &&
             (iVar4 = strcmp((char *)piVar6[2],(char *)piVar7[3]), iVar4 == 0)) {
            pcVar8 = (char *)piVar6[3];
            iVar4 = strcmp(pcVar8,"rc_support");
            if (iVar4 == 0) {
                add_rc_support(piVar6[4]);
            }
            else {
                nvram_set(pcVar8,piVar6[4]);
            }
        }
    }
    uVar2 = 1;
LAB_00082c44:
    if (local_24 == __stack_chk_guard) {
        return;
    }
                                        /* WARNING: Subroutine does not return */
    __stack_chk_fail(uVar2);
}
```

FUN_00082e68

```
void FUN_00082e68(int param_1)

{
    int iVar1;
    undefined4 uVar2;
    char *__s2;
    int iVar3;
    int *piVar4;
    int *piVar5;
    int iVar6;
    char *__s1;
    char acStack44 [8];
    int local_24;

    local_24 = __stack_chk_guard;
    if (DAT_000fa284 == 0) {
        if (param_1 != 0) {
            DAT_000fa284 = 1;
        }
        iVar1 = FUN_0001a2d8();
        if ((iVar1 != 0) || (iVar1 = is_passwd_default(), iVar1 != 0)) {
            uVar2 = FUN_0007a854("rc_support");
            iVar1 = find_word(uVar2,"tcode");
            if (iVar1 != 0) {
                uVar2 = FUN_0007a854("territory_code");
                iVar1 = snprintf(acStack44,7,"%s",uVar2);
                if (0 < iVar1) {
                    iVar1 = get_model();
                    __s2 = (char *)FUN_0007a854("odmpid");
                    if (param_1 == 0) {
                        piVar4 = &tcode;_lang_list;
LAB_00082f98:
                        do {
                            piVar5 = piVar4;
                            piVar4 = piVar5 + 5;
                            iVar6 = *piVar5;
                            if (iVar6 == 0) goto LAB_00082f28;
                            if ((iVar1 == iVar6) &&
                                 (((char *)piVar5[1] == (char *)0x0 ||
                                    (iVar3 = strcmp((char *)piVar5[1],__s2), iVar3 ==
0)))) {
                                __s1 = (char *)piVar5[2];
                                iVar6 = strncmp(__s1,acStack44,2);
                                if ((iVar6 == 0) || (iVar6 = strcmp(__s1,"GLOBAL"), iVar6
== 0)) break;
                                if (iVar1 != -1) goto LAB_00082f98;
                            }
                            else {
                                if (iVar6 != -1) goto LAB_00082f98;
                                __s1 = (char *)piVar5[2];
                                iVar6 = strncmp(__s1,acStack44,2);
                                if (iVar6 == 0) break;
                            }
                            iVar6 = strcmp(__s1,"GLOBAL");
```

```
                    } while (iVar6 != 0);
                    iVar1 = piVar5[4];
                    if (iVar1 != 0) {
                        iVar1 = 1;
                    }
                }
                else {
                    FUN_0007a854("preferred_lang");
                    iVar1 = FUN_00082994();
                }
                goto LAB_00083038;
            }
        }
LAB_00082f28:
        iVar1 = 1;
        goto LAB_00083038;
    }
}
iVar1 = 0;
LAB_00083038:
if (local_24 != __stack_chk_guard) {
                                    /* WARNING: Subroutine does not return */
    __stack_chk_fail(iVar1);
}
return;
}
```