trendnet several default credential vulnerability

In several trendnet products there exists default credential vulnerabilities which allows remote attacker to gain administrative privileges.

Affected products

1. TI-G160i with version v1_1.0.5.S0, https://www.trendnet.com/products/product-detail?prod=115_TI-G160i
2. TI-PG102i with version v1_1.0.11, v1_1.0.13 and v1_1.0.15, https://www.trendnet.com/store/products/industrial/10-Port-Industrial-Gigabit-L2-Managed-PoEplus-DIN-Rail-Switch-24-57V-TI-PG102i
3. TPL-430AP with version 1.0.1, https://www.trendnet.com/products/powerline/wifi-everywhere-powerline-1200-av2-wireless-access-point-TPL-430AP

Details

These products contains a Use of Weak Credential vulnerability.

TI-PG102i and TI-G160i series

In the /etc/passwd file, there contains the following contents

```
root:$1$$f83ImQzueI8CSjBqf4l921:0:0:root:/root:/bin/sh
bin:*:1:1:bin:/bin:/sbin/nologin
```

Several services uses the credential for authentication。 For example, the `dropbear` service, which is the same as ssh services for embedded systems, uses `getpwnam` to retrive contents from `/etc/passwd` for authentication.

```
1  int __fastcall login_init_entry(char *a1, int a2, int a3, int a4, int a5, int a6, int a7, int a8, int a9)
2  {
3    const char *v12; // $s2
4    struct passwd *v14; // $v0
5
6    v12 = a1 + 144;
7    memset(a1, 0, 0x260u);
8    *((_DWORD *)a1 + 18) = a2;
9    if ( a9 )
10     line_fullname(a1 + 80, a9, 64);
11   if ( a3 )
12   {
13     strlcpy(v12, a3, 64);
14     v14 = getpwnam(v12);
15     if ( !v14 )
16       v14 = (struct passwd *)dropbear_exit("login_init_entry: Cannot find user \"%s\"", v12);
17     *((_DWORD *)a1 + 19) = v14->pw_uid;
18   }
19   if ( a4 )
20     strlcpy(a1 + 208, a4, 256);
21   return 1;
22 }
```

By decrypting the credentials, unauthenticated attackers can decrypt these file and issue unauthorized attack.

TPL-430AP

The etc/shadow file contains the following contents, which is used for authentication in the `dropbear` binary

```
root:$1$BOYmzSKq$ePjEPSpkQGeBcZjlEeLqI.:13796:0:99999:7:::
```

```
int svr_auth_password()
{
  const char *v0; // $s2
  struct spwd *v1; // $v0
  char *sp_pwdp; // $v0
  const char *v3; // $s0
  char *v4; // $s1
  int v6[3]; // [sp+18h] [-Ch] BYREF

  v0 = (const char *)dword_43A720;
  v1 = getspnam((const char *)dword_43A71C);
  if ( v1 )
  {
    sp_pwdp = v1->sp_pwdp;
    if ( sp_pwdp )
      v0 = sp_pwdp;
  }
  if ( *v0 )
  {
    if ( !buf_getbool(dword_43A690, 4325376) )
    {
      v3 = (const char *)buf_getstring(dword_43A690, v6);
      v4 = crypt(v3, v0);
      m_burn(v3, v6[0]);
      _m_free(v3);
      if ( !strcmp(v4, v0) )
      {
        dropbear_log(
          5,
          "password auth succeeded for '%s' from %s",
          (const char *)dword_43A71C,
          (const char *)dword_43A768);
        return send_msg_userauth_success();
      }
      dropbear_log(4, "bad password attempt for '%s' from %s", (const char *)dword_43A71C, (const char *)dword_43A768);
    }
  }
  else
  {
    dropbear_log(4, "user '%s' has blank password, rejected", (const char *)dword_43A71C);
  }
  return send_msg_userauth_failure(0, 1);
}
```