Ubiquiti several Hard-coded credential Vulnerability

Affected firmware and version

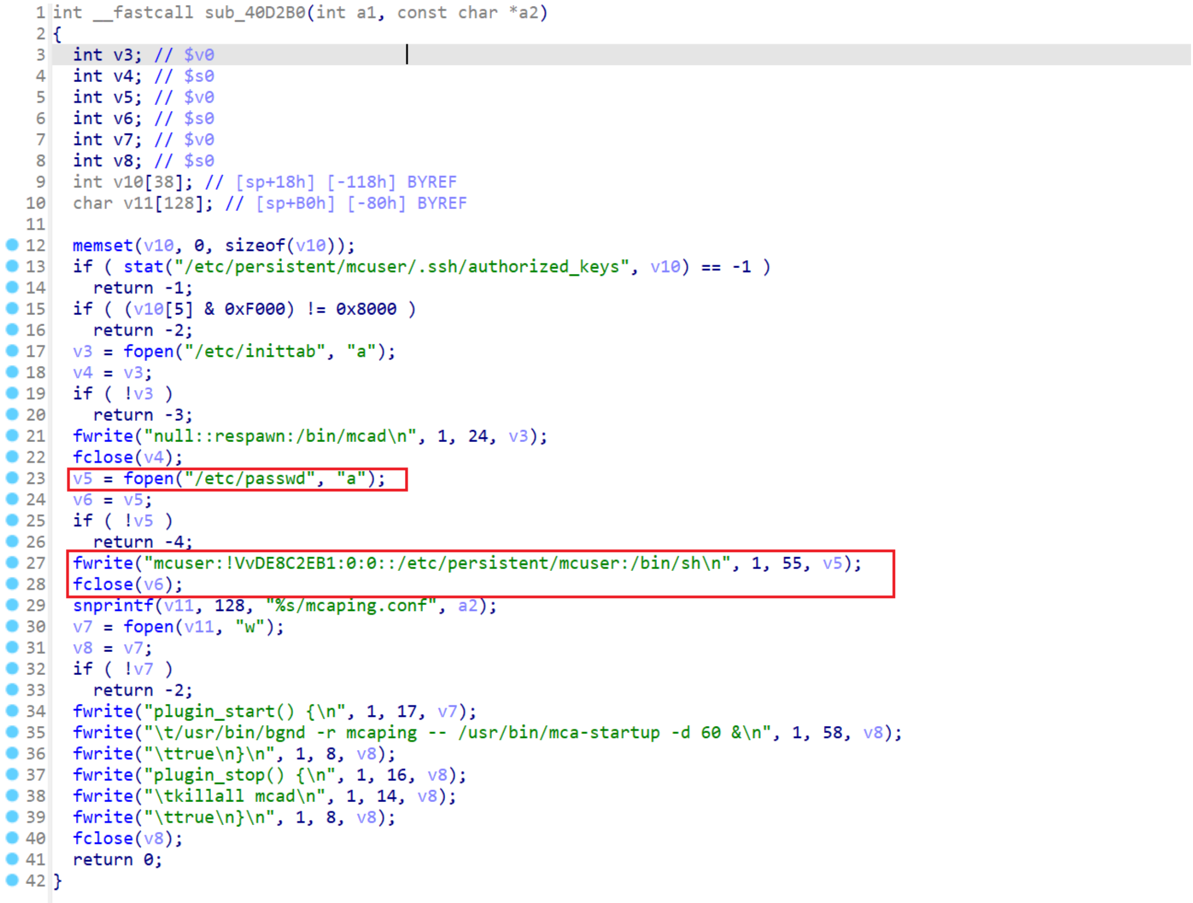
- GigaBeam,v1.4.2
  - GBE.v1.4.2.a96cd2e9.230330.1133.bin
  - URL: https://fw-download.ubnt.com/data/unifi-firmware/4c9a-UBB-1.0.7-9ff2dcefaa25471298e709680726544a.bin
- TI board,v6.3.11
  - Version: TI.v6.3.11.33396.230425.1547.bin
  - URL: https://dl.ubnt.com/firmwares/XN-fw/v6.3.11/TI.v6.3.11.33396.230425.1547.bin
- XM board,v3.6.11
  - XM.v6.3.11.33396.230425.1742.bin
  - URL: https://dl.ubnt.com/firmwares/XN-fw/v6.3.11/XM.v6.3.11.33396.230425.1742.bin
- EdgePower,v1.9.0
  - EP.v1.9.0.a67ced.210524.1407.bin
  - https://dl.ubnt.com/firmwares/edgemax/EdgePower/v1.9.0/EP.v1.9.0.a67ced.210524.1407.bin
- XC board,v8.7.0
  - XC.v8.7.11.42152.200203.1256.bin
  - https://dl.ubnt.com/firmwares/XC-fw/v8.7.11/XC.v8.7.11.46972.220614.0419.bin
- TI board,v6.3.6
  - TI.v6.3.6.33330.210818.1900.bin
  - https://dl.ubnt.com/firmwares/XN-fw/v6.3.6/TI.v6.3.6.33330.210818.1900.bin
- 2WA board,v8.7.4
  - 2WA.v8.7.4.45112.210415.1103.bin
  - https://dl.ubnt.com/firmwares/XC-fw/v8.7.4/2WA.v8.7.4.45112.210415.1103.bin
- 2XC board,v8.7.8
  - 2XC board,v8.7.8
  - https://dl.ubnt.com/firmwares/XC-fw/v8.7.8/2XC.v8.7.8.46705.220201.1820.bin

Description

The above Ubiquiti firmware contains Use of Weak Credential vulnerability. The root credential is embedded in binary `ubntbox`. During firmware startup, the following hard-coded credential will be written into `etc/passwd`.

In the following code, The below line 23 opens `/etc/passwd`, then it writes the following constant string into `etc/passwd`,

```
mcuser:!VvDE8C2EB1:0:0::/etc/persistent/mcuser:/bin/sh
```



```
int __fastcall sub_40D2B0(int a1, const char *a2)
{
  int v3; // $v0
  int v4; // $s0
  int v5; // $v0
  int v6; // $s0
  int v7; // $v0
  int v8; // $s0
  int v10[38]; // [sp+18h] [-118h] BYREF
  char v11[128]; // [sp+B0h] [-80h] BYREF

  memset(v10, 0, sizeof(v10));
  if ( stat("/etc/persistent/mcuser/.ssh/authorized_keys", v10) == -1 )
    return -1;
  if ( (v10[5] & 0xF000) != 0x8000 )
    return -2;
  v3 = fopen("/etc/inittab", "a");
  v4 = v3;
  if ( !v3 )
    return -3;
  fwrite("null::respawn:/bin/mcad\n", 1, 24, v3);
  fclose(v4);
  v5 = fopen("/etc/passwd", "a");
  v6 = v5;
  if ( !v5 )
    return -4;
  fwrite("mcuser:!VvDE8C2EB1:0:0::/etc/persistent/mcuser:/bin/sh\n", 1, 55, v5);
  fclose(v6);
  snprintf(v11, 128, "%s/mcaping.conf", a2);
  v7 = fopen(v11, "w");
  v8 = v7;
  if ( !v7 )
    return -2;
  fwrite("plugin_start() {\n", 1, 17, v7);
  fwrite("\t/usr/bin/bgnd -r mcaping -- /usr/bin/mca-startup -d 60 &\n", 1, 58, v8);
  fwrite("\ttrue\n}\n", 1, 8, v8);
  fwrite("plugin_stop() {\n", 1, 16, v8);
  fwrite("\tkillall mcad\n", 1, 14, v8);
  fwrite("\ttrue\n}\n", 1, 8, v8);
  fclose(v8);
  return 0;
}
```

Malicious attacker can reverse engineer the firmware and decrypt and gain the credential to log into the firmware.

Security Compliance

According to the **NIST SP 800-63B** Digital Identity Guidelines, predictable or static passwords (even if hashed) are not allowed for initial user authentication.

https://pages.nist.gov/800-63-3/sp800-63b.html

> Memorized secrets that are randomly chosen by the CSP (e.g., at enrollment) or by the verifier (e.g., when a user requests a new PIN) SHALL be at least 6 characters in length and SHALL be generated using an approved random bit generator [SP 800-90Ar1].