OpenSource Security Ralf Spenneberg
Am Bahnhof 3-5
48565 Steinfurt
info@os-s.net

OS-S Security Advisory 2016-19

Title: Epson WorkForce multi-function printers do not use signed firmware images and allow unauthorized malicious firmware-updates

Authors: Yves-Noel Weweler <y.weweler@gmail.com>, Ralf Spenneberg <ralf@os-t.de>, Hendrik Schwartke <hendrik@os-t.de>

Date: September 26th 2015

Vendor contacted: September 29th 2015

Vendor response: December 12th 2015

Updated firmware available: January 28th 2016

CVSS: 10

Abstract

Epson multi function printers support firmware-Updates via USB and HTTP. When using HTTP, the update is initialized with a GET request and the firmware is uploaded via a POST request. No authorization is required. An attacker can exploit this unauthorized mechanism using Cross-Site-Request-Forgery (CSRF). Because the firmware itself is neither encrypted nor digitaly signed an attacker can create malicious firmware images including backdoors and other malware.

Impact

Very High. Epson is the third largest printer manufacturer worldwide and sells millions of devices with this vulnerability. If this devices are network enabled, an attacker can upload malicious firmware directly or implicitly using CSRF. We were able to craft and install a malicious firmware image implementing a backdoor using the builtin data/fax modem. This backdoor may serve as a bridge head in to a network otherwise not connected to the internet.

Exploit

Exploit code just needs to mimic the HTTP update mechanism directly or using CRSF.

With a basic understanding of the firmware format and checksums, an attacker can create malicious firmware images including backdoors and malware for the devices.

Vulnerable

Tested: Epson WF-2540 MFP

Not-tested but probable after inspection of the firmware and IPv4-scans are most of the devices in the WorkForce and Stylus series.

We believe huge amounts of the devices produced since 1999 to use this mechanism and could be vulnerable.

Technical description

Firmware provided for these devices consists of an embedded linux operating system

packaged in Epson's proprietary firmware format. This format is not digitaly signed. With basic knowlege of the checksums used in the firmware an attacker is able to create a malicious firmware image.

Using the HTTP based firmware update mechanism this firmware may be installed like follows:

1. Initialize update

```
    GET /FIRMWAREUPDATE HTTP/1.1\r\n

    Accept: */*\r\n

    Connection: Keep-Alive\r\n

    \r\n
```

2. Upload firmware

```
   POST /DOWN/FIRMWAREUPDATE/ROM1 HTTP/1.1\r\n

    Accept: */*\r\n

    Content-Type: multipart/form-data;
boundary=---------------------------

        EPSONOP2HANAOKAGROUP1999\r\n

    Content-Length: xxx\r\n

    Connection: Keep-Alive\r\n

    \r\n

    ---------------------------EPSONOP2HANAOKAGROUP1999\r\n
    Content-Disposition: form-data; name=``fname'';
filename=``/DUMMY.DAT''\r\n

    Content-Type: application/octet-stream\r\n

    \r\n

    insert firmware here

    \r\n

    ---------------------------EPSONOP2HANAOKAGROUP1999--\r\n
```

After uploading the firmware the device automatically installs the image. Since this mechanism does not require any authorization and no further counter-measures against CSRF are met, an attacker can easily upload new firmware.

Solution

A Modification of the Upgrade Mechanism is required.

Vendor Response

Epson responded on December 2nd 2015 (Quote):

[Vulnerability]
WF-2540 MFP has the vulnerability that you kindly advised. However firmware check function by our original algorithm has been implemented to the current products as the countermeasure for the vulnerability, and it will be implemented to all the future products also.

[Solution]
We will release new firmware for WF-2540 by the end of January, 2016. (It will be delivered to a customer by a firmware updater (utility) from our internet server or website.) In addition, we may be willing to provide a new firmware for other older products corresponding to the request by a customer.

[Network security for our products]
We are going to publish network security guidance for customers so that they will mitigate the effects of this issue by following the guidance.