HMS Security Advisory Report

HMSSAR-2015-12-16-001
Publication date: 16 December 2015

Ewon Security Enhancement (FW 10.1s0)

Ewon SECURITY ENHANCEMENT Ref: #7529-01

Ewon Reference: Ewon Login Session Improvement

Affected devices: All Ewon devices

Affected firmware versions: All firmware versions inferior to 10.1s0

Impact/description:

The log off button displays a message recommending the user to close the browser to completely invalidate session. The session remains indeed active until the browser is closed.

Mitigating factors:

None.

Solution (since version 10.1s0):

In order to logout users without having to close the browser we included a mechanism that clears the current Basic Authentication credentials.

The log off button actually invalidate the current user browser session and it is then not anymore mandatory to close the browser to completely log off.

-----

Ewon Reference: Limited CSRF Exposure

Affected devices: All Ewon devices

Affected versions: All firmware versions

Impact/description:


Any form on Ewon firmware can be directly submitted and executed according to its user credentials requirements through the browser URL.

By extension there are no mechanism granting temporary access to a specific form for any logged user. All forms can then be submitted by a logged user through the URL even if he/she is not currently on the form page and thus without forcing the user to click on any form button.

That feature implies any logged user on an Ewon could for instance execute a form by clicking on a link received in a fraudulent email.

**Mitigating factors:**

Many requirements have to be met for a successful attack:

The attacker needs a valid login to the Ewon.

The attacker needs HTTP access to the Ewon (e.g. Ewon web server exposed to the public Internet).

Also connections to Ewon devices should in standard use cases only occur through:

- a point-to-point LAN, a secured LAN (sniffing the victim IP is not really achievable in these two cases)

- or a secured VPN (VPN allocated IP address is then defined by the VPN server).

**Solution / Advice:**

Always connect to Ewon in a closed work environment using a point-to-point LAN, a secured LAN or through a secured VPN (for instance using Talk2M).

-----

**Ewon Reference: Improved User Rights Management**

**Affected devices:** All Ewon devices

**Affected versions:** All firmware versions inferior to 10.1s0

**Impact/description:**

Using a forged URL, an unprivileged connected user could gather informations and status of I/O servers.

Using a forged URL, an unprivileged connected user could impact I/O servers configuration parameters or delete some users.
Mitigating factors:

These informations are already available through Ewon User Manual. No user's specific information is disclosed.

Solution (since version 10.1s0):

User Rights Management has been improved. The IO servers page don't leak informations to unprivileged users anymore.

User Rights Management has been improved. Any unprivileged access is now prevented.

-----

Ewon Reference: Limited Cross-Site Scripting exploit

Affected devices: All Ewon devices

Affected versions: All firmware versions

Impact/description:

It is possible to save html <script> tags inside some Ewon configuration form fields (user firstname and lastname, user information, tag description) and to include <script> tags inside form status messages querystring through browser URL. This offers the possibility to execute remote scripts that could possibly access informations from the Users or Tags pages.

Mitigating factors:

All these XSS exploits require at least to be authenticated on Ewon and to have configuration modification right.

Solution / Advice:

Such hijacking of Ewon form fields is not considered a real threat since it can be done by an Ewon admin only.

------

Ewon Reference: Password visibility

Affected devices: Ewon Flexy/CD

Affected versions: All firmware versions
Impact/description:

It is possible to "sniff" passwords when the firmware website is accessed through standard non-secure HTTP.

Furthermore the autocomplete feature integrated with the evergreen browsers might suggest in clear text previous passwords in the Ewon User Setup creation/edition page.

Mitigating factors:

Connections to Ewon devices should only be done through a point-to-point LAN, a secured LAN or a secured VPN. Sniffing is thus not a valid attack use case as it concerns closed work environment (limited connectivity) or secure environment.

Regarding the second issue the internet browser is supposed to be manipulated by the Ewon administrator only as the page that leaks passwords requires configuration management right.

Solution / Advice:

Always connect to Ewon using a closed work environment (limited connectivity) using a point-to-point LAN, a secured LAN or a secured VPN (for instance using Talk2M).

Since Ewon firmware version 10.1s0 we disable password fields auto completion.

Ewon Reference: Ewon web server requests payload interpretation

Affected devices: Ewon Flexy/CD

Affected versions: All firmware versions

Impact/description:

The Ewon firmware web server doesn't make any difference between POST and GET parameters and thus any form submitted can be reproduced using a simple URL.

Mitigating factors:

This could be an issue regarding the CSRF attacks described above. However as already mentioned the Ewon firmware exposure to CSRF attacks is really limited. Thus having equivalent POST and GET parameters handling for each request sent to the Ewon webserver is by extension not problematic.

Solution / Advice:
Always connect to Ewon using a closed work environment (limited connectivity) using a point-to-point LAN, a secured LAN or a secured VPN (for instance using Talk2M).