Table of Contents

1. INTRODUCTION

ABB Drives SREA-01 and SREA-50 monitoring products are based on legacy Netbiter hardware and software versions from HMS Industrial Networks AB. Products have a software version which is no longer actively maintained. In May/June 2017 a security issue was announced:

> "Bertin Jose and Fernandez Ezequiel has found a vulnerability in legacy NetBiter products.
> The vulnerability can make files in the product's internal filesystem accessible by non-authenticated users.
> By using the vulnerability, the internal password file can be retrieved and then the password can be identified using a brute force attack of the password hash.
> When the password is decoded the attacker is able to login to the device."

Successful exploitation of this vulnerability may allow a remote attacker to remotely log in to the target device and viewing data, change device configuration and send commands to connected devices.

A Software patch for HMSSAR-2017-05-24-001 has been released to fix the described issue. This document is bundled with ABB specific patch ABBVU-RMDR-3AXD10000621970. This document describes how to install the patch.

2. SECURITY RECOMMENDATIONS FOR SREA-01 AND SREA-50

It is highly recommended to install the provided patch, which will blocks the reported security issues. However in addition to applying the patch, ABB recommends the following mitigations:

- VPN (Virtual Private Networking) access should be used to connect to the web interface of the SREA-01 module from further locations than the local network, as the web pages use unencrypted HTTP communication.
    - The VPN solution including devices and software should be also kept up to date with latest security information
    - The web interface of the SREA-01 and SREA-50 Remote Monitoring Tools should never be exposed directly to public Internet.

- Recommended security practices and firewall configurations can help protect the Remote Monitoring Tools from attacks that originate from outside the network. Such practices include that Remote Monitoring tools are physically protected from direct access by unauthorized personnel, have no direct connections to the Internet, and are separated from other networks by means of a firewall system that has a minimal number of ports exposed, and others that have to be evaluated case by case. Portable computers should be carefully scanned for viruses before they are connected to the network.

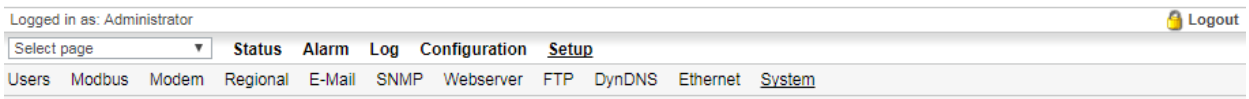
- More information on recommended practices can be found in the following documents: 3AXD10000492137, Technical guide: Cybersecurity for ABB drives

3. APPLYING THE PATCH TO FIX THE ISSUE

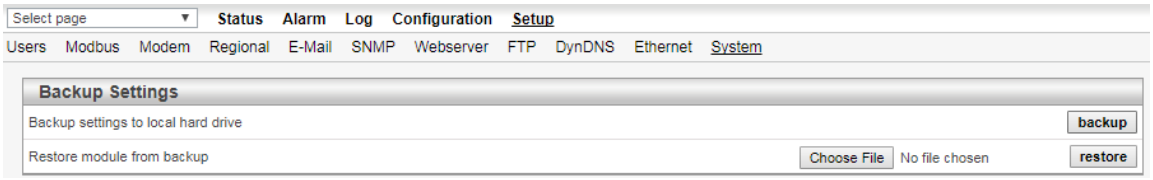
On ABB SREA-01 the patch can be applied as follows:

1. Log in as administrator:

2. Navigate to main menu bar item Setup

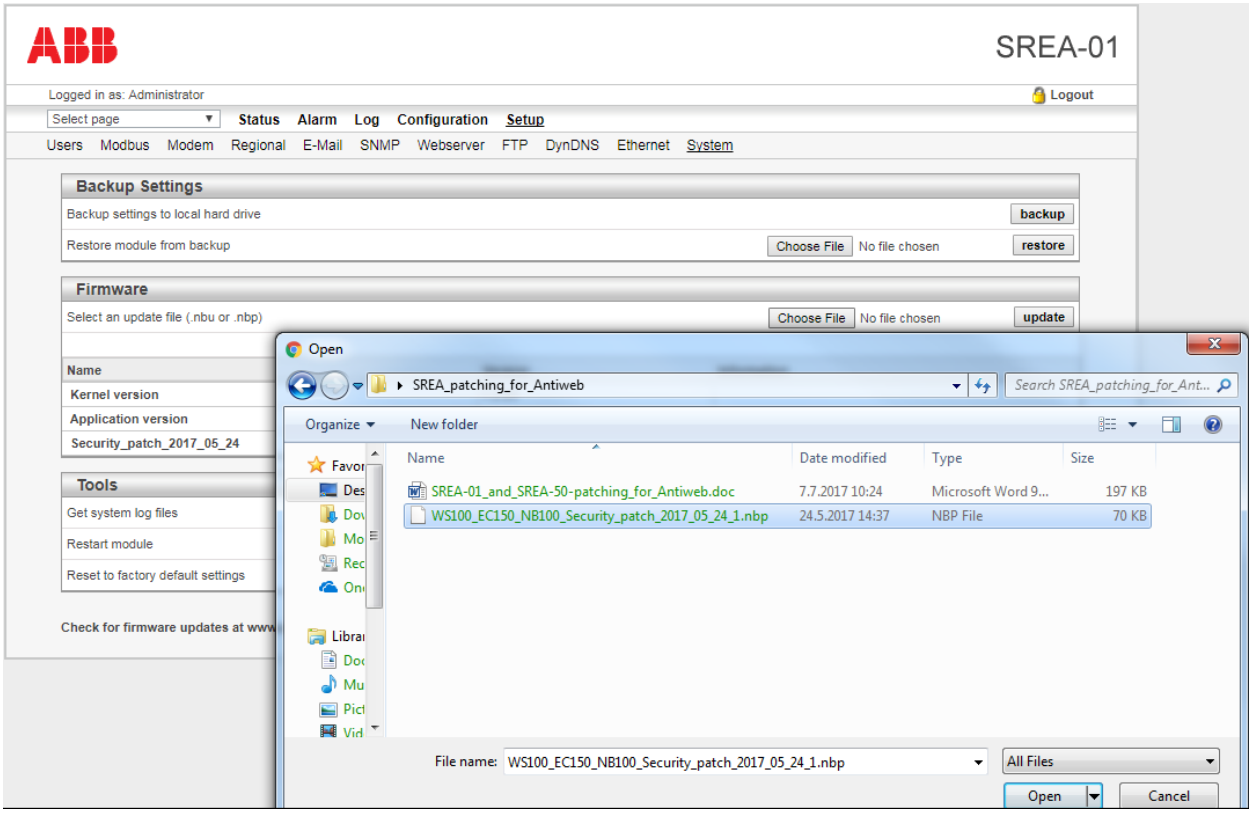


3. Navigate to sub navigation bar (gray background) item System
    a. Recommended step: take a backup of SREA-01 setting by clicking the button “backup” next to text “Backup settings to local hard drive”. Store the settings backup in case if patching fails and if would need to restore factory settings.

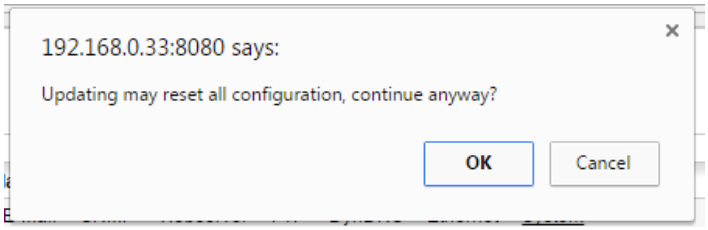


4. Find on the page a panel titled “Firmware”

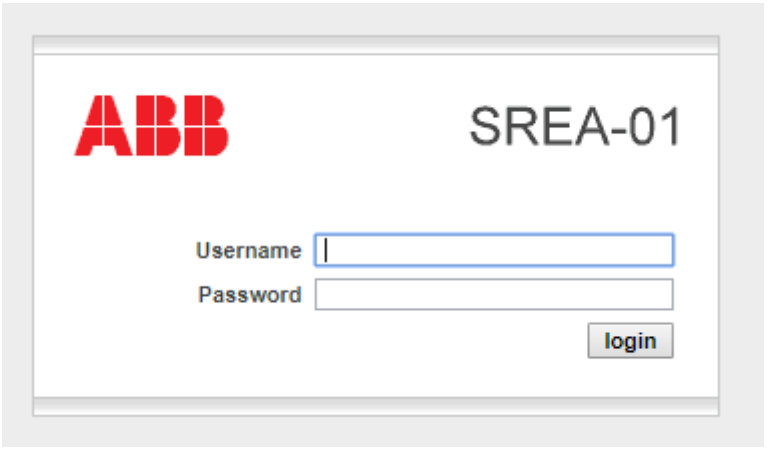
5. Within the “Firmware” panel click button “Choose file”
6. Navigate to extracted patch files, choose file WS100_EC150_NB100_Security_patch_2017_05_24_1.nbp



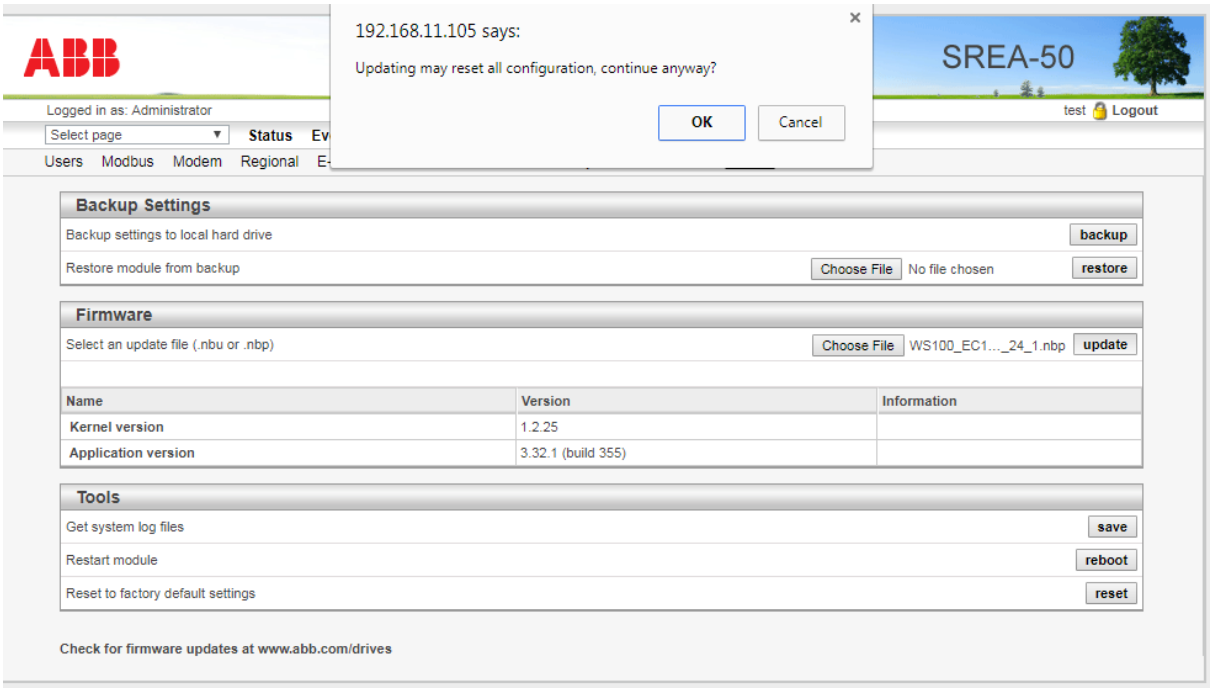
7. Choose the file and click “Update”
8. When a dialog box appears asking whether to continue, click OK



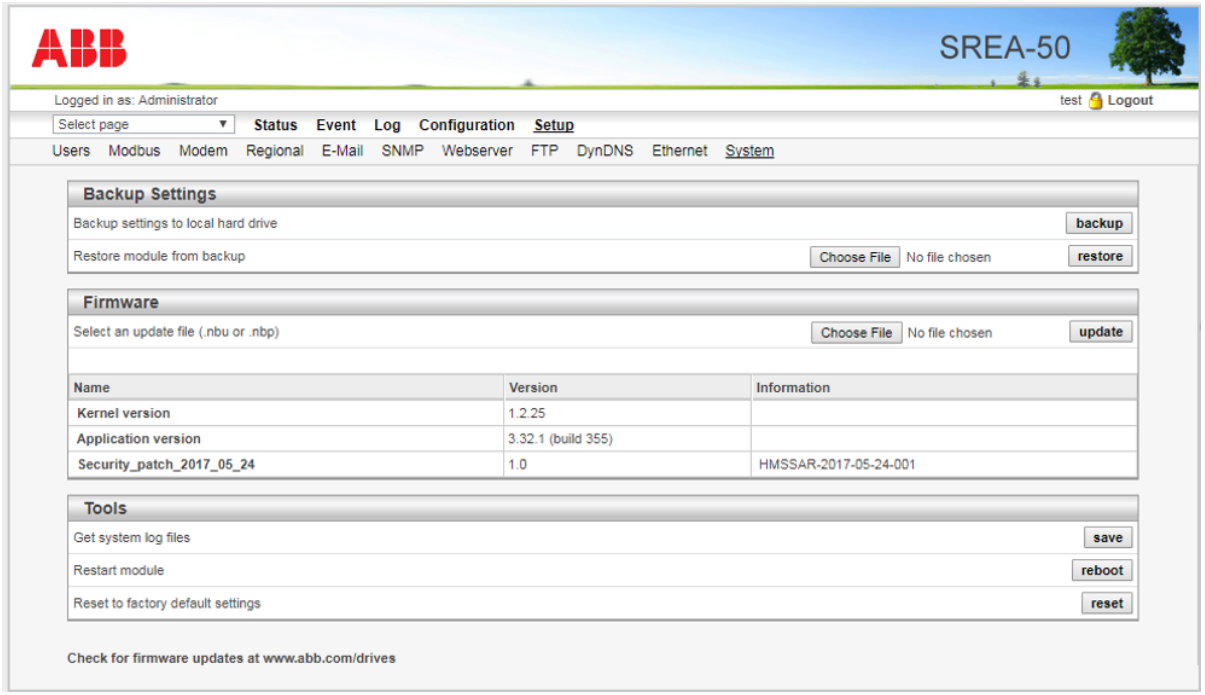
9. After a successful update you should be directed back to login page of the SREA-01:



Patching procedure is similar for the SREA-50 as described for the SREA-01 except for the page layout. An example while of applying the patch for a SREA-50 using Chrome web browser:

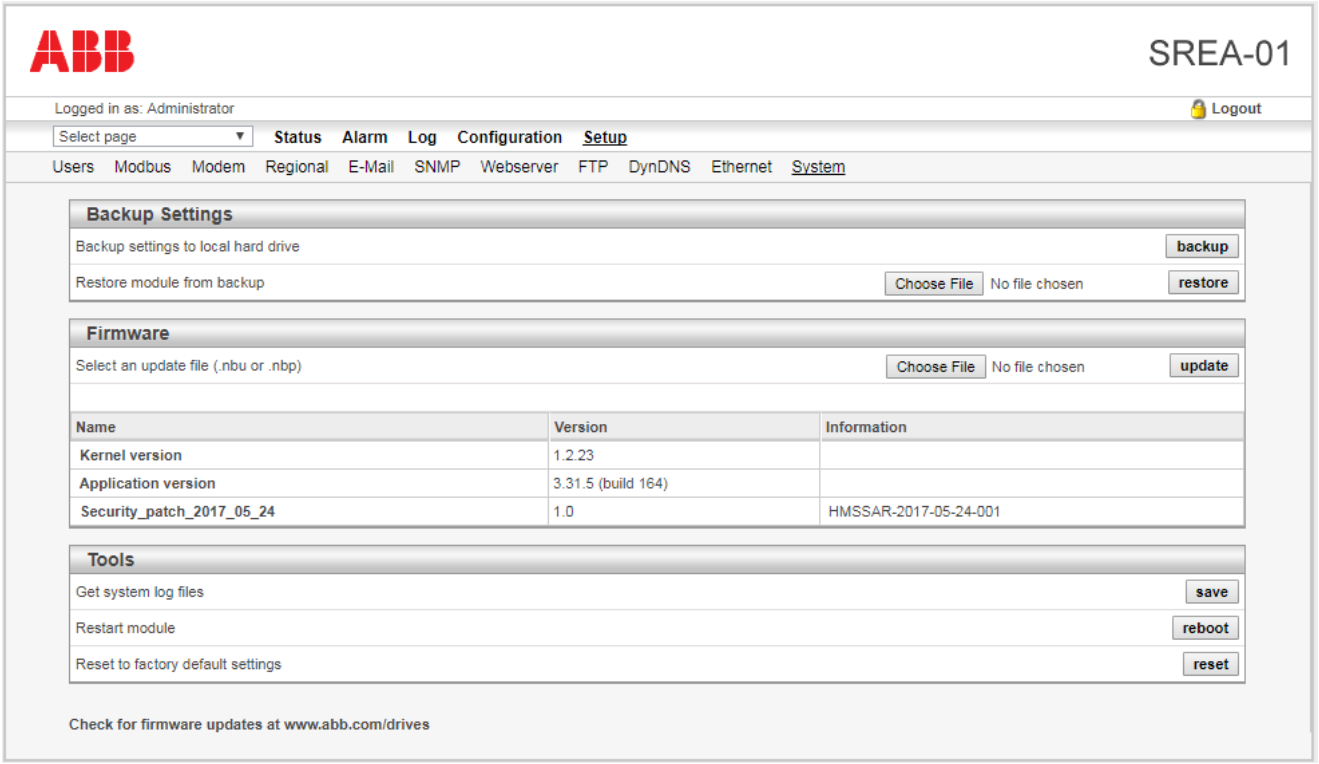


... and after applying the patch for SREA-50



4. VERIFYING THE INSTALLATION OF THE PATCH

Patch can be verified after logging in, under the Setup -> System, Firmware section, as an additional software name and version ("Security_patch_2017_05_24"):



5. DOCUMENT VERSION HISTORY

2017-07-10	Draft	Initial instruction, ready for getting a document number
2017-07-10	Rev. A	Added screenshots after patching
2017-08-11	Rev. B	Updated screenshots. SREA-50 screenshot included.