

29 November 2016

Security Advisory 2016/11/29

2016/11/29 – Phoenix Contact GmbH & Co. KG

Synopsis

A firmware update to version 8.4.0 resets the password of the user “admin”.

The update files were available between Nov. 19, 2016 and Nov 25, 2016 on the Phoenix Contact web pages.

Issue

When updating an mGuard device to version 8.4.0 via the update-upload facility, the update will succeed but it will reset the password of the “admin” user to its default value “mGuard”.

Affected products

Only devices that have been updated to version 8.4.0 are affected. Other versions are not affected by this issue.

Details

During an update the new firmware will be installed on a second partition. During this process the current configuration, all existing configuration profiles and the system-user credentials that are not part of the configuration are copied from the old firmware installation partition. The mechanism to initially set the “admin” password when flashing the device was also executed during the update, which did reset his password.

Mitigation

Use the update to version 8.4.1 (or higher, if applicable). If an update to version 8.4.0 already has been performed, please change the “admin” password via WebUI or command line. If SSH or HTTPS access was possible from untrusted sources after an update to version 8.4.0, please flash the device and exchange all private keys and passphrases in the configuration.