PHOENIX CONTACT GmbH & Co. KG
Flachsmarktstraße 8
32825 Blomberg, Germany
Telefon: +49 5235 300
Telefax: +49 5235 3-41200
Internet: http://www.phoenixcontact.com
USt-Id-Nr.: DE124613250
WEEE-Reg.-Nr.: DE50738265

PHOENIX CONTACT GmbH & Co. KG · 32825 Blomberg

11 May 2017
S1: 300373012/pbsa56

Security Advisory for mGuard products [CVE-2017-7937]

Synopsis

Unauthorized User-Firewall login with RADIUS.

Affected products

All Phoenix Contact and Innominate Security Technologies devices running the mGuard Firmware 8.4.0 to 8.4.2 with enabled User-Firewall and RADIUS authentication.

Issue

An attacker could use a known login name with any password to login to the User-Firewall whilst configured RADIUS server(s) are unreachable to enable the firewall rules configured for this login. The administrative login to mGuard with RADIUS authentication is not affected.

Preconditions:

- The User-Firewall is enabled and a user with RADIUS login or “RADIUS group authentication” is enabled.
- The User-Firewall login is permitted for the interface the attacker uses to login.
- The login name used by the attacker is not configured with local password.

Details

The User-Firewall authentication via RADIUS server takes any error like an unreachable server as successful login. A proper RADIUS reject message still rejects the login attempt.

Mitigation

Customers using this feature with vulnerable Firmware versions are recommended to update to firmware version 8.5.0 or higher which fixes this vulnerability.