

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: 300372960/pbsa56

Security Advisory for mGuard products [CVE-2017-7935]

Synopsis

Denial of Service against IPsec.

Affected products

All Phoenix Contact and Innominate Security Technologies devices running mGuard Firmware 8.3.0 to 8.4.2 using IPsec connections.

Issue

When an mGuard receives too many initial main/aggressive requests exceeding the licensed amount of VPN channels within a short period, no further initial main/aggressive mode requests will be accepted until the mGuard is rebooted.

Details

The mGuard allows a limited number of not completely established main/aggressive mode sessions. When reaching this limit, it will reject any further connection attempts. Due to an implementation issue, each rejection will result in an unestablished main/aggressive mode session of infinite lifetime.

<u>Mitigation</u>

Customers using IPsec VPN with vulnerable Firmware versions are strongly encouraged to update to firmware version 8.5.0 or higher which fixes this vulnerability.

Executive Vice Presidents: Frank Stührenberg (CEO) Roland Bent

Deutsche Bank AG (BLZ 360 700 50) 226 2665 00 BIC: DEUTDEDEXXX **IBAN** DE93 3607 0050 0226 2665 00

Commerzbank AG (BLZ 476 400 51) 226 0396 00 **BIC: COBADEFFXXX IBAN** DE31 4764 0051 0226 0396 00