

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.

### Mitigation

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.