Rudower Chaussee 13
12489 Berlin
T +49 30 921028-0
F +49 30 921028-020
www.innominate.com

Innominate AG ▪ Rudower Chaussee 13 ▪ 12489 Berlin

# Security Advisory 2014/12/17-002

2014/12/17 - Innominate Security Technologies AG, Berlin, Germany

## Synopsis

Denial of Service attack against the mGuard IPSec TCP encapsulation

## Issue

The mGuard TCP encapsulation of IPSec traffic uses an OpenVPN connection to tunnel IPSec packets. Because of CVE-2014-8104 an attacker may interrupt such TCP encapsulated connections.

## Reference

CVE-2014-8104

## Affected products

All Innominate mGuard devices running with firmware version 6.1.0 up to firmware version 8.1.3 are affected if listening for TCP encapsulated connections is enabled. The firmware versions 8.1.4 and higher are not affected. The mGuard firmware 7.6.6 patch release also fixes this issue.

## Details

In case the “Listening for incoming TCP encapsulated VPN connections” option is set and TCP encapsulated connections are used, an attacker may restart the TCP Encapsulated connections. The attack requires mGuard specific settings to be successful.
Non TCP encapsulated IPSec connections are not affected nor interrupted. This issue does not affect the data integrity or confidentiality of TCP encapsulated connections.

## Mitigation

All users of the affected Innominate mGuard devices may either update to one of the fixed firmware versions or disable the TCP encapsulation option mentioned above.