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 2015/07/14-001

2015/07/14 - Innominate Security Technologies AG, Berlin, Germany

Synopsis

Temporary denial of service during VPN Phase II (IPsec SA) establishment

Issue

A specifically crafted configuration sent during the establishment of VPN Phase II (IPsec SA) may cause a temporary outage of the VPN service on the remote side.

Reference

CVE-2015-3966

Affected products

All Innominate mGuard devices running firmware versions 8.0.0 to 8.1.6 are affected. Firmware version 7 is not affected.

Details

If a VPN peer sends a specifically crafted configuration during the establishment of the IPsec SA, it may cause a restart of the VPN service on the remote VPN peer. To exploit this vulnerability, a successful authentication via X.509 certificate or Pre-Shared Secret Key is required.

Mitigation

All users of the affected Innominate mGuard devices may update to firmware version 8.1.7 which fixes this vulnerability.