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 2015/04/07-001

2015/04/07 - Innominate Security Technologies AG, Berlin, Germany

Synopsis

RSA silently downgrades to EXPORT_RSA [Client] (known as FREAK)

Issue

A Man-in-the-middle may force the server to use export-grade ciphers, which will be accepted by the HTTPS client on the mGuard.

Reference

CVE-2015-0204

Affected products

All Innominate mGuard devices running with firmware versions up to 8.1.4 are affected. The firmware versions 8.1.5 and higher are not affected. The mGuard firmware 7.6.8 patch release also fixes this issue.

Details

The mGuard HTTPS client for downloading configuration profiles with the “Central Management” functionality will accept the use of an RSA temporary key in a non-export RSA key exchange ciphersuite. A server could present a weak temporary key and downgrade the security of the session.

Mitigation

All users of the affected Innominate mGuard devices may either update to one of the fixed firmware versions or update the download server to refuse the request for export-grade ciphers.