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

Innominate AG ▪ Rudower Chaussee 13 ▪ 12489 Berlin

Security Advisory 2014/06/06

2014/06/06 - Innominate Security Technologies, Berlin

Synopsis

OpenSSL SSL/TLS MITM vulnerability (CVE-2014-0224)

Issue

Because of a bug in the OpenSSL library used in mGuard products for HTTPS communication, they are vulnerable to a Man-In-The-Middle attack.

Other cryptographic communication (SSH, VPN) are not affected.

This bug is present in the mGuard 8.0.0, 8.0.1, 8.0.2 and 8.1.0 releases. Older releases are only affected when communicating to HTTPS servers that use a vulnerable version of the OpenSSL library. Users that utilize private Configuration Pull Servers or Update Servers should ensure that these HTTPS servers are using a version of OpenSSL not vulnerable to CVE-2014-0224.

Affected products

All Innominate mGuard products running with firmware version 8.0.0, 8.0.1, 8.0.2 or 8.1.0 are affected.

Details

An attacker using a carefully crafted handshake can force the use of weak keying material in OpenSSL SSL/TLS clients and servers. This can be exploited by a Man-In-The-Middle (MITM) attack where the attacker can decrypt and modify traffic from the attacked client and server.

The attack can only be performed between a vulnerable client **and** server.

According to published analyses the commonly used browsers (IE, Firefox, Chrome on Desktop and iOS, Safari etc) aren't affected.

Mitigation

All users of the affected mGuard firmware versions 8.0.0, 8.0.1, 8.0.2 and 8.1.0 should upgrade to mGuard firmware version 8.0.3 or 8.1.1.

Innominate recommends to limit access to the administrative interfaces via firewall rules to the minimum.