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 2014/10/22

2014/10/22 - Innominate Security Technologies, Berlin, Germany

Synopsis

SSL protocol 3.0 security issue (CVE-2014-3566 aka "POODLE")

Issue

The SSL protocol 3.0 has a weakness that allows man-in-the-middle attackers to obtain cleartext data of SSL connections. This affects administrative HTTPS communication with the mGuard device as well as outgoing HTTPS communication initiated by the mGuard for an online-update or configuration pull.

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

This weakness is present in all mGuard versions up to and including version 7.6.4. The mGuard versions 7.6.5, 8.0.0 and later are not affected, because they do not support the SSL protocol 3.0.

Affected products

All Innominate mGuard products running with firmware version 7.6.4 or below are affected.

Details

The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and other products, uses nondeterministic CBC padding, which makes it easier for man-in-the-middle attackers to obtain cleartext data via a padding-oracle attack, aka the "POODLE" issue.

The attack can only be performed if the client and the server support the SSL protocol 3.0.

Mitigation

All users of the affected mGuard firmware versions 7.6.4 and below are advised to update to version 7.6.5.

Alternatively all browsers used to administratively access the mGuard and all web servers configured in the mGuard for online update or configuration pull may be configured to refuse SSL version 3.0.

The default Innominate update servers already refuse the SSL protocol 3.0.

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