Innominate
Security Technologies

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 2014/04/11

2014/04/11 - Innominate Security Technologies, Berlin

Synopsis

OpenSSL CVE-2014-0160 "Heartbleed" data leakage issue

Issue

Because of a bug in the OpenSSL library used in mGuard products for HTTPS communication, private information may be leaked to a remote attacker. Other cryptographic communication (SSH, VPN) are not affected. This bug is only present in the mGuard 8.0.0 and 8.0.1 releases. Older releases are not affected as an older version of the OpenSSL library without the vulnerable functionality is used.

Affected products

8.0.0 and 8.0.1 software versions only!

Details

mGuard firmware version 8.0 uses the OpenSSL cryptographic library and TLS layer implementation version 1.0.1. The version used in mGuard 8.0.0 and 8.0.1 is vulnerable to a possible information leak described in CVE-2014-0160:

General impact related to the OpenSSL library:

- Due to an incorrect length check it is possible to obtain read-only access to memory regions of the HTTPS communication process. The contents of this memory is not predictable and may contain secret information as the private key used in HTTPS communication and clear text parts of the communicated data. The exploit of this vulnerability requires an established TLS (HTTPS) communication connection.

Specific impact on mGuard devices:

- Due to the memory layout of the HTTPS comunication process not being predictable it is possible that the private key of the mGuard Web GUI is disclosed. An attacker might have used this key to

impersonate himself as the mGuard attacked and might have performed a man-in-the-middle attack.

- mGuard uses separate single processes for the TLS encryption layer so that it is not possible for an attacker to access memory regions of other communications or processes. Contents transferred via HTTPS are hence not affected by the information disclosure beyond the possibility of a man-in-the-middle-attack.

Mitigation

All users of the affected mGuard firmware versions 8.0.0 and 8.0.1 should upgrade to mGuard firmware version 8.0.2. Innominate recommends to update the keys on the affected products. The mGuard firmware 8.0 provides a combined function to replace both the HTTPS and SSH keys.

This can be done by one of the following measures:

1. Use the Rescue Procedure to install the Software version 8.0.2.
2. Use the update mechanism to update the devices to version 8.0.2. After the update the existing keys must be replaced by using the "Generate new 2048 bit keys" button in the menu "Web Settings -> Access" or "System Settings -> Shell Access"

In the case a man-in-the-middle attack might have taken place users should review their configuration for sensible information like passwords and private key material and replace them. Innominate recommends to limit access to the administrative interfaces via firewall rules to the minimum.