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 2014/06/26

2014/06/26 - Innominate Security Technologies, Berlin

Synopsis

Unauthorized download of system information from Innominate mGuard devices.

Issue

An attacker using a carefully crafted URL may download a configuration snaphot without prior authorization. (CVE-2014-2356, ICS-VU-311092)

Affected products

All Innominate mGuard devices running with firmware version 4.0.0 up to firmware version 8.0.2 are affected. The firmware versions 8.0.3, 8.1.0, 8.1.1 and higher are not affected. The mGuard firmware 7.6.4 patch release also fixes this issue.

Details

Innominate mGuard devices provide a functionality to download a configuration snapshot to support customers configuring their system.
This information can be accessed unauthorized via the HTTPS CGI interface. It contains configuration data, current system information and logfiles, but no confidential data like RSA private keys, Pre-Shared keys nor any passwords. From the data an attacker might gather information about network topology, traffic flows, and other connected systems.
This issue was found by the Applied Risk Research team http://www.applied-risk.com and is referenced there as ARA-2014001.

Mitigation

All users of the affected Innominate mGuard devices may either update to one of the fixed firmware versions mentioned above or use the “hotfix-CVE-2014-2356” patch-update to fix their systems without updating any other component.
The patch can be applied by either uploading the patch-update as “Local Update” or by the “Online Update” functionality and using “hotfix-CVE-2014-2356” as “*Package set name”.*
Additionally, Innominate recommends to limit access to the administrative interfaces via firewall rules to the minimum.