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

Innominate AG ▪ Rudower Chaussee 13 ▪ 12489 Berlin ▪ Germany

Security Advisory 2012-06-14-001

2012/06/14 - Innominate Security Technologies, Berlin

Synopsis
Probably weak HTTPS and SSH keys on mGuard products.

Reference
ICS-VU-873212

Issue
Because of an insufficient use of entropy, the generated keys for HTTPS and SSH access on mGuard products may be too weak. An attacker could be able to calculate the private keys and perform a Man-In-The-Middle attack to exploit the vulnerability.

Impact
Several prerequisites are required to stage an attack exploiting this vulnerability:

- successful guessing or computation of the private key of the mGuard device to be attacked, and
- physical access to the network path between the mGuard device to be attacked and a legitimate administrator of that device or deviation of legitimate traffic to the mGuard device to the attacker's computer by techniques such as arp spoofing.

With a subsequent man-in-the-middle attack, the attacker could get hold of the mGuard's administrative passwords to then login into and manipulate the attacked mGuard device.

Keys that are loaded as part of the mGuard configuration (VPN et al) are not affected, because they were generated externally. The correct generation of these keys is not subject of this advisory.

Affected products (All software versions)
All products introduced into the market before 2008:
mGuard smart (discontinued)
HW-101020 HW-101050 BD-101010 BD-101020
mGuard industrial RS (discontinued)
HW-105000 BD-501000 BD-501010 BD-501020

mGuard delta (discontinued)
HW-103050 BD-201000
mGuard PCI
HW-102020 HW-102050 BD-111010 BD-111020
mGuard blade
HW-104020 HW-104050
EAGLE mGuard
HW-201000 BD-301010
All variants of these products manufactured before 2006
order numbers 5xxxx

Non-affected products

All products introduced into the market since 2009:
mGuard smart²
HW-101130 BD-101030
mGuard rs2000/rs4000
HW-108010 HW-107010 BD-701000
mGuard delta²
HW-103060 BD-211010
mGuard centerport
HW-106000 BD-601000 BD-602000 HW-106100 BD-611000 BD-612000

Solution

Software Version 7.5.0 or later properly uses existing entropy before generating HTTPS and SSH keys.
It additionally increases the size of the RSA keys from 1024 to 2048 bit.

Innominate recommends updating the keys on the affected products. This can be done by any of the following measures:

1) Use the Rescue Procedure to install the Software version 7.5.0 or later. New keys will be generated as part of this process.

2) Use the update mechanism to update the devices to version 7.5.0 or later.
   2.1) Install the update, existing keys will be kept.
   2.2) After the update the existing keys must be replaced using one of the following methods:
   (The process will take up to a minute to complete, no reboot necessary)
      a) Web UI
         - Login as root or admin
         - Click the "Generate new 2048 bit keys" button either in the "Web Settings -> Access" or in the "System Settings -> Shell Access" menu
         - Note the fingerprint output of the newly generated keys.
         - Login via HTTPS and compare the certificate information provided by the browser.
      b) Console
         - Login via serial console or SSH as user root or admin
         - Execute the program

```
$ rsa_renewal update
```

         - Note the fingerprint output of the newly generated keys.
         - Login via SSH and compare the fingerprints shown by SSH

3) Upload and execute a shell script via SSH as root, provided by Innominate. The script will generate new 2048 bit keys without requiring an update to software version 7.5.0 or later. All software versions starting with 4.2.0 are supported. The script can be downloaded at
`http://www.innominate.com/en/downloads/software-and-misc`

- Use scp to copy the script onto the mGuard like
  `$ scp generate_2048key.sh root@192.168.1.1:/root/`
- Login via SSH as root
- Execute the script as shown below
  `$ sh /root/generate_2048key.sh`
- Note the fingerprint output of the newly generated keys.
- Login via SSH and compare the fingerprints shown by SSH

Innominate recommends changing the administrative passwords of affected mGuard devices.

Credits

This issue was reported to us by Nadia Heninger (UCSD), Zakir Durumeric (UMICH), Eric Wustrow (UMICH), J. Alex Halderman (UMICH) as a result of their research work. More details can be found at
`https://freedom-to-tinker.com/blog/nadiah/new-research-theres-no-need-panic-over-factorable-keys-just-mind-your-ps-and-qs`