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

Innominate AG ▪ Rudower Chaussee 13 ▪ 12489 Berlin

Security Advisory 2014/12/17-001

2014/12/17 - Innominate Security Technologies AG, Berlin, Germany

Synopsis

Privilege escalation of the admin user.

Issue

An attacker authorized as user “admin” may use special configuration settings to execute arbitrary commands as root user with UID 0.

Reference

CVE-2014-9193

Affected products

All Innominate mGuard devices running with any firmware version up to firmware version 8.1.3 are affected. The firmware versions 8.1.4 and higher are not affected. The mGuard firmware 7.6.6 patch release also fixes this issue.

Details

By using specially crafted PPP settings an administrator may execute arbitrary commands with root privileges.
In most use cases the "admin" and the "root" role are represented by the same individuals reducing the impact.

Mitigation

All users of the affected Innominate mGuard devices may update to one of the fixed firmware versions mentioned above.
Additionally, Innominate recommends to limit access to the administrative interfaces via firewall rules to the minimum.