Security Advisory 2015-01-20-001

2015/01/20 – Phoenix Contact, Blomberg

Synopsis

The NTP service on the mGuard is vulnerable to remote attacks if enabled.

Reference

CVE-2014-9295

Issue

Possible unprivileged remote code execution by exploiting the NTP vulnerabilities tracked as CVE-2014-9295.

Details

An attacker may use specially crafted NTP packets to remotely exploit the NTP vulnerability tracked as CVE-2014-9295 and execute arbitrary code as unprivileged user or to interrupt the NTP service. The mGuard is only vulnerable to this attack if the NTP service on the mGuard is enabled, which is not the default setting.
Due to the nature of the NTP protocol exploiting the vulnerability from remote is possible if an attacker can inject malicious packets into communication opened from the mGuard to a remote NTP server.

Affected products

All mGuard devices running with any firmware version up to firmware version 8.1.4 are affected. The firmware versions 8.1.5 and higher are not affected. The mGuard firmware 7.6.7 patch release also fixes this issue.

Mitigation

All users of the affected mGuard devices may update to one of the fixed firmware versions mentioned above or disable the NTP service on the mGuard.