PHOENIX CONTACT GmbH & Co. KG
Flachsmarktstraße 8
32825 Blomberg, Germany
Telefon: +49 5235 300
Telefax: +49 5235 3-41200
Internet: http://www.phoenixcontact.com
USt-Id-Nr.: DE124613250
WEEE-Reg.-Nr.: DE50738265

PHOENIX CONTACT GmbH & Co. KG · 32825 Blomberg

17 July 2017
S1: 300379953/pbsa56

Security Advisory for mGuard products [CVE-2013-6466]

Synopsis

CVE-2013-6466: Remote denial of service vulnerability of the IKE daemon.

Affected products

All Phoenix Contact and Innominate Security Technologies devices running the mGuard firmware version 8.0.0 to 8.5.1.

Issue

Cited from the original report CVE-2013-6466: “Openswan 2.6.39 and earlier allows remote attackers to cause a denial of service (NULL pointer dereference and IKE daemon restart) via IKEv2 packets that lack expected payloads.”

Details

Specially crafted IKEv2 packets may force an IKE daemon restart and force a restart of all IPsec connections. There is no access to sensitive information or tunnel content possible by this attack.

Mitigation

Customers using Phoenix Contact or Innominate mGuard devices with affected firmware versions are recommended to update to firmware version 8.5.2 or higher which fixes this vulnerability.