

# Phoenix Contact mGuard line protects industrial networks

MIDDLETOWN, Pa. – Following the latest report of vulnerabilities in a control platform, the U.S. Department of Homeland Security recently issued an alert recommending several strategies to mitigate damage and protect control systems from attacks. Phoenix Contact's FL mGuard line of security appliances can help make these strategies a reality.

In December 2011, independent researcher Ruben Santamarta publicly released vulnerabilities he discovered within several Schneider Electric PLCs. The U.S. Department of Homeland Security's Industrial Control Systems Cyber Emergency Response Team (US ICS-CERT) quickly issued an alert confirming the findings and providing mitigation strategies.

The agency recommended users to:

- Minimize network exposure for all control system devices. Control system devices should not face the Internet.
- Locate control system networks and devices behind firewalls, and isolate them from the business network (also known as a defense-in-depth solution).
- If remote access is required, use secure methods, such as Virtual Private Networks (VPNs).

"This is just the latest news report about threats to control systems, but, unfortunately, it won't be the last," said Dan Schaffer, industrial network security specialist for Phoenix Contact. "Whatever control platform they are using, control engineers should follow the recommendations of the US ICS-CERT group to prevent malicious or accidental network damage. The mGuard products meet the needs of both the automation and IT worlds, making it easy to implement this type of defense-in-depth solution."

The mGuard provides firewall protection to block both attacks and unwanted network traffic that can negatively impact sensitive control networks. Additionally, the mGuard's advanced logging capabilities can alert the network manager if somebody has tried access to the network. These logs can be stored locally, or the mGuard can send them to a central location to make auditing and compliance reporting easier. If the application requires Internet access (such as for remote support or diagnostics), the mGuard can create a secure VPN tunnel for safe and secure communication.

ICS-CERT is coordinating mitigations with Mr. Santamarta and Schneider Electric. Schneider Electric has produced a fix for two of the reported vulnerabilities and is continuing to develop additional mitigations.

For more information about the mGuard or about Phoenix Contact, visit

## Phoenix Contact mGuard line protects industrial networks

Published on Electronic Component News (<http://www.ecnmag.com>)

---

<http://www.phoenixcontact.com/mguard> [1], or call technical service at 800-322-3225, e-mail [info@phoenixcon.com](mailto:info@phoenixcon.com) [2].

### Source URL (retrieved on *12/04/2013 - 12:15pm*):

<http://www.ecnmag.com/products/2012/01/phoenix-contact-mguard-line-protects-industrial-networks>

### Links:

[1] <http://www.phoenixcontact.com/mguard>

[2] <mailto:info@phoenixcon.com>