******PSIRT website helps achieve a high level of security**

# Within the scope of Industry 4.0 and the Industrial Internet of Things (IIoT), network-based data transmission is becoming increasingly common.

# However, with the advantage of borderless communication there is also a greater risk of unauthorised access if appropriate precautions are not taken. Despite extensive experience and the utmost care being taken with all products, errors may occur during programming and these can result in security vulnerabilities. With this in mind, Phoenix Contact is one of the first companies to have established an international Product Security Incident Response Team (PSIRT).

# On the website <http://www.phoenixcontact.com/psirt> customers, scientists, authorities, and all those involved in the field of access security can report potential security vulnerabilities. Acknowledgment of receipt will be provided within two working days. Following extensive testing and the provision of patches, details of the security vulnerability will be published on the PSIRT website. This is common practice so as not to alert potential hackers to the security vulnerability before users have been able to protect their application with a bug-fixed software version. For example, security specialists from Positive Technologies, a security solutions provider, identified a security vulnerability in switches from the FL SWITCH product family and reported this via the PSIRT website. The vulnerability was removed by means of a firmware update and the relevant information was then published online. With regard to the publication of security vulnerabilities, the PSIRT team also works closely with CERT@VDE, a platform for the coordination of IT security problems specifically intended for small and medium-sized companies working in the field of industrial automation.

# The PSIRT website lists all security vulnerabilities that have been identified thus far for Phoenix Contact products and the website is continuously updated. If users want to make sure they are always kept up to date, they can also subscribe to the PSIRT newsletter. The reporting and rapid removal of security vulnerabilities and associated information also help ensure that Phoenix Contact products and the applications in which they are used always satisfy current security requirements.

**ENDS**

**July 2018**

**PR5059GB**

Phoenix Contact Ltd

Halesfield 13

Telford

Shropshire

TF7 4PG

Tel: 0845 881 2222

Fax: 0845 881 2211

[www.phoenixcontact.co.uk](http://www.phoenixcontact.co.uk)

[info@phoenixcontact.co.uk](mailto:info@phoenixcontact.co.uk)

**For news updates from Phoenix Contact visit:**

**Phoenix Contact Press Room** – http://www.mynewsdesk.com/uk/phoenix-contact-uk

**Twitter** - @phoenixcontactu

**YouTube** – Phoenix Contact UK

**Blog** – www.phoenixcontact.co.uk/blog

**LinkedIn** – www.linkedin.com/company/phoenix-contact-uk