Cyber Security Incident Response Team (CSIRT) Policy of PROFIBUS Nutzerorganisation e. V.

Version 1.0 – Date August 2020

Order No.: 8.722

File name : PNO_CSIRT_Policy_8722_V10_Aug20.docx

Comments to be submitted to the Editor of the Document Karl-Heinz@Niemann-on-line.de
.

Prepared by PI Working Group PG10 “Security” in Committee B “PROFINET”.

The attention of adopters is directed to the possibility that compliance with or adoption of PI (PROFIBUS&PROFINET International) specifications may require use of an invention covered by patent rights. PI shall not be responsible for identifying patents for which a license may be required by any PI specification, or for conducting legal inquiries into the legal validity or scope of those patents that are brought to its attention. PI specifications are prospective and advisory only. Prospective users are responsible for protecting themselves against liability for infringement of patents.

NOTICE:

The information contained in this document is subject to change without notice. The material in this document details a PI specification in accordance with the license and notices set forth on this page. This document does not represent a commitment to implement any portion of this specification in any company's products.

WHILE THE INFORMATION IN THIS PUBLICATION IS BELIEVED TO BE ACCURATE, PI MAKES NO WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, WITH REGARD TO THIS MATERIAL INCLUDING, BUT NOT LIMITED TO ANY WARRANTY OF TITLE OR OWNERSHIP, IMPLIED WARRANTY OF MERCHANTABILITY OR WARRANTY OF FITNESS FOR PARTICULAR PURPOSE OR USE.

In no event shall PI be liable for errors contained herein or for indirect, incidental, special, consequential, reliance or cover damages, including loss of profits, revenue, data or use, incurred by any user or any third party. Compliance with this specification does not absolve manufacturers of PROFIBUS or PROFINET equipment, from the requirements of safety and regulatory agencies (TÜV, BIA, UL, CSA, etc.).

PROFIBUS® and PROFINET® logos are registered trade marks. The use is restricted to members of PROFIBUS&PROFINET International. More detailed terms for the use can be found on the web page www.profibus.com/Downloads. Please select button "Presentations & logos".

In this specification the following key words (in **bold** text) will be used:

may: indicates flexibility of choice with no implied preference.

should: indicates flexibility of choice with a strongly preferred implementation.

shall: indicates a mandatory requirement. Designers **shall** implement such mandatory requirements to ensure interoperability and to claim conformance with this specification.

Publisher:
PROFIBUS Nutzerorganisation e.V.
Haid-und-Neu-Str. 7
76131 Karlsruhe
Germany
Phone : +49 721 / 96 58 590
Fax: +49 721 / 96 58 589
E-mail: info@profibus.com
Web site: www.profibus.com

Content

Revision Log

Version	Ersteller	Datum	Kommentar
0.4	Niemann	05. June 2020	Version for publishing
0.5	Niemann	23.07.2020	Chapter 4 (Advisories) removed, minor changes
1.0	Niemann	20 August 2020	First published version

1 Introduction

The increasing networking of production facilities increases the risk of cyber-attacks. The communication technologies specified and supported by PROFIBUS and PROFINET International (PI) are also exposed to this risk. To address this risk, PROFIBUS and PROFINET International operates a Cyber Security Incident and Response Team (CSIRT).

- The PNO-CSIRT provides information and support to PI member companies and users of PI's technologies. This includes assistance in implementing proactive measures to reduce the risk of computer security breaches and to respond to such breaches or incidents as soon as they occur. The PNO-CSIRT is also intended to serve as a contact for the regional PROFIBUS and PROFINET organizations (RPAs).
- The PNO-CSIRT sees itself as an intermediary between technology suppliers, component manufacturers, system manufacturers and users of the technologies of PROFIBUS and PROFINET International (PI).
- The PNO-CSIRT serves as a contact for other CSIRTs / CERTs as well as other national and international institutions (e.g. BSI, ENISA) in questions concerning the technologies of the PROFIBUS User Organization (PI) and maintains corresponding contacts with these institutions.

The special role of the PNO as a manufacturer association means that the PNO-CSIRT sees its focus on the handling of weaknesses in the specifications of the technologies of the PROFIBUS User Organization (PI) and that the handling of product-dependent weaknesses is the responsibility of the respective technology, component or system suppliers. In this case, the PNO-CIRT will provide the necessary support to forward incoming vulnerability reports to the appropriate addressees and to provide appropriate feedback to the reporting person / company.

2 Policy

The following rules apply to the work of the CSIRT:

- PI is committed to a relationship of trust with manufacturers and users. For this reason, vulnerability reports are only made available to the responsible group of people during processing and are securely stored.
- PI has a responsible disclosure policy. Prior to the publication of a vulnerability that may affect their products, manufacturers are given the opportunity to work out a solution to resolve the vulnerability or mitigation in a reasonable time.
- PI publishes advisories of known vulnerabilities and the associated fixes or mitigations after a reasonable period of time.
- Technical experts from member companies, who support PI in the analysis of weaknesses, are bound to confidentiality - also within their own company.
- PI will forward vulnerability reports concerning a company's products, together with information about the person making the report, to that company for problem resolution. Passing on the contact information of the person making the report is intended to speed up problem resolution. If anonymous forwarding is desired, this can be specified in the reporting form.

3 Reporting of vulnerabilities

When reporting vulnerabilities that affect products, please contact the manufacturer of the respective product.

You can report weaknesses that are likely to be caused by PI communication protocols here. If the cause is unclear or unknown, you can also report it here. PI will then evaluate the message and, if necessary, forward it to the affected manufacturer for problem resolution.

The notification of vulnerabilities in PI's protocols can be done as follows:

- PI receives reports of vulnerabilities via an online form on www.profinet.com/security or via the e-mail address security@profinet.com.
- Encrypted communication can be used if desired. The public PGP key of the CSIRT can be found at www.profibus.com/security
- Please use preferably the following fillable form on this web page.
- The receipt of the message is acknowledged by PI. The reporting person is informed about the status of the processing.
- In case you select completely anonymous reporting please note, that you will not receive any confirmation nor information about the case reported.
- If you decide to make a partially anonymous report, your contact details will be recorded and processed in the office. However, the technical specialists involved in processing will not receive any information about your identity.

Please note that when reporting vulnerabilities, you must observe legal provisions or other obligations, especially confidentiality obligations or export control regulations.

PI will in many cases contact the manufacturer of the component or the manufacturer of any technology components (e.g. protocol stacks) used to clarify the vulnerability report.

4 Disclaimer

PI will handle submitted vulnerability reports free of charge with reasonable care.

PI does not assume any liability whatsoever, neither expressly nor implicitly, for the correctness, absence of errors, absence of industrial property rights and copyrights accruing to third parties, completeness or usability of any information in connection with vulnerability reports and their handling and resolution, except in in case of willful intent and fraudulent intent.

Furthermore, PI shall not be liable for damage of a tangible or intangible nature caused directly or indirectly through vulnerability reports, their handling and resolution, unless PI is verifiably culpable of intent or gross negligence. PI will be liable for damages arising because of injury to life, limb or health in accordance with statutory law.

PROFIBUS Nutzerorganisation e. V. (PNO)
PROFIBUS & PROFINET International (PI)
Haid-und-Neu-Str. 7 ● 76131 Karlsruhe ● Germany
Phone +49 721 96 58 590 ● Fax +49 721 96 58 589
E-mail info@profibus.com
www.profibus.com ● www.profinet.com