Coordinated Vulnerability Disclosure Policy

Perinet GmbH welcomes reports of security vulnerabilities in our products. This policy describes how to report a vulnerability to us and what you can expect when you do.

1 Scope

This policy covers all Perinet products with digital elements and their related firmware and software: periCORE, periNODE (periNODE GPIO, periNODE 0-10V, periNODE 4-20mA, periNODE Modbus), periMICA, periSWITCH, periSTART, periSNOOP and periTUNNEL. It also covers vulnerabilities in third-party components integrated into these products.

2 How to report

> **Preferred channel — Email: security@perinet.io**
>
> Post: Perinet GmbH, „Security“, Rudower Chaussee 29, 12489 Berlin, Germany

Email is our preferred channel, but you remain free to choose the means of communication for your report and for our exchange. Your report is received and handled by a person, not an automated system.

Alternatively, you may report the vulnerability — anonymously if you wish — through Germany's coordinating CSIRT, the Federal Office for Information Security (BSI / CERT-Bund).

Helpful contents of a report: affected product and firmware version, a description of the vulnerability, steps to reproduce, and your assessment of the impact. Partial information is welcome too — do not hold back a report because it is incomplete.

3 What we do with your report

This applies to reports that fall within section 1, are not excluded by section 6, and describe a plausible security issue in enough technical detail to be assessed. For such a report, and where you have given us a way to reach you, we confirm receipt, analyse it, and come back to you: whether we confirm or reject the vulnerability, any questions we need answered, and — once the analysis is complete — which products and versions are affected and how we intend to address it. Where the analysis takes longer, we keep you informed.

We may decide not to respond to out-of-scope, automated or bulk submissions, or to submissions that contain no assessable technical information.

4 Coordinated disclosure

We ask you to give us a reasonable opportunity to analyse and remediate the vulnerability before any public disclosure. We agree the timing of disclosure with you, taking severity and the complexity of the remediation into account.

Information about confirmed and remediated vulnerabilities is published on the security page on perinet.io, where customers, distributors and system integrators find advisories for our products.

5 Good-faith research

We will not take legal action against security researchers who act in good faith within this policy:

- do not exploit a vulnerability beyond what is needed to demonstrate it,
- do not access, modify or delete third-party data,
- do not degrade the availability of systems in productive use,
- keep vulnerability details confidential until coordinated disclosure.

6 Out of scope

Reports on the perinet.io website itself, spam or phishing that merely names Perinet, and findings without security impact are outside this policy.