Vulnerability disclosure policy

Introduction

This document describes how to act if you believe you have found a security vulnerability in a SKOV product.

Scope

This description of how to report vulnerabilities is only relevant to products mentioned in the list of SKOV products and software versions below. Products or software versions that are no longer being produced or actively being maintained, are no longer supported in terms of security updates.

- BlueControl v8.x.x and newer
- AlarmUnit v4.x.x and newer
- DOL 43x, 53x, 63x, 83x v7.8.x
- DOL532 Tunnel v8.x.x and newer

Reporting a vulnerability to SKOV

Please read this document fully prior to reporting any vulnerabilities to ensure that you understand the policy and can act in compliance with it. Please report your findings in scope (see the section above) to cybersecurityreport@skov.com and provide the following information (in English):

- Information about the product (software version, variant, backup of configuration etc.)
- How vulnerability can be exploited and the impact of the issue. It may be helpful to include screenshots to illustrate the vulnerability.
- Step-by-step instructions to reproduce the issue.

Please do not send us confidential information such as your password or any other person-related data.

What you can expect from us

After you submit your report, we will respond within 4 business days and let you know that we have received it. Afterward, within an additional 10 business days, we will inform you about how we prioritize your reported incident and, if needed, when the security issue is expected to be solved and ready for testing. If we have further questions, we'll get back to you.

After the initial triage, priority for remediation is assessed by looking at the impact, severity, and exploit complexity. Vulnerability reports might take some time to address, and you are welcome to inquire about the status, but you should avoid doing so more than once every 14 days. This allows our teams to focus on the remediation.

We will notify you when the reported vulnerability is remediated, and you may be invited to confirm that the solution adequately covers the vulnerability.