

Guideline on Coordinated Disclosure

Scope

This policy applies to security vulnerabilities in the BENS G5 software and in the infrastructure operated by Suchy MIPS that is related to BENS G5. It does not cover third-party systems, even if BENS G5 is used on them - please report any issues relating to such systems directly to the relevant operator.

How to report a vulnerability

- Send your report to info@suchymips.de.
- Describe the vulnerability as precisely as possible: affected version(s) of BENS G5, steps to reproduce the issue, technical details, potential impact.
- Encrypted transmission of sensitive details is available on request.

What you can expect from us

- Confirmation of receipt within 3 working days.
- Initial assessment of the severity within 10 working days.
- Regular status updates until the issue is resolved, at least every 14 days.
- Your name or pseudonym will be included in our acknowledgements, if desired.

Responsible Disclosure (“Safe Harbour”)

We do not regard security research carried out in good faith and within the scope of this policy as unauthorised access. We will not take legal action against reporters, provided the following rules are observed:

- No access to or alteration of third-party data beyond the minimum necessary to reproduce the issue.
- No denial-of-service attacks, no social engineering directed at staff or customers, and no physical attacks on premises.
- The vulnerability must not be made public before a fix is available or a joint disclosure deadline has been agreed.

Disclosure period

We aim to rectify reported vulnerabilities within 90 days. Should this not be possible for technical reasons, we will agree a revised, joint disclosure period with you. Public disclosure before the expiry of this period or before a fix is available will only take place following mutual agreement.

Outside the scope

- Pure spam, phishing or social engineering attempts with no technical connection to BENS G5.
- Vulnerabilities in outdated configurations, those modified by the customer themselves, or unsupported configurations.
- Missing security headers or deviations from best practice without a concrete, verifiable impact.

Contact

info@suchymips.de — technical enquiries are handled by Sascha Leiter (Technical Director), whilst general or escalated enquiries are handled by Waldemar Suchy (Managing Director).