Vulnerability disclosure

Version 1.3 | Last updated 29 September 2026

This is a translation of the French original, which governs in case of divergence.

The security of our systems improves partly thanks to the people who take the time to report a flaw. This policy says what we expect from a report, what we undertake to do with it, and which Belgian legal frame it sits in.

Scope

Covered are the systems Avanserv SRL operates on its own account: the avanserv.com site, the app.avanserv.com application and its API, and the infrastructure serving them. Not covered are our clients' systems and applications, even where we host them: they belong to their owners, and any research on them needs those owners' authorisation.

The rules

Keep your investigation to what is needed to demonstrate the vulnerability, and stop at the first proof. Do not exfiltrate data beyond that proof, do not modify or delete anything, do not degrade the service: denial-of-service attacks, social engineering, phishing and physical intrusion all fall outside this policy. Disclose nothing publicly before the coordination described below has finished.

How to report

Write to security@avanserv.com describing the vulnerability, the steps that reproduce it, the impact you estimate and, if you wish, a way to credit you. To benefit from the legal protection described below, report it too, following the procedure published by the Centre for Cybersecurity Belgium (CCB): a simplified report within 24 hours of discovery, then a complete report within 72 hours. Writing to us alone does not obtain that protection.

We acknowledge receipt within five working days, keep you posted on progress, and aim at a fix in a period proportionate to the severity. We agree a publication date together, with a default horizon of 90 calendar days after the report, that date

remaining subject to the agreement of the Centre for Cybersecurity Belgium. With your agreement we are glad to credit your contribution; we run no bounty programme.

The Belgian legal frame

Belgian law protects vulnerability research carried out in good faith. Under articles 22 and 23 of the law of 26 April 2024 establishing a framework for the cybersecurity of networks and information systems, a person who discovers a vulnerability may benefit from legal protection if they act without fraudulent intent or intent to harm, if they go no further than is necessary and proportionate to establish that the vulnerability exists, if they send a simplified report within 24 hours of discovery and then a complete report within 72 hours to the Centre for Cybersecurity Belgium (CCB) as well as to the organisation concerned, and if they disclose nothing publicly without the CCB's agreement. How to report to the CCB is published on ccb.belgium.be. This policy amounts, for our own systems, to joining that frame: we will file no complaint and bring no civil claim against research that respects those conditions and the rules above.

The security.txt file

A file meeting RFC 9116 is published at https://avanserv.com/.well-known/security.txt. It names the address given above, this page as the policy itself, French and English as the languages we read, and an expiry date the site renews on each build of the site. The policy it points at covers both systems, the site and the application, as the scope section sets out.

It is not quoted here. A contact address written down twice is one an amendment can leave in two states, and the file is the one a machine reads.