CYBER & SECURITY SOLUTIONS

SC2

SECURITY MANAGEMENT PLATFORM VULNERABILITIES REPORT

LEONARDO

Leonardo products are designed and developed according to Cyber Resilience methodologies, and the cyber secure-by-design approach which makes the reliability of the systems intrinsic right from the design and development phase. At Leonardo we are committed to protecting our users' security and the integrity of our products. We value security researchers' contributions in identifying and reporting vulnerabilities, guidelines on reporting vulnerabilities as well as interactions with Product Security Incident Response Team (PSIRT) are outlined in the Policy reported at the end of this document.

Vulnerability and Exposures management is all about reducing risks in IT systems. The following tables summarize all identified vulnerabilities for SC2 platform

INSUFFICIENT VERIFICATION OF DATA AUTHENTICITY [MEDIUM]		
TEST	**CVSS3.1 Metrics**	**Value**
Insertion of files through file upload functionality, in order to prevent introduction of potentially malicious or non-compliant elements.	Attack Vector	Network
	Attack Complexity	Low
	Privileges Required	High
RESULTS	User Interaction	None
Application does not check the bytes of the file, but only the extension. This exposes to the risk of intrusion of potentially malicious files which could generate unexpected exceptions	Scope	Unchanged
	Confidentiality	None
	Integrity	Low
	Availability	Low

INFORMATION EXPOSURE [LOW]		
TEST	**CVSS3.1 Metrics**	**Value**
Possibility to acquire useful information about the application: technologies, services or software versions in use.	Attack Vector	Network
	Attack Complexity	Low
	Privileges Required	High
RESULTS	User Interaction	None
Vulnerability can increase the attack surface of the system and could allow an attacker to design and build complex attacks based on the acquired data	Scope	Unchanged
	Confidentiality	None
	Integrity	Low
	Availability	Low

Vulnerability Disclosure Policy

Leonardo fosters an open, collaborative, and transparent disclosure process to enhance the security of his products. We encourage you to contact us to report potential vulnerabilities in our products. This policy applies exclusively to vulnerabilities found in Leonardo SC2 product.
If you make a good faith effort to comply with this policy during your security research, we will consider your research to be authorized. We will work with you to understand and resolve the issue quickly, and Leonardo will not recommend or pursue legal action related to your research.

Responsible Disclosure Guidelines

Under this policy, "research" means activities in which you:

- Notify us as soon as possible after you discover a real or potential security issue;
- Make every effort to avoid privacy violations, degradation of user experience, disruption to production systems, and destruction or manipulation of data;
- Only use exploits to the extent necessary to confirm a vulnerability's presence. Do not use an exploit to compromise or exfiltrate data, establish persi stent access, or use the exploit to pivot to other systems.;
- Do not publicly disclose the vulnerability, any related details, or proof-of-concept code until Leonardo has had investigated, remediated and publicly disclosed the issue. This allows us to protect our users and avoid widespread exploitation;
- Do not submit a high volume of low-quality reports.

Once you've established that a vulnerability exists or encounter any sensitive data (including personally identifiable information, financial information, or proprie- tary information or trade secrets of any party), you must stop your test, notify us immediately, and not disclose this data to anyone else.

Out of Scope Activities and Vulnerabilities:

The following test methods are not authorized:

- Denial of Service (DoS/DDoS) attacks or any actions intended to disrupt, degrade, or overwhelm our services or infrastructure.
- Social Engineering (e.g., phishing, vishing, smishing) against Leonardo employees, contractors, or users.
- Physical attacks on Leonardo facilities, data centers, or personnel.
- Accessing, modifying, or destroying user data or Leonardo's proprietary information beyond what is strictly necessary to demonstrate the existence of a vulnerability.
- Automated scanning tools that generate a high volume of traffic or reports without manual verification and analysis.
- Exploiting vulnerabilities for personal gain, data exfiltration, establishing persistent access, or pivoting to other systems.
- Testing third-party applications or websites that integrate with Leonardo's products but are not directly owned or controlled by Leonardo. Please report these directly to the respective third party's disclosure program.
- Spamming, mass submission, or submitting low-quality/duplicate reports.
- Reporting theoretical vulnerabilities without a clear, reproducible proof of concept or issues that are not practically exploitable (e.g. Self-XSS or sel f-DoS, Broken link hijacking, tabnabbing, CSRF, Clickjacking on pages with no sensitive actions, software version disclosure, etc.)
- Issues related to TLS/SSL configurations or missing best practices (e.g., weak cipher suites, old TLS versions, missing security headers, etc.) unless accompanied by a demonstrated, exploitable vulnerability.

Any other Leonardo products, corporate IT infrastructure, or non-integrated third-party software are excluded from this policy's scope and are not authorized for testing. Additionally, vulnerabilities found in systems from our vendors fall outside of this policy's scope and should be reported directly to the vendor according to their disclosure policy (if any). If you aren't sure whether a system is in scope or not, contact us at psirt@leonardo.com before starting your research.

Reporting a vulnerability

Report any security vulnerability to us immediately. We accept vulnerability reports via email to: psirt@leonardo.com

What we would like to see from you

- For a swift response, include:
- Vulnerability Title: Concise summary.
- Detailed Description: Clear explanation of its nature and impact.
- Affected Components/Versions: Specific versions, modules, or environments.
- Steps to Reproduce: Precise, step-by-step instructions (with prerequisites/configurations) for validation.
- Proof of Concept (PoC): Relevant code, scripts, URLs, screenshots, or videos demonstrating the benign, non-destructive vulnerability.
- Impact Assessment: Your perspective on the security impact (e.g., data access, privilege escalation).
- Your Contact Information: Name/alias and email, with credit preference (there is no monetary reward for the present disclosure program).

What you can expect from us

- When you choose to share your contact information with us, we commit to coordinating with you as openly and as quickly as possible.
- We will acknowledge that your report has been received.
- To the best of our ability, we will confirm the existence of the vulnerability to you and be as transparent as possible about what steps we are taking during the remediation process, including on issues or challenges that may delay resolution.
- We will maintain an open dialogue to discuss regarding the reported issue.
- We will publicly disclose the vulnerability once the issue has been investigated and remediated. To demonstrate maximum transparency, each vulnerabi lity report includes a precise Common Vulnerabilities and Exposures (CVE) code, where applicable, including the Common Weakness Enumeration (CWE).

Questions

Questions regarding this policy may be sent to psirt@leonardo.com. We also invite you to contact us with suggestions for **improving** this policy.

For more information:
cyberandsecurity@leonardo.com

Leonardo Cyber & Security Solutions Division
Via R. Pieragostini, 80 - Genova 16151 - Italy

LDO_IT25_01520 08-25
August 2025 © Leonardo S.p.A.

leonardo.com