AdaCore Product Security Policy

Abstract: Publicly available description of AdaCore Product Security Incident Response policy

Scope: 🟢 External

Rationale

As outlined in the AdaCore Security Policy, AdaCore maintains two Incident Response teams. This document details the mission and commitments of the Product Security Incident Response Team (PSIRT).

We serve a global clientele across both civilian and defense-related industries by developing and supporting tools and services that facilitate the creation of high-integrity software. We also actively engage in collaborative research and development initiatives.

To meet the needs of customers with stringent security requirements who handle diverse forms of regulated and proprietary data, AdaCore provides products that are an integral part of their supply chain. A sample of these offerings include a comprehensive compilation toolchain, an Integrated Development Environment (IDE), static and dynamic analysis tools, and code generation tools

Ensuring our products do not introduce vulnerabilities or data leaks is a top priority for both AdaCore and our customers.

Commitments

Availability

The Product Security team can be contacted via email at product-security@adacore.com or through our internal Security Portal. In case of an emergency, or if standard communication services are unavailable, the contact information for the Head of Product Security is available in AdaCore's emergency contact list.

Incident handling

When a new Product Security incident occurs, the Product Security Incident Response Team (PSIRT) follows an established internal procedure to ensure the incident is managed according to its severity.

All incidents are tracked in our internal issue tracker, which is regularly updated with progress towards resolution. An incident coordinator is assigned to each case to oversee and coordinate the various teams involved.

Once the severity of an incident is determined, the details are shared with MITRE as appropriate. Information is made publicly available after a 90-day embargo period.

Triage

Incident triage involves technical analysis and severity assessment, which dictates the resolution approach and timeframe. High severity incidents require fixing, with security incident response targets outlined in the AdaCore Coordinated Disclosure Policy.

Severity levels and actions:

- **High**: Vulnerability **must** be fixed, and customers are notified before disclosure.
- **Medium**: Vulnerability **may** be fixed and must be documented with a workaround, if feasible.
- **Low**: Vulnerability is not considered a threat but **may** be fixed, or a workaround may be published.

Vulnerability assessment

Any vulnerabilities that may impact our products are assessed and documented. These details are made available to our customers along with product releases on our customer portal, GnatTracker.

Version updates or patches addressing high-severity vulnerabilities are integrated as soon as possible. This ensures our products will not be affected by these vulnerabilities in the next release.

Continuous monitoring for any new vulnerabilities potentially impacting AdaCore products is performed, starting from version 24.2. This release and all subsequent versions are actively monitored.

Document control information

If relevant fill those informations

Title	AdaCore Product Security Policy	
ID	ISMS.POL.EXT.APSP	
TN		
Version	1.0	
Scope	External	
Distribution	IT	
AdaCore Restricted Links		
Author	Frederic Leger	May 14, 2025 FL
Verifier	Michael Cleaves	May 15, 2025 MC
Approver	Olivier Ramonat	Jun 17, 2025 OR