Gnatcoll project loader attribute sanitization default

ADACORE SECURITY ADVISORY

Document Id: SEC.GNATCOLL-CORE-0162

Version 2 - Jul 01, 2026

AdaCore

Title	Gnatcoll project loader attribute sanitization default	
Status	Final	
Author	Thomas Serabian	
Reviewed by	Frédéric Léger	

Revision History

Version	Date	Comments
1	Jun 05, 2026	Initial version
2	Jul 01, 2026	Fixed a typo in the title

Contents

1. Preface

1.1. Scope

This document is an advisory describing the security impact of GNATCOLL-CORE-0162. The issue is tracked under the ticket number GNATCOLL-CORE-0162 in AdaCore's issue tracking database.

This document also presents possible workarounds and mitigation for the issue.

1.2. Distribution

This advisory is made available in confidence to AdaCore customers under embargo until 2026-08-14 so that they can address the issue it describes before public availability.

1.3. Contact

For questions on this document, please contact AdaCore support at product-security@adacore.com or using the standard reporting procedures if you are an AdaCore customer.

2. Vulnerability

2.1. Affected Products

The vulnerability described in this document was reported for the following product versions:

- *GNATcoll-Core* - `gnatcoll-core-src` *26.1* (20260107)

The vulnerability described in this document applies to the following product versions:

- `gnatcoll-core-src` < 26.2

2.2. Severity and Impact

CVSS v3.1 score: 8.8 (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:T/RC:C)

This vulnerability allows an *Arbitrary Code Execution* attack on an *GNATcoll-Core* if a compromised file is loaded via `GNATCOLL.Projects.Load`

A CVE (*Common Vulnerabilities and Exposures*) has been created for that case, and will be referred as `CAN-2026-2030263` (until MITRE delivers a real CVE ID).

2.3. Detailed Description

Thanks to the investigation work done by Jon Hood, a vulnerability on *GNATcoll-Core* has been discovered.

GNATCOLL.Projects in AdaCore GNATCOLL allows Code Execution when a GNAT project file (.gpr) is loaded via GNATCOLL.Projects.Load. The library reads the IDE Gnatlist attribute and passes its value directly to Non_Blocking_Spawn without sanitization or validation checks. This allows a remote attacker to execute arbitrary code via a crafted .gpr file if a user opens it in an environment that loads the project, such as GNAT Studio or the Ada Language Server.

3. Solution

3.1. Workarounds

No work around is available

3.2. Correction

The vulnerability described in this document is corrected in the following product versions:

- *GNATcoll-Core* - `gnatcoll-core-src` >= 26.2

Starting from build date `20260601`, the *GNATcoll-Core* component is fixed on `wavefront`.

4. Appendix

4.1. CVSS Score Justification

Metric	Justification
AV:N	The vulnerable component is bound to the network stack and the set of possible attackers extends beyond the other options listed in *Attack Vector: Adjacent*, up to and including the entire Internet.
AC:L	The attacker only needs to send a crafted .gpr file to the target machine that has an environment to load the project.
PR:N	There is no privilege needed.
UI:R	The attacker must convince an user to open a compromised file which looks like a normal project file.
S:U	Both the vulnerable component and the impacted component are managed by the same security authority.
C:H	A successful attack would give attackers access to all of the user data on the compromised machine.
I:H	A successful attack would allow the attacker to tamper with all data accessible to the user on the compromised machine.
A:H	A successful attack would allow the attacker to perform a denial of service on the compromised machine.