Single carriage returns are not filtered out by gnatcoll emails

ADACORE SECURITY ADVISORY

Document Id: SEC.GNATCOLL-CORE-0164

Version 1 - Jul 01, 2026

AdaCore

Title	Single carriage returns are not filtered out by gnatcoll emails	
Status	Final	
Author	Thomas Serabian	
Reviewed by	Frédéric Léger	

Revision History

Version	Date	Comments
1	Jun 30, 2026	Initial description

Contents

1. Preface

1.1. Scope

This document is an advisory describing the security impact of GNATCOLL-CORE-0164. The issue is tracked under the ticket number GNATCOLL-CORE-0164 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 2026-08-13 so that they can address the issue it describes before public availability.

Thereafter, it will be available to the general public under the terms of the CC BY-ND 4.0 license.

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` *24.0* (20231011)

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: 6.5 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N)

This vulnerability allows an *Improper Neutralization of CRLF Sequences* and/or *XML Injection* attack on an *GNATcoll-Core* if a compromised email is forwarded by an MTA (Message Transfer Agent) using `GNATcoll.email`.

A CVE (*Common Vulnerabilities and Exposures*) has been created for that case, and will be referred as `CAN-2026-2032501` (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.

In the `GNATcoll.email` module of `GNATcoll-core`, when utilizing functions like `Attach` and `New_Message`, caller-supplied `String` values for parameters like `MIME_Type`, `Charset`, `Description`, `Recommended_Filename`, and `Path` are spliced into header bodies without sufficient sanitization.

The serializer logic correctly strips `ASCII.LF`, but a standalone `ASCII.CR` is preserved and serialized onto the wire. Downstream lenient Message Transfer Agents interpret this bare carriage return as a header separator, enabling attackers to perform header injection (e.g., adding BCC recipients or splitting MIME parts) if they can control any of these parameters.

3. Solution

3.1. Workarounds

No workaround 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 `20260528`, 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	A crafted email must be transferred by a vulnerable MTA. The attacker can expect repeatable success with the same kind of attack.
PR:N	There is no privilege needed.
UI:N	Any invalid email may be used, no need for a user interaction once it is created.
S:U	Both the vulnerable component and the impacted component are managed by the same security authority.
C:L	There is some loss of confidentiality. Access to some restricted information is obtained, but the attacker does not have control over what information is obtained, or the amount or kind of loss is limited.
I:L	he email content may not be changed, but the list of receivers may be modified.
A:N	There is no impact to availability within the impacted component.