Unbounded Parser Expansion in XML/Ada Readers

ADACORE SECURITY ADVISORY

Document Id: SEC.XMLADA-0008

Version 2 - Jun 30, 2026

AdaCore

Title	Unbounded Parser Expansion in XML/Ada Readers	
Status	Final	
Author	Thomas Serabian	
Reviewed by	Frédéric Léger	

Revision History

Version	Date	Comments
1	Jun 10, 2026	Issue is fixed on 27.0
2	Jun 30, 2026	Updated impacted and fixed versions

Contents

1. Preface

1.1. Scope

This document is an advisory describing the security impact of `XMLADA-0008`. The issue is tracked under the ticket number `XMLADA-0008` 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:

- *XML/Ada* - `xmlada` *26.1* (20260107)

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

- `xmlada` < 27.0

2.2. Severity and Impact

CVSS v3.1 score: 9.1 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:H/E:P/RL:U/RC:C)

This vulnerability allows a *Denial of Service* attack and execution of external entities on *XML/Ada SAX Parser* if the attacker submits a crafted XML file containing external entities or exponential expansions to an application using the vulnerable component.

A CVE (*Common Vulnerabilities and Exposures*) has been created for that case, and will be referred as `CAN-2026-2030893` (until MITRE delivers a real CVE ID).

2.3. Detailed Description

Thanks to the investigation work done by Jon Hood, a vulnerability on *XML/Ada* has been discovered.

An issue in the SAX parser component of AdaCore XML/Ada allows remote attackers to cause a denial of service or execute XML External Entity (XXE) attacks via crafted XML data. The parser resolves and expands external general entities and external parameter entities by default. While the API exposes standard SAX feature flags (External_General_Entities_Feature and External_Parameter_Entities_Feature), configuring them via Set_Feature has no effect because the values are not consulted by the entity-resolution code paths in sax-readers.adb. Downstream applications that parse untrusted XML without explicitly overriding Resolve_Entity are vulnerable to arbitrary local file disclosure and exponential entity expansion (Billion Laughs), leading to unbounded CPU and memory consumption.

3. Solution

3.1. Workarounds

No work around is available

3.2. Correction

The Vulnerability described in this document is fixed in the following product versions:

- *XML/Ada* - `xmlada` >= 27.0

Starting from build date `20260615`, the *XML/Ada* component is fixed on `wavefront`.

4. Appendix

4.1. CVSS Score Justification

Metric	Justification
AV:N	The vulnerable XML/Ada SAX parser can process untrusted data received over the network, allowing remote attackers up to and including the entire Internet to trigger the vulnerability.
AC:L	The attacker only needs to submit a crafted XML payload to a downstream application utilizing the parser.
PR:N	There is no privilege needed.
UI:N	There is no user interaction needed.
S:U	The exploited vulnerability only impacts the downstream application processing the XML file, meaning the vulnerable and impacted components remain within the same security authority.
C:H	Resolution of external entities allows for arbitrary local file disclosure, resulting in a high impact on confidentiality.
I:N	The vulnerability does not allow modification of application data or system files, resulting in no impact on integrity.
A:H	Exponential entity expansion causes unbounded CPU and memory consumption, leading to a complete denial of service.