Path Traversal Vulnerability in Ada Web Server Attachment Processing

ADACORE SECURITY ADVISORY

Document Id: SEC.AWS-0175

Version 1 - Sep 01, 2026

AdaCore

Title	Path Traversal Vulnerability in Ada Web Server Attachment Processing	
Status	Final	
Author	Thomas Serabian	
Reviewed by	Frédéric Léger	

Revision History

Version	Date	Comments
1	Sept 01, 2026	Initial version

Contents

1 Preface **4**
1.1 Scope . . . 4
1.2 Distribution . . . 4
1.3 Contact . . . 4

2 Vulnerability **5**
2.1 Affected Products . . . 5
2.2 Severity and Impact . . . 5
2.3 Detailed Description . . . 5

3 Solution **6**
3.1 Workarounds . . . 6
3.2 Correction . . . 6

4 Appendix **7**
4.1 CVSS Score Justification . . . 7

1. Preface

1.1. Scope

This document is an advisory describing the security impact of `AWS-0175`. The issue is tracked under the ticket number `AWS-0175` 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 2026-10-30 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:

- *Ada Web Server* - `aws` *26.0* (20260107)

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

- `aws` < 26.2

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:N/I:H/A:H)

This vulnerability allows an Arbitrary Path Traversal attack (leading to Arbitrary File Write) on Ada Web Server if a malicious email attachment is processed via `AWS.POP.Write`.

A CVE (*Common Vulnerabilities and Exposures*) has been created for that case, and will be referred as `CAN-2026-2036805` (until MITRE delivers a real CVE ID).

2.3. Detailed Description

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

In Ada Web Server (AWS) up to and including version 26.2, AWS.POP.Write (Attachment, Directory) constructs output file paths by directly concatenating the user-supplied Directory parameter with the raw filename parameter extracted from an attachment's Content-Disposition MIME header. Neither AWS.Headers.Values.Search nor AWS.POP.Write sanitizes this input to remove path traversal sequences (..), directory separators, leading slashes, NUL bytes, or Windows drive letters. An unauthenticated remote attacker sending a crafted email can exploit this behavior to write or overwrite arbitrary files on the filesystem with the privileges of the AWS process user, potentially leading to remote code execution.

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:

- *Ada Web Server* - `aws` >= 26.2

Starting from build date `20260827`, the *Ada Web Server* 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 can be exploited remotely across the Internet without local network constraints.
AC:L	The attacker only needs to send a crafted email message containing a malicious attachment filename header to trigger the flaw.
PR:N	There is no privilege needed.
UI:N	No user interaction is required; attachment processing in AWS.POP.Write occurs automatically upon receiving the email.
S:U	Both the vulnerable component and the impacted component are managed by the same security authority.
C:N	The arbitrary file write flaw does not directly expose or read confidential system data.
I:H	A successful attack allows writing or overwriting arbitrary files accessible to the AWS process user account.
A:H	Overwriting critical application, configuration, or system files can cause a complete denial of service.