AWS does not handle timeout during SSL handshake

ADACORE SECURITY ADVISORY

Document Id: SEC.AWS-0095

Version 1 - Jun 30, 2025

AdaCore

Title	AWS does not handle timeout during SSL handshake	
Status	Final	
Author	Thomas Serabian	
Reviewed by	Frédéric Léger, Olivier Ramonat	

Revision History

Version	Date	Comments
1	Jun 15, 2025	Issue is fixed on wavefront

Contents

1. Preface

1.1. Scope

This document is an advisory describing the security impact of `AWS-0095`. The issue is tracked under the ticket number `AWS-0095` in AdaCore's issue tracking database.

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

1.2. Distribution

This advisory is made available in confidence to AdaCore customers under embargo until 2025-09-03 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` licence.

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` *25.2* (20250603)

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

- `aws` < 26.0

2.2. Severity and Impact

CVSS v3.1 score: 7.5 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H)

This vulnerabilty allows a *Denial of Service* attack on an *Ada Web Server* if the attacker sends a crafted 'hello' message of an incorrect size to the server during the initialization phase of the SSL handshake.

A CVE (*Common Vulnerabilities and Exposures*) has been created for that case, and will be referred as `CVE-2025-52494`.

2.3. Detailed Description

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

When a client initiates an HTTPS connection, the server performs the SSL handshake before assigning the connection to a processing slot. However, there is no specific timeout set for this phase, and the server uses the default socket timeout, which is effectively infinite.

An attacker can exploit this by sending a malformed TLS ClientHello message with incorrect length values. This causes the server to wait indefinitely for data that never arrives, blocking the worker thread (Line) handling the connection. By opening multiple such connections,up to the server's maximum limit, the attacker can exhaust all available working threads, preventing the server from handling new, legitimate requests.

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:

- *Ada Web Server* - `aws` > 25.2

Starting from build date `20250615`, 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 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 must only be able to send crafted TLS ClientHello packets.
PR:N	There is no privilege needed.
UI:N	There is no user interaction needed.
S:U	Both the vulnerable component and the impacted component are managed by the same security authority.
C:N	There is no impact on confidentiality.
I:N	There is no impact on integrity
A:H	A basic attack could result in a complete denial of service.