11.03.2026

Subject: Security Advisory for AEAD Cipher Vulnerability CVE 2025-15467

Dear Valued Utimaco Customer:

Utimaco has been made aware of a vulnerability affecting distribution of OpenSSL: This document provides an overview of the vulnerability, affected products and provides mitigation scenarios.

1 Affected products

- Enterprise Secure Key Manager (ESKM) Version 8 Software Releases 8.54.3 and earlier.

2 Issue

2.1 Description

A security regression (CVE-2025-15467) was discovered with Authenticated Encryption with Associated Data (AEAD) used in various versions of OpenSSL software. AEAD It is a modern cryptographic mode that simultaneously ensures the confidentiality (encryption), integrity, and authenticity of data. AEAD allows specific non-encrypted data (associated data) to be authenticated alongside the encrypted payload. AES-GCM is an AEAD cipher and issued by Utimaco's ESKM product.

Parsing CMS AuthEnvelopedData or EnvelopedData message with maliciously crafted AEAD parameters can trigger a stack buffer overflow.

Because the overflow occurs prior to authentication, no valid key material is required to trigger it. While exploitability to remote code execution depends on platform and toolchain mitigations, the stack-based write primitive represents a severe risk.

This issue has been reserved in the Common Vulnerabilities and Exposures list as CVE-2025-15467.
Details can be found here: NVD - CVE-2025-15467.

2.2 Detailed description

- OpenSSL versions from (including) 3.0.0 up to 3.0.19 (excluding)

ESKM has been released with OpenSSL software in the impacted range and uses AES-GCM cipher for:
SSL/TLS communications and to Wrap/Unwrap requests in cloud hold your own key (HYoK) implementations.

As of 3/9/2026, no exploitation has been identified in the wild.

Utimaco ESKMv8: is impacted by this vulnerability since it uses OpenSSL versions between 3.0.0 and 3.0.18.

Utimaco ESKMv5: Is not impacted by this vulnerability.

3 What To Do

3.1 Mitigation

A temporary workaround is not available.

4 Final Fix and Upcoming Changes in Next Release

ESKM Software Release 8.54.5 and all subsequent releases use OpenSSL 3.0.19 or greater and are available at Utimaco Support portal

5 Technical support

You can find technical support for Utimaco products in any of these ways:

- Download product information from https://support.hsm.utimaco.com/support
- Contact us at support@utimaco.com
- Contact our support hotline: EMEA +49 800-627-3081, Americas +1-844-UTIMACO (+1 844-884-6226), APAC +81 800-919-1301.

6 Legal notices

This Advisory is subject to the effective agreement executed between you and Utimaco IS GmbH, or otherwise the General Terms and Conditions of Utimaco IS GmbH: https://hsm.utimaco.com/terms-and-conditions/