ASSA ABLOY Global Solutions

Document ID	Revision	Date	Document category	
AAGS-KAM-SA-2025-02	**1.0**	**28/05/2025**	**Security Advisory**	
Confidentiality level			Status	Page (of)
Public			**Approved**	**1 (4)**

AAGS-KAM-SA-2025-02

Key and Asset Management

TLP:WHITE

Disclosure is not limited.

Overview

Traka is aware of a vulnerability report, CVE-2025-32433 concerning a critical vulnerability found in the SSH implementation of specific Erlang/OTP versions, arising from improper handling of SSH protocol messages, potentially allowing unauthenticated attackers to execute arbitrary code on affected systems.

While Traka products are not directly affected by the vulnerability and the SSH functionality is not enabled by default in Erlang/OTP installations, Erlang is installed as a dependency of RabbitMQ, which is in turn is an optional component of the TrakaWEB installation for customers using the following features:

- Real Time Update Service (RTUS)
- Allowance Across Systems (AAS)
- Scheduled Reports

Advisory Status

Investigation Done

Where a customer is using TrakaWEB with RabbitMQ 3.13.7 and Erlang 26.2.5.0, an Erlang patch has been tested to remediate this issue and we therefore recommend that you take action to apply it by following the guidance issued by Erlang: Otp 26.2.5.11 - Erlang/OTP as advised below.

AFFECTED PRODUCTS

Note: RabbitMQ and Erlang is not installed by default and is typically installed with the features outlined in the overview section.

TrakaWEB version	Erlang/OTP version	Rabbit MQ version	Resolution
Version 3.7.x	Version 26.2.5.0	Version 3.13.7	Erlang/OTP version 26.2.5.11
Version 3.8.x	Version 26.2.5.0	Version 3.13.7	Erlang/OTP version 26.2.5.11

Vulnerability Description

At the time of writing, TrakaWEB v4.5 is bundled with the optional installation of RabbitMQ 3.13.7 which in turn utilizes Erlang/OTP 26.2.5 (also known as Erlang/OTP 26.2.5.0). If you are using any other version of Erlang or unsure, please reach out to your Traka support team.

The vulnerability is specifically concerned with the Erlang programming language and runtime environment directly, where applications built upon it can utilise SSH functionality. RabbitMQ, at the time or writing, does not utilise the SSH functionality of Erlang, so therefore Traka's installation and utilization of RabbitMQ and Erlang is not vulnerable to this CVE. This is supported by the following RabbitMQ article, outlining that RabbitMQ is not affected by CVE-2025-32433 (an Erlang/OTP CVE) – take note of the affected versions of Erlang.

Furthermore, TrakaWEB is designed to be installed as an intranet facing application and is therefore not to be exposed directly to the public Internet. That said, we are aware that some customers may utilise Erlang for other software applications or purposes, in addition to TrakaWEB. This is why we still recommend taking the remedial action described below.

IMPACT

The vulnerability stems from a flaw in the SSH protocol message handling within Erlang/OTP's SSH server. Specifically, the server fails to properly enforce the SSH protocol sequence, allowing an attacker to send certain protocol messages before authentication is completed. This oversight enables the attacker to execute arbitrary code on the server without providing valid credentials.

SEVERITY

The Critical Vulnerability Scoring System (CVSS) has rated this as a critical vulnerability with a rating of 10, however it is important to appreciate that Traka requires the Erlang programming language runtime environment as a dependency of RabbitMQ. RabbitMQ is only installed where customers require the specific functionality outlined by the above features.

REMEDIATION

- If you do not use AAS, RTUS or Scheduled reports then there is no remedial action necessary.
- If you do use AAS, RTUS or Scheduled reports then check with your IT team if any other applications are dependent on Erlang. This is outside of Traka's scope.
- If TrakaWEB is used with RabbitMQ 3.13.7 and Erlang 26.2.5.0, an Erlang patch has been tested to remediate this issue and we therefore recommend that you take action to apply it by following the guidance issued by Erlang: Otp 26.2.5.11 - Erlang/OTP
- If you have another application or applications that also require the use of Erlang (alongside Traka, although this deployment approach is typically not recommended), we recommend that you discuss with your IT department before applying the patch to ensure that your other applications continue to be compatible with the latest update. Failure to consider other applications dependent upon Erlang may result in those application(s) failing to run.
- We would also encourage checking whether your Erlang installation and dependent applications (outside of Traka) have SSH enabled, if so, discuss with your central IT team whether this is required or whether it can be disabled. Failure to assess whether SSH is enabled may result in systems continuing to be vulnerable to other attacks in the future. It should be noted that any deployment where Erlang is used solely for Traka features then SSH is not enabled as part of our installation.

Contact Information

If you have additional questions, please contact your local Traka technical support.

REFERENCES

	Source	Locations
•	Erlang OTP/SSH article	https://www.offsec.com/blog/cve-2025-32433/
•	Erlang security Patch for Erlang v26.2.5.11	https://www.erlang.org/patches/otp-26.2.5.11
•	RabbitMQ is not affected by CVE-2025-32433	https://www.rabbitmq.com/blog/2025/04/24/rabbitmq-is-not-affected-by-cve-2025-32433

REVISION HISTORY

Revision	Date	Description
1. 1	[•]14/07/2025	[•]
2. [•]	[•]	[•]

TERMS OF USE