PSIRT Vulnerability Management Security Bulletin

Vulnerability in Thales Luna EFT

TLP:CLEAR

CVE-2024-5264

PURPOSE

The purpose of this document is to release a vulnerability affecting the Thales product or solution below.

VULNERABILITY SUMMARY

Network Transfer with AES KHT in **Thales Luna EFT 2.1 and before** allows a user with administrative console access to access backups taken via offline analysis.

IMPACT

This vulnerability impacts the following technologies:

- Thales Luna EFT

CVE DETAILS

CVE-ID			
CVE-2024-5264		Date	2024-05-23

Sentinel HASP Runtime

CVSS Scores & Vulnerability Types

CVSS Overall Score	5.9

https://www.first.org/cvss/calculator/3.1#CVSS:3.1/AV:N/AC:H/PR:H/UI:N/S:U/C:H/I:H/A:N

CVSS Base Score	5.9

CVSS Temporal Score	N/A

Vulnerability Type	Use of Crypt. Weak Pseudo-Random Number Generator (PRNG)
CWE ID	CWE-338

Product Affected by CVE

#	Product Type	Vendor	Product	Version
1	Application	Thales DIS	Luna EFT	<= 2.1.0

References for CVE

References:

1. https://supportportal.thalesgroup.com
2. https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2024-5264
3. https://cwe.mitre.org/data/definitions/338.html

Strategy

Fixed version	2.1.1
Fix release date	2024-05-20

SUPPORT CONTACT

- Please contact Thales PSIRT if you have more inquiries about the topic. Please use psirt@thalesgroup.com mail address.
- Visit Thales PSIRT page for encryption keys: https://www.thalesgroup.com/en/global/group/psirt