

# PSIRT Vulnerability Management Security Bulletin

## Vulnerability in Sentinel HASP Runtime

**TLP:CLEAR**

CVE-2024-0197

### PURPOSE

---

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

### VULNERABILITY SUMMARY

---

A flaw in the installer for **Thales SafeNet Sentinel HASP LDK prior to 9.16** on Windows allows an attacker to escalate their privilege level via local access.

### IMPACT

---

This vulnerability impacts the following technologies:

- Sentinel HASP Runtime

## CVE DETAILS

| CVE-ID                                                                                                                                                                                      |              |                               |                       |            |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------|-------------------------------|-----------------------|------------|
| CVE-2024-0197                                                                                                                                                                               |              |                               | Date                  | 2024-01-02 |
| Sentinel HASP Runtime                                                                                                                                                                       |              |                               |                       |            |
| CVSS Scores & Vulnerability Types                                                                                                                                                           |              |                               |                       |            |
| CVSS Overall Score                                                                                                                                                                          |              |                               |                       | 7.8        |
| <a href="https://www.first.org/cvss/calculator/3.1#CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H">https://www.first.org/cvss/calculator/3.1#CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H</a> |              |                               |                       |            |
| CVSS Base Score                                                                                                                                                                             |              | 7.8                           |                       |            |
| CVSS Temporal Score                                                                                                                                                                         |              | N/A                           |                       |            |
| Vulnerability Type                                                                                                                                                                          |              | Improper Privilege Management |                       |            |
| CWE ID                                                                                                                                                                                      |              | CWE-269                       |                       |            |
| Product Affected by CVE                                                                                                                                                                     |              |                               |                       |            |
| #                                                                                                                                                                                           | Product Type | Vendor                        | Product               | Version    |
| 1                                                                                                                                                                                           | Application  | Thales DIS                    | Sentinel HASP Runtime | < 9.16     |
| References for CVE                                                                                                                                                                          |              |                               |                       |            |
| References:                                                                                                                                                                                 |              |                               |                       |            |
| 1. <a href="https://supportportal.thalesgroup.com">https://supportportal.thalesgroup.com</a>                                                                                                |              |                               |                       |            |
| 2. <a href="https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2024-0197">https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2024-0197</a>                                                  |              |                               |                       |            |
| 3. <a href="https://cwe.mitre.org/data/definitions/269.html">https://cwe.mitre.org/data/definitions/269.html</a>                                                                            |              |                               |                       |            |
| Strategy                                                                                                                                                                                    |              |                               |                       |            |
| Fixed version                                                                                                                                                                               |              |                               |                       | 9.16       |
| Fix release date                                                                                                                                                                            |              |                               |                       | 2024-02-18 |

## SUPPORT CONTACT

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