Stored XSS vulnerability in Sentinel ACC

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2026-3457
State	PUBLISHED
Assigner	THA-PSIRT
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-03-27 09:16:20 UTC
Updated	2026-03-30 13:26:29 UTC
Description	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Thales Sentine

Risk And Classification

Primary CVSS: v4.0 7 HIGH from psirt@thalesgroup.com

CVSS:4.0/AV:L/AC:L/AT:N/PR:N/UI:N/VC:L/VI:H/VA:N/SC:L/SI:H/SA:N/E:P/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSC:X/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

EPSS: 0.000290000 probability, percentile 0.082600000 (date 2026-04-02)

Problem Types: CWE-79 | CWE-79 CWE-79 Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting')

Version	Source	Type	Score	Severity	Vector
4.0	psirt@thalesgroup.com	Secondary	7	HIGH	CVSS:4.0/AV:L/AC:L/AT:N/PR:N/UI:N/VC:L/VI:H/VA:N/SC:L/SI:H/SA:N/E:
4.0	CNA	CVSS	7	HIGH	CVSS:4.0/AV:L/AC:L/AT:N/PR:N/UI:N/VC:L/VI:H/VA:N/SC:L/SI:H/SA:N/E:

CVSS v4.0 Breakdown

Attack Vector

Local

Attack Complexity

Low

Attack Requirements

None

Privileges Required

None

User Interaction

None

Confidentiality

Low

ntegrity

High

vailability

None

ub Conf.

Low

ub Integrity

High

ub Availability

None

CVSS:4.0/AV:L/AC:L/AT:N/PR:N/UI:N/VC:L/VI:H/VA:N/SC:L/SI:H/SA:N/E:P/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSC:X/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Thales	Sentinel LDK Runtime	affected 10.22 custom	Windows

References

Reference	Source	Link	Tags
supportportal.thalesgroup.com/csm	psirt@thalesgroup.com	supportportal.thalesgroup.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

Vendor Comments And Credit

Discovery Credit

CNA: Josh Dillon (en)

Additional Advisory Data

Solutions

CNA: Upgrade current Sentinel LDK Runtime to version 10.22 or higher.

There are currently no legacy QID mappings associated with this CVE.

site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registred trademarks of The MITRE Corporation and the authoritative source of CVE content is MITRE's CVE web site. This site includes MITRE data granted under the following license.

CVE.report and Source URL Uptime Status status.cve.report