CVE-2026-3989

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2026-3989
State	PUBLISHED
Assigner	certcc
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-03-12 12:15:59 UTC
Updated	2026-04-07 19:16:47 UTC
Description	SGLangs `replay_request_dump.py` contains an insecure pickle.load() without validation and proper deserialization. An atta

Risk And Classification

Primary CVSS: v3.1 7.8 HIGH from ADP

CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H

EPSS: 0.000160000 probability, percentile 0.034910000 (date 2026-04-07)

Problem Types: CWE-502: Deserialization of Untrusted Data

Version	Source	Type	Score	Severity	Vector
3.1	ADP	DECLARED	7.8	HIGH	CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H
3.1	134c704f-9b21-4f2e-91b3-4a467353bcc0	Secondary	7.8	HIGH	CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H

CVSS v3.1 Breakdown

Attack Vector

Local

Attack Complexity

Low

Privileges Required

None

User Interaction

Required

Scope

Unchanged

Confidentiality

High

Integrity

High

Availability

High

CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	SGLang	SGLang	affected 0.5.10	Not specified

References

Reference	Source	Link	Tags
orca.security/resources/blog/sglang-llm-framework-rce-vulnerabilities	cret@cert.org	orca.security	
github.com/sgl-project/sglang/pull/20904	cret@cert.org	github.com	
github.com/sgl-project/sglang/releases/tag/v0.5.10	cret@cert.org	github.com	
github.com/sgl-project/sglang/blob/main/scripts/playground/replay_reques...	cret@cert.org	github.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

No vendor comments have been submitted for this CVE.

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