Missing integrity verification in Triton inference handler in Amazon SageMaker Python SDK

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

Summary

CVE	CVE-2026-8597
State	PUBLISHED
Assigner	AMZN
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-05-14 20:17:21 UTC
Updated	2026-05-15 14:10:31 UTC
Description	Missing integrity verification in the Triton inference handler in Amazon SageMaker Python SDK v2 before v2.257.2 and v3 b

Risk And Classification

Primary CVSS: v4.0 6.4 MEDIUM from ff89ba41-3aa1-4d27-914a-91399e9639e5

CVSS:4.0/AV:N/AC:L/AT:N/PR:H/UI:N/VC:N/VI:N/VA:N/SC:H/SI:H/SA:H/E:X/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: 0.000980000 probability, percentile 0.266960000 (date 2026-05-17)

Problem Types: CWE-354 | CWE-354 CWE-354 Improper validation of integrity check value

Version	Source	Type	Score	Severity	Vector
4.0	ff89ba41-3aa1-4d27-914a-91399e9639e5	Secondary	6.4	MEDIUM	CVSS:4.0/AV:N/AC:L/AT:N/PR:H/UI:N/VC:N/VI:N/VA
4.0	CNA	CVSS	6.4	MEDIUM	CVSS:4.0/AV:N/AC:L/AT:N/PR:H/UI:N/VC:N/VI:N/VA
3.1	ff89ba41-3aa1-4d27-914a-91399e9639e5	Secondary	7.2	HIGH	CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H
3.1	CNA	CVSS	7.2	HIGH	CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H

CVSS v4.0 Breakdown

Attack Vector

Network

Attack Complexity

Low

Attack Requirements

None

Privileges Required

High

User Interaction

None

Confidentiality

None

Integrity

None

Availability

None

Sub Conf.

High

Sub Integrity

High

Sub Availability

High

CVSS:4.0/AV:N/AC:L/AT:N/PR:H/UI:N/VC:N/VI:N/VA:N/SC:H/SI:H/SA:H/E:X/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

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

High

User Interaction

None

Scope

Unchanged

Confidentiality

High

Integrity

High

Availability

High

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

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Amazon SageMaker Python SDK	AWS	affected 2.199.0 2.257.1 custom	Not specified
CNA	Amazon SageMaker Python SDK	AWS	affected 3.0.0 3.7.1 custom	Not specified

References

References

Reference	Source	Link
github.com/aws/sagemaker-python-sdk/releases/tag/v3.8.0	ff89ba41-3aa1-4d27-914a-91399e9639e5	github.com
aws.amazon.com/security/security-bulletins/2026-031-aws	ff89ba41-3aa1-4d27-914a-91399e9639e5	aws.amazon.c
github.com/aws/sagemaker-python-sdk/releases/tag/v2.257.2	ff89ba41-3aa1-4d27-914a-91399e9639e5	github.com
github.com/aws/sagemaker-python-sdk/security/advisories/GHSA-rq6v-x3j8-7qgf	ff89ba41-3aa1-4d27-914a-91399e9639e5	github.com
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

No vendor comments have been submitted for this CVE.

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