Remote Code Execution in Google Agent Development Kit (ADK)

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

Summary

CVE	CVE-2026-4810
State	PUBLISHED
Assigner	GoogleCloud
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-04-13 09:16:08 UTC
Updated	2026-04-13 15:01:43 UTC
Description	A Code Injection and Missing Authentication vulnerability in Google Agent Development Kit (ADK) versions 1.7.0 (and 2.0.0

Risk And Classification

Primary CVSS: v4.0 9.3 CRITICAL from f45cbf4e-4146-4068-b7e1-655ffc2c548c

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

EPSS: 0.002950000 probability, percentile 0.528740000 (date 2026-04-15)

Problem Types: CWE-306 | CWE-306 CWE-306 Missing authentication for critical function

Version	Source	Type	Score	Severity	Vector
4.0	f45cbf4e-4146-4068-b7e1-655ffc2c548c	Secondary	9.3	CRITICAL	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:
4.0	CNA	CVSS	9.3	CRITICAL	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:

CVSS v4.0 Breakdown

Attack Vector

Network

Attack Complexity

Low

Attack Requirements

None

Privileges Required

None

User Interaction

None

None

Confidentiality

High

Integrity

High

Availability

High

Sub Conf.

High

Sub Integrity

High

Sub Availability

High

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

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Google Cloud	Agent Development Kit ADK	affected 1.7.0 1.28.1 custom	Not specified
CNA	Google Cloud	Agent Development Kit ADK	affected 2.0.0a1 2.0.0a2 custom	Not specified

References

Reference	Source	Link	Tags
github.com/google/adk-python/blob/main/CHANGELOG.md	f45cbf4e-4146-4068-b7e1-655ffc2c548c	github.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: Yoshizawa (en)

Additional Advisory Data

Solutions

CNA: Customers need to redeploy the ADK to version 1.28.1 (or 2.0.0a2) or later to receive the fix on their production environments. In addition, if they are running ADK Web locally, they also need to upgrade their local instance.

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

Free CVE JSON API cve.report/api

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