

Google Cloud Application Integration: Exposed internal APIs allow Information Disclosure and Remote Code Execution.

[MITRE](#)

[NVD](#)

[CVE.ORG](#)

[JSON API](#)

[Print: PDF](#)

Summary	
CVE	CVE-2026-2031
State	PUBLISHED
Assigner	GoogleCloud
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-05-15 16:16:14 UTC
Updated	2026-05-15 16:16:14 UTC
Description	An Improper Access Control vulnerability in several internal API endpoints for Google Cloud Application Integration prior to

Risk And Classification

Primary CVSS: v4.0 10 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:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSX/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/UC:ear

EPSS: 0.003230000 probability, percentile 0.554830000 (date 2026-05-17)

Problem Types: CWE-862 | CWE-862 CWE-862 Missing Authorization

Version	Source	Type	Score	Severity	Vector
4.0	f45cbf4e-4146-4068-b7e1-655ffc2c548c	Secondary	10	CRITICAL	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:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSX/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/UC:ear
4.0	CNA	CVSS	10	CRITICAL	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:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSX/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/UC:ear

CVSS v4.0 Breakdown

Attack Vector

Network

Attack Complexity

Low

Attack Requirements

None

Privileges Required

None

User Interaction

None

Confidentiality

High

Integrity

High

Availability

High

Sub Conf.

High

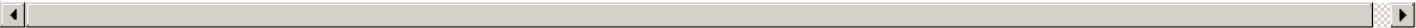
Sub Integrity

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:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSX:MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:CIear



Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Google Cloud	Internal Integration Platform APIs	affected 2026-01-23 date	Not specified

References

Reference	Source	Link	Tags
docs.cloud.google.com/gemini/enterprise/docs/release-notes	f45cbf4e-4146-4068-b7e1-655ffc2c548c	docs.cloud.google.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical



Vendor Comments And Credit

Discovery Credit
CNA: Arvin Shivram (en)

Additional Advisory Data

Solutions
CNA: These APIs were intended for internal Google use and access has been restricted to only authenticated Google employees. No action is required from external users.

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

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered 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](#).

Free CVE JSON API [cve.report/api](#)

CVE.report and Source URL Uptime Status [status.cve.report](#)