Gardyn Cloud API Authorization Bypass Through User-Controlled Key

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2026-25197
State	PUBLISHED
Assigner	icscert
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-04-03 21:17:09 UTC
Updated	2026-04-03 21:17:09 UTC
Description	A specific endpoint allows authenticated users to pivot to other user profiles by modifying the id number in the API call.

Risk And Classification

Primary CVSS: v4.0 9.3 CRITICAL from ics-cert@hq.dhs.gov

CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:N/SC:N/SI:N/SA:N/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: 0.000280000 probability, percentile 0.080640000 (date 2026-04-04)

Problem Types: CWE-639 | CWE-639 CWE-639

Version	Source	Type	Score	Severity	Vector
4.0	ics-cert@hq.dhs.gov	Secondary	9.3	CRITICAL	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:N/SC:N/SI:N/SA:N/E:
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:N/SC:N/SI:N/SA:N
3.1	ics-cert@hq.dhs.gov	Secondary	9.1	CRITICAL	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N
3.1	CNA	CVSS	9.1	CRITICAL	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N

CVSS v4.0 Breakdown

Attack Vector

Network

Attack Complexity

Low

Attack Requirements

None

Privileges Required

None

User Interaction

None

Confidentiality

High

Integrity

High

Availability

None

Sub Conf.

None

Sub Integrity

None

Sub Availability

None

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

None

User Interaction

None

Scope

Unchanged

Confidentiality

High

Integrity

High

Availability

None

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

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Gardyn	Cloud API	affected 2.12.2026 custom	Not specified

References

Reference	Source	Link	Tags

github.com/cisagov/CSAF/blob/develop/csaf_files/OT/white/2026/icsa-26-05...	ics-cert@hq.dhs.gov	github.com	
mygardyn.com/security	ics-cert@hq.dhs.gov	mygardyn.com	
www.cisa.gov/news-events/ics-advisories/icsa-26-055-03	ics-cert@hq.dhs.gov	www.cisa.gov	
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: Michael Groberman reported these vulnerabilities to CISA. (en)

Additional Advisory Data

Solutions

CNA: Gardyn states that the relevant fixes are included in the latest version of the Gardyn mobile application. Users are required to run a supported version of the Gardyn App on their phone in order to access Gardyn services and devices. The current versions of the Gardyn App and the Gardyn Home firmware can be checked in the Gardyn App. For all vulnerabilities, Gardyn recommends users ensure their home kit and studio devices are upgraded to firmware master.622 or later. Gardyn also recommends that users update their mobile application to the most recent version. Gardyn requests that users ensure their devices have network connectivity in order to automatically download needed firmware updates. Unconnected devices will automatically update when configured with a working Internet connection.

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