

CVE-2024-39891

Twilio Authy Information Disclosure Vulnerability

CISA KEV since Jul 23, 2024

Actively exploited

In the Twilio Authy API, accessed by Authy Android before 25.1.0 and Authy iOS before 26.1.0, an unauthenticated endpoint provided access to certain phone-number data, as exploited in the wild in June 2024. Specifically, the endpoint accepted a stream of requests containing phone numbers, and responded with information about whether each phone number was registered with Authy. (Authy accounts were not compromised, however.)

EVRS 75 _{/100} Urgent priority	CVSS V3.1 5.3 Medium · NVD	EPSS 0.017 76.6th percentile · FIRST	CISA DEADLINE Aug 13, 2024 KEV since 2024 · listed over a year
--	--	--	--

Signals behind the score

☒ counted in the score ☐ not counted

evidence for 6 of 8 signals

☒ CISA KEV	Listed in the catalog	☐ Vendor exploitation	Confirmed exploitation in the wild
☐ Ransomware	No known ransomware campaign association	☐ KEV recency	On the CISA KEV catalog for over two years
☒ EPSS	0.017 probability	☐ Pre-patch disclosure	Disclosure status unavailable
☒ CVSS	Base score 5.3	☐ Microsoft Exploitability Index	Not a Microsoft CVE

Remediation

Patch This Cycle No patch reported by the connected remediation source

CISA required action: Apply mitigations per vendor instructions or discontinue use of the product if mitigations are unavailable.

Basis: CISA KEV required action

Affected and fixed versions

PACKAGE	AFFECTED	FIXED IN	SOURCE
authy	< 26.1.0	26.1.0	NVD
authy authenticator	< 25.1.0	25.1.0	NVD

Sources

Vendor guidance	cwe.mitre.org/data/definitions/203.html	Additional guidance	bleepingcomputer.com/news/security/hackers-abused-api-to-verify-millions-of-authy-mfa-phone-numbers/
Additional guidance	twilio.com/docs/usage/security/reporting-vulnerabilities	Additional guidance	twilio.com/en-us/changelog
twilio.com	twilio.com/en-us/changelog/Security_Alert_Authy_App_Android_iOS	NVD	nvd.nist.gov/vuln/detail/CVE-2024-39891
CISA KEV	cisa.gov/known-exploited-vulnerabilities-catalog	ENISA EUVD	euvd.enisa.europa.eu/vulnerability/EUVD-2024-38291
Current data	evulnable.com/vulnerability-management/cve/CVE-2024-39891		

Snapshot at generation time. EPSS can move quickly. A public exploit module is not evidence of active exploitation.