Authlib: 1-click Account Takeover

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

Summary

CVE	CVE-2025-68158
State	PUBLISHED
Assigner	GitHub_M
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-01-08 18:15:59 UTC
Updated	2026-03-30 13:16:21 UTC
Description	Authlib is a Python library which builds OAuth and OpenID Connect servers. In versions 1.0.0 through 1.6.5, cache-backed

Risk And Classification

Primary CVSS: v3.1 8.8 HIGH from nvd@nist.gov

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

EPSS: 0.000250000 probability, percentile 0.069680000 (date 2026-04-24)

Problem Types: CWE-352 | CWE-352 CWE-352: Cross-Site Request Forgery (CSRF)

Version	Source	Type	Score	Severity	Vector
3.1	nvd@nist.gov	Primary	8.8	HIGH	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H
3.1	security-advisories@github.com	Secondary	5.7	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:U/C:H/I:N/A:N
3.1	CNA	DECLARED	5.7	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:U/C:H/I:N/A:N

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

Required

Scope

Unchanged

Confidentiality

High

ntegrity

High

Availability

High

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Authlib	Authlib	All	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Authlib	Authlib	affected >= 1.0.0, < 1.6.6	Not specified

References

Reference	Source	Link
github.com/authlib/authlib/commit/2808378611dd6fb2532b189a9087877d8f0c0489	security-advisories@github.com	github.com
github.com/authlib/authlib/commit/7974f45e4d7492ab5f527577677f2770ce423228	security-advisories@github.com	github.com
github.com/authlib/authlib/security/advisories/GHSA-fg6f-75jq-6523	134c704f-9b21-4f2e-91b3-4a467353bcc0	github.com
CVE Program record	CVE.ORG	www.cve.or
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.