

jupyterhub / **oauthenticator** Public[Code](#) [Issues](#) 46 [Pull requests](#) 7 [Actions](#) [Projects](#) [Wiki](#) [Security](#)

# Authentication Bypass in Auth0Authenticator via Unverified Email Claims

High minrk published **GHSA-rrvg-cxh4-qhrv** yesterday

## Package

 **oauthenticator** (pip)

### Affected versions

&lt;= 17.3.1

### Patched versions

17.4.0

## Description

### Summary

An authentication bypass vulnerability in `oauthenticator` allows an attacker with an unverified email address on an Auth0 tenant to login to JupyterHub. When `email` is used as the `username_claim`, this gives users control over their username and the possibility of account takeover.

### Impact

This is an **Authentication Bypass Vulnerability**. Any Auth0 tenant leveraging the `Auth0Authenticator` mapping the `email` claim to the JupyterHub username is impacted. By default, Auth0 handles email verification as a user flag, not a hard block to authentication streams. If an attacker can register an account with the Auth0 tenant with an unverified email and knows the email of an existing user on the system, they can authenticate as that user.

### Patches

- Upgrade `oauthenticator` to 17.4

### Workarounds

- Check `email_verified` field in an `Authenticator.post_auth_hook` function
- Do not use `email` as the username claim

- [Enforce email verification in auth0](#)

### Severity

**High** 8.8 / 10

#### CVSS v3 base metrics

Attack vector	Network
Attack complexity	Low
Privileges required	Low
User interaction	None
Scope	Unchanged
Confidentiality	High
Integrity	High
Availability	High

[Learn more about base metrics](#)

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

### CVE ID

CVE-2026-33175

### Weaknesses

- ▶ CWE-287
- ▶ CWE-290

### Credits



Jaynornj

Reporter



Pr00fOf3xploit

Reporter