Authentication Cookies Remain Valid After Password Reset and Server Restart

Moderate **Yann-P** published **GHSA-5mrq-x3x5-8v8f** 8 hours ago

Package

jupyter-server (pip)

Affected versions	Patched versions
<=2.17.0	2.18.0

Description

Summary

A persistent cookie secret vulnerability allows authenticated users to maintain indefinite access even after password changes.

The cookie secret used to sign authentication cookies is stored in a permanent file (`~/.local/share/jupyter/runtime/jupyter_cookie_secret`) that is never automatically rotated or cleared, allowing stolen or compromised cookies to remain valid indefinitely regardless of password resets.

PoC

- Start a Jupyter server with password authentication: `jupyter server password`, `jupyter server`
- Log in with the password and capture the authentication cookie (e.g., just login with a browser).
- Change the password to revoke access: `jupyter server password`
- Restart the server
- Use the old stolen cookie => remains valid and provides full authenticated access.

Impact

- All jupyter-server deployments using password authentication where security incidents may occur
- Multi-user systems where one user's compromised session should be revocable by administrators
- Shared or public-facing Jupyter servers where credential rotation is a security requirement
- Any deployment where password changes are expected to revoke existing sessions

Patches

Jupyter Server 2.18+

Workaround

```
rm ~/.local/share/jupyter/runtime/jupyter_cookie_secret
# Then restart the server
```

Severity

Moderate 6.8 / 10

CVSS v3 base metrics

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

Learn more about base metrics

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

CVE ID

CVE-2026-40934

Weaknesses

▶ CWE-613

Credits


emin63 Reporter


Yann-P Coordinator