CVE-2026-21622

Password Reset Tokens Do Not Expire

« Back to all CVEs

See on OSV.dev »

Weakness Type (CWE)

CWE-613 — CWE-613 Insufficient Session Expiration

CAPEC

CAPEC-21 — CAPEC-21 Exploitation of Session Variables, Resource IDs and other Trusted Credentials

CVSS 4.0 Score

9.5

CRITICAL

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

Vulnerability description

Insufficient Session Expiration vulnerability in hexpm hexpm/hexpm ('Elixir.Hexpm.Accounts.PasswordReset' module) allows Account Takeover.
Password reset tokens generated via the "Reset your password" flow do not expire. When a user requests a password reset, Hex sends an email containing a reset link with a token. This token remains valid indefinitely until used. There is no time-based expiration enforced.

If a user's historical emails are exposed through a data breach (e.g., a leaked mailbox archive), any unused password reset email contained in that dataset could be used by an attacker to reset the victim's password. The attacker does not need current access to the victim's email account, only access to a previously leaked copy of the reset email.

This vulnerability is associated with program files `lib/hexpm/accounts/password_reset.ex` and program routines `'Elixir.Hexpm.Accounts.PasswordReset':can_reset?/3`.

This issue affects hexpm: from 617e44c71f1dd9043870205f371d375c5c4d886d before bb0e420919.

Affected

pkg:github/hexpm/hexpm

Module	Source File	Routine
`Hexpm.Accounts.PasswordReset`	lib/hexpm/accounts/password_reset.ex	`Hexpm.Accounts.PasswordReset.can_reset?/3`

Status	Type	Version	Changes / Fixed in
Affected	git ⓘ	617e44c71f	< bb0e420919

`hexpm / hex.pm`

Status	Type	Version	Changes / Fixed in
Affected	date	`2025-08-01`	< `2026-03-05`

Workarounds

Users who suspect email exposure should:

- Immediately reset their password.
- Enable and enforce 2FA.

There is no complete mitigation without implementing token expiration.

References

- https://github.com/hexpm/hexpm/security/advisories/GHSA-6r94-pvwf-mxqm vendor-advisory related
- https://osv.dev/vulnerability/EEF-CVE-2026-21622 related
- https://github.com/hexpm/hexpm/commit/bb0e42091995945deef10556f58d046a52eb7884 patch

Credits

- **Finder**: Michael Lubas / Paraxial.io
- **Remediation developer**: Jonatan Männchen / EEF
- **Remediation reviewer**: Eric Meadows-Jönsson / Hex.pm

CVE record as JSON: `GET /cves/CVE-2026-21622.json`
OSV record as JSON: `GET /osv/EEF-CVE-2026-21622.json`