



EEF-CVE- 2026-21622

[See a problem?](#)

Please try reporting it [to the source](#) [↗](#) first.

Source	https://cna.erlef.org/osv/EEF-CVE-2026-21622.html ↗
Import Source	https://cna.erlef.org/osv/EEF-CVE-2026-21622.json ↗
JSON Data	https://api.osv.dev/v1/vulns/EEF-CVE-2026-21622 ↗
Aliases	CVE-2026-21622 GHSA-6r94-pvww-mxqm
Published	2026-03-05T21:18:03.883Z
Modified	2026-04-21T08:30:06.594674Z
Severity	9.5 (Critical) CVSS_V4 - 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 CVSS Calculator ↗

Summary Password Reset Tokens Do Not Expire

Details

Summary

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/passwordreset.ex` and *program routines*

'Elixir.Hexpm.Accounts.PasswordReset':canreset?/3.


This issue affects hexpm: from 617e44c71f1dd9043870205f371d375c5c4d886d before bb0e42091995945deef10556f58d046a52eb7884.

Workaround




Users who suspect email exposure should:

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

There is no complete mitigation without implementing token expiration.

Database specific  {

```
"cpe_ids": [  
  "cpe:2.3:a:hexpm:hexpm:*:*:*:*:*:*:*:*"  
],  
"capec_ids": [  
  "CAPEC-21"  
],  
"cwe_ids": [  
  "CWE-613"  
]  
}
```

References <https://github.com/hexpm/hexpm/security/advisories/GHSA-6r94-pvwf-mxqm> 
<https://cna.erlef.org/cves/CVE-2026-21622.html> 
<https://github.com/hexpm/hexpm/commit/bb0e42091995945deef10556f58d046a52eb7884> 

Credits

Michael Lubas / Paraxial.io - FINDER
Jonatan Männchen / EEF - REMEDIATION_DEVELOPER
Eric Meadows-Jönsson / Hex.pm - REMEDIATION_REVIEWER

Affected packages


Git
github.com/hexpm/hexpm.git

Affected ranges 


Type GIT

Repo <https://github.com/hexpm/hexpm.git>

Events Introduced

[617e44c71f1dd9043870205f371d375c5c4d886d](#) 

Fixed

[bb0e42091995945deef10556f58d046a52eb7884](#) 

Database specific 

▶ source
