CVE-2026-32148

Lockfile checksums not verified in Hex allows dependency integrity bypass

« Back to all CVEs

See on OSV.dev »

Weakness Type (CWE)

CWE-354 — CWE-354 Improper Validation of Integrity Check Value

CVSS 4.0 Score

8.9

HIGH

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

Vulnerability description

Insufficient Verification of Data Authenticity vulnerability in hexpm hex (`Hex.RemoteConverger` module) allows dependency integrity bypass via unverified lockfile checksums.
Hex stores checksums for dependencies in the `mix.lock` file to ensure reproducible and integrity-checked builds. However, `Hex.RemoteConverger.verify_resolved/2` never executes checksum verification because the lock data returned by `Hex.Utils.lock/1` uses string-based dependency names, while the verification logic compares against atom-based names. This type mismatch causes the verification code path to be silently skipped. Checksums are still validated when packages are initially downloaded from the registry, but mismatches between the lockfile and resolved dependencies are not detected.

An attacker who can influence cached packages (e.g., via local cache poisoning or a compromised registry) can provide modified dependency contents that will be accepted without detection. The `mix.lock` file is silently rewritten with the checksum values from the registry, erasing evidence of tampering.

This issue affects hex: from 0.16.0 before 2.4.2.

Affected

`pkg:otp/hex`

Module	Source File	Routine
`Hex.RemoteConverger`	`lib/hex/remote_converger.ex`	`Hex.RemoteConverger.verify_resolved/2`

Status	Type	Version	Changes / Fixed in
Affected	semver ⓘ	`0.16.0`	< `2.4.2`

pkg:github/hexpm/hex

Module	Source File	Routine
`Hex.RemoteConverger`	lib/hex/remote_converger.ex	`Hex.RemoteConverger.verify_resolved/2`

Status	Type	Version	Changes / Fixed in
Affected	git ⓘ	e01576f28c	< d7528c8199

References

- https://github.com/hexpm/hex/security/advisories/GHSA-hmv9-4mfr-m92v **vendor-advisory** **related**
- https://osv.dev/vulnerability/EEF-CVE-2026-32148 **related**
- https://github.com/hexpm/hex/commit/d7528c8199a11445111508bf3a6460026a5a14c8e **patch**

Credits

- **Finder**: Paul Fleischer
- **Remediation developer**: Jonatan Männchen / EEF
- **Remediation reviewer**: Eric Meadows-Jönsson / Hex.pm

CVE record as JSON: `GET /cves/CVE-2026-32148.json`
OSV record as JSON: `GET /osv/EEF-CVE-2026-32148.json`