EEF-CVE-2026-32148

See a problem?
Please try reporting it to the source first.

Source	https://cna.erlef.org/osv/EEF-CVE-2026-32148.html
Import Source	https://cna.erlef.org/osv/EEF-CVE-2026-32148.json
JSON Data	https://api.osv.dev/v1/vulns/EEF-CVE-2026-32148
Aliases	CVE-2026-32148 GHSA-hmv9-4mfr-m92v
Published	2026-04-30T18:17:03.783Z
Modified	2026-04-30T18:26:27.900731685Z
Severity	8.9 (High) CVSS_V4 - 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 CVSS Calculator
Summary	Lockfile checksums not verified in Hex allows dependency integrity bypass

Details

Summary

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.

Database specific


```
{
    "cpe_ids": [
        "cpe:2.3:a:hexpm:hex:*:*:*:*:*:*:*:*"
    ],
    "cwe_ids": [
        "CWE-354",
        "CWE-494"
    ],
    "capec_ids": []
}
```


References

https://github.com/hexpm/hex/security/advisories/GHSA-hmv9-4mfr-m92v

https://cna.erlef.org/cves/CVE-2026-32148.html

https://github.com/hexpm/hex/commit/d7528c8199a1144511508bf3a6460026a5a14c8e

Credits

Paul Fleischer - FINDER

Jonatan Männchen / EEF - REMEDIATION_DEVELOPER

Eric Meadows-Jönsson / Hex.pm - REMEDIATION_REVIEWER

Affected packages

Git
github.com/hexpm/hex.git

Affected ranges

Type GIT

Repo https://github.com/hexpm/hex.git

Events Introduced
e01576f28c64af9fae6eb17e2dad30f6efcb303c
Fixed
d7528c8199a1144511508bf3a6460026a5a14c8e

Affected versions

- v0.*
- v1.*
- v2.*

Database specific

- source
