



# Lockfile checksums not verified in Hex allows dependency integrity bypass

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

## Summary

|                        |  |
|------------------------|--|
| <b>CVE</b>             | CVE-2026-32148   |
| <b>State</b>           | PUBLISHED  |
| <b>Assigner</b>        | EEF  |
| <b>Source Priority</b> | CVE Program / NVD first with legacy fallback   |
| <b>Published</b>       | 2026-04-30 19:16:09 UTC  |
| <b>Updated</b>         | 2026-05-05 02:16:49 UTC  |
| <b>Description</b>     | Insufficient Verification of Data Authenticity vulnerability in hexpm hex (Hex.RemoteConverger module) allows dependency |

## Risk And Classification

**Primary CVSS:** v4.0 8.9 HIGH from 6b3ad84c-e1a6-4bf7-a703-f496b71e49db

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/E:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSX/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

**EPSS:** 0.000190000 probability, percentile 0.052090000 (date 2026-05-04)

**Problem Types:** CWE-354 | CWE-494 | CWE-354 CWE-354 Improper Validation of Integrity Check Value | CWE-494 CWE-494 Download of Code Without Integrity Check

| Version | Source                               | Type      | Score | Severity | Vector   |
|---------|--------------------------------------|-----------|-------|----------|--|
| 4.0     | 6b3ad84c-e1a6-4bf7-a703-f496b71e49db | Secondary | 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/E:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSX/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X |
| 4.0     | CNA                                  | CVSS      | 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/E:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSX/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X |
| 3.1     | nvd@nist.gov                         | Primary   | 5.9   | MEDIUM   | CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:H/A:N   |

## CVSS v4.0 Breakdown

Attack Vector

Network

Attack Complexity

Low

Attack Requirements

Present

Privileges Required

None

User Interaction

Active

Confidentiality

High

Integrity

High

Availability

High

Sub Conf.

High

Sub Integrity

High

Sub Availability

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/E:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSX/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

### CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

High

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

None

Integrity

High

Availability

None

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

### NVD Known Affected Configurations (CPE 2.3)

| Type        | Vendor | Product | Version | Update | Edition | Language |
|-------------|--------|---------|---------|--------|---------|----------|
| Application | Hex    | Hex     | All     | All    | All     | All      |

### Vendor Declared Affected Products

| Source | Vendor | Product | Version |
|--------|--------|---------|---------|
|--------|--------|---------|---------|

| Source | Vendor                | Product             | Version  |
|--------|-----------------------|---------------------|--|
| CNA    | <a href="#">Hexpm</a> | <a href="#">Hex</a> | affected 0.16.0 2.4.2 semver   |
| CNA    | <a href="#">Hexpm</a> | <a href="#">Hex</a> | affected e01576f28c64af9fae6eb17e2dad30f6efcb303c d7528c8199a1144511508bf3a6460026a5a14c8e git |

## References

| Reference  | Source                               | Link                          |
|--|--------------------------------------|-------------------------------|
| github.com/hexpm/hex/commit/d7528c8199a1144511508bf3a6460026a5a14c8e | 6b3ad84c-e1a6-4bf7-a703-f496b71e49db | <a href="#">github.com</a>    |
| osv.dev/vulnerability/EEF-CVE-2026-32148                             | 6b3ad84c-e1a6-4bf7-a703-f496b71e49db | <a href="#">osv.dev</a>       |
| cna.erlef.org/cves/CVE-2026-32148.html                               | 6b3ad84c-e1a6-4bf7-a703-f496b71e49db | <a href="#">cna.erlef.org</a> |
| github.com/hexpm/hex/security/advisories/GHSA-hmv9-4mfr-m92v         | 134c704f-9b21-4f2e-91b3-4a467353bcc0 | <a href="#">github.com</a>    |
| CVE Program record   | CVE.ORG                              | <a href="#">www.cve.org</a>   |
| NVD vulnerability detail   | NVD                                  | <a href="#">nvd.nist.gov</a>  |

## Vendor Comments And Credit

Discovery Credit

**CNA:** Paul Fleischer (en)

**CNA:** Jonatan Männchen / EEF (en)

**CNA:** Eric Meadows-Jönsson / Hex.pm (en)

There are currently no legacy QID mappings associated with this CVE.

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

Free CVE JSON API [cve.report/api](#)

CVE.report and Source URL Uptime Status [status.cve.report](#)