



# Unsafe Deserialization of Erlang Terms in hex\_core

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

## Summary

<b>CVE</b>	CVE-2026-21619
<b>State</b>	PUBLISHED
<b>Assigner</b>	EEF
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2026-02-27 18:16:11 UTC
<b>Updated</b>	2026-04-06 17:17:07 UTC
<b>Description</b>	Uncontrolled Resource Consumption, Deserialization of Untrusted Data vulnerability in hexpm hex_core (hex_api modules)

## Risk And Classification

**Primary CVSS:** v4.0 2 LOW from 6b3ad84c-e1a6-4bf7-a703-f496b71e49db

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

**Problem Types:** CWE-400 | CWE-502 | CWE-400 CWE-400 Uncontrolled Resource Consumption | CWE-502 CWE-502 Deserialization of Untrusted Data

Version	Source	Type	Score	Severity	Vector
4.0	6b3ad84c-e1a6-4bf7-a703-f496b71e49db	Secondary	2	LOW	CVSS:4.0/AV:N/AC:L/AT:P/PR:L/UI:A/VC:N/VI:N/VA:L
4.0	CNA	CVSS	2	LOW	CVSS:4.0/AV:N/AC:L/AT:P/PR:L/UI:A/VC:N/VI:N/VA:L
3.1	nvd@nist.gov	Primary	7.5	HIGH	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

## CVSS v4.0 Breakdown

Attack Vector

Network

Attack Complexity

Low

Attack Requirements

Present

Privileges Required

Low

User Interaction

Active

Confidentiality

None

Integrity

None

Availability

Low

Sub Conf.

None

Sub Integrity

None

Sub Availability

None

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

Low

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

None

Integrity

None

Availability

High

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

### NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Erlang	Rebar3	All	All	All	All
Application	Hex	Hex	All	All	All	All
Application	Hex	Hex Core	All	All	All	All

### Vendor Declared Affected Products

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

CNA	<a href="#">Hexpm</a>	<a href="#">Hex Core</a>	affected eb327f8edfe45507351e38cc0805aa12fa647f0b cdf726095bca85ad2549d146df1e831ae93c2b13 git
CNA	<a href="#">Hexpm</a>	<a href="#">Hex Core</a>	affected 0.1.0 0.12.1 semver
CNA	<a href="#">Hexpm</a>	<a href="#">Hex</a>	affected 314546ac432229518714cc8e3336e916b9da6305 636739f3322514e9303ca335fb630696fcb3c95 g
CNA	<a href="#">Hexpm</a>	<a href="#">Hex</a>	affected 2.3.0 2.3.2 semver
CNA	<a href="#">Erlang</a>	<a href="#">Rebar3</a>	affected 209c02ec57c2cc3207ee0174c3af3675b8dc8f79 1d4478f527e373de0b225951e53115450e0d9b9d g
CNA	<a href="#">Erlang</a>	<a href="#">Rebar3</a>	affected 3.9.1 3.27.0 semver

## References

Reference	Source	Link
github.com/hexpm/hex/commit/636739f3322514e9303ca335fb630696fcb3c95	6b3ad84c-e1a6-4bf7-a703-f496b71e49db	<a href="#">github.co</a>
github.com/erlang/rebar3/commit/1d4478f527e373de0b225951e53115450e0d9b9d	6b3ad84c-e1a6-4bf7-a703-f496b71e49db	<a href="#">github.co</a>
cna.erlef.org/cves/CVE-2026-21619.html	6b3ad84c-e1a6-4bf7-a703-f496b71e49db	<a href="#">cna.erlef.</a>
github.com/hexpm/hex_core/security/advisories/GHSA-hx9w-f2w9-9g96	6b3ad84c-e1a6-4bf7-a703-f496b71e49db	<a href="#">github.co</a>
github.com/hexpm/hex_core/commit/cdf726095bca85ad2549d146df1e831ae93c2b13	6b3ad84c-e1a6-4bf7-a703-f496b71e49db	<a href="#">github.co</a>
osv.dev/vulnerability/EEF-CVE-2026-21619	6b3ad84c-e1a6-4bf7-a703-f496b71e49db	<a href="#">osv.dev</a>
CVE Program record	CVE.ORG	<a href="#">www.cve</a>
NVD vulnerability detail	NVD	<a href="#">nvd.nist.g</a>

## Vendor Comments And Credit

### Discovery Credit

**CNA:** Michael Lubas / Paraxial.ia (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](#).

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