Unsafe Deserialization of Erlang Terms in hex_core

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2026-21619
State	PUBLISHED
Assigner	EEF
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-02-27 18:16:11 UTC
Updated	2026-04-06 17:17:07 UTC
Description	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/MSC:X/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

ntegrity

None

vailability

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/MSC:X/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

CVSS v3.1 Breakdown

ttack Vector

Network

ttack Complexity

Low

rivileges Required

None

ser Interaction

None

cope

Unchanged

onfidentiality

None

ntegrity

None

vailability

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	Hexpm	Hex Core	affected eb327f8edfe45507351e38cc0805aa12fa647f0b cdf726095bca85ad2549d146df1e831ae93c2b13 git
CNA	Hexpm	Hex Core	affected 0.1.0 0.12.1 semver
CNA	Hexpm	Hex	affected 314546ac432229518714cc8e3336e916b9da6305 636739f3322514e9303ca335fb630696fcbb3c95 g
CNA	Hexpm	Hex	affected 2.3.0 2.3.2 semver
CNA	Erlang	Rebar3	affected 209c02ec57c2cc3207ee0174c3af3675b8dc8f79 1d4478f527e373de0b225951e53115450e0d9b9d g
CNA	Erlang	Rebar3	affected 3.9.1 3.27.0 semver

References

Reference	Source	Link
github.com/hexpm/hex/commit/636739f3322514e9303ca335fb630696fcbb3c95	6b3ad84c-e1a6-4bf7-a703-f496b71e49db	github.co
github.com/erlang/rebar3/commit/1d4478f527e373de0b225951e53115450e0d9b9d	6b3ad84c-e1a6-4bf7-a703-f496b71e49db	github.co
cna.erlef.org/cves/CVE-2026-21619.html	6b3ad84c-e1a6-4bf7-a703-f496b71e49db	cna.erlef.
github.com/hexpm/hex_core/security/advisories/GHSA-hx9w-f2w9-9g96	6b3ad84c-e1a6-4bf7-a703-f496b71e49db	github.co
github.com/hexpm/hex_core/commit/cdf726095bca85ad2549d146df1e831ae93c2b13	6b3ad84c-e1a6-4bf7-a703-f496b71e49db	github.co
osv.dev/vulnerability/EEF-CVE-2026-21619	6b3ad84c-e1a6-4bf7-a703-f496b71e49db	osv.dev
CVE Program record	CVE.ORG	www.cve
NVD vulnerability detail	NVD	nvd.nist.g

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.