Denial of Service via Oversized Package Upload

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2026-23940
State	PUBLISHED
Assigner	EEF
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-03-13 19:54:14 UTC
Updated	2026-04-06 17:17:08 UTC
Description	Uncontrolled Resource Consumption vulnerability in hexpm hexpm/hexpm allows Excessive Allocation. Publishing an overs

Risk And Classification

Primary CVSS: v4.0 7.1 HIGH from 6b3ad84c-e1a6-4bf7-a703-f496b71e49db

CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:N/VI:N/VA:H/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-400 CWE-400 Uncontrolled Resource Consumption

Version	Source	Type	Score	Severity	Vector
4.0	6b3ad84c-e1a6-4bf7-a703-f496b71e49db	Secondary	7.1	HIGH	CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:N/VI:N/VA:
4.0	CNA	CVSS	7.1	HIGH	CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:N/VI:N/VA:
3.1	nvd@nist.gov	Primary	6.5	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H

CVSS v4.0 Breakdown

Attack Vector

Network

Attack Complexity

Low

Attack Requirements

None

Privileges Required

Low

User Interaction

None

Confidentiality

None

Integrity

None

Availability

High

Sub Conf.

None

Sub Integrity

None

Sub Availability

None

CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:N/VI:N/VA:H/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

Attack Vector

Network

Attack Complexity

Low

Privileges Required

Low

User Interaction

None

Scope

Unchanged

Confidentiality

None

Integrity

None

Availability

High

CVSS:3.1/AV:N/AC:L/PR:L/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	Hex	Hexpm	All	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Hexpm	Hexpm	affected 495f01607d3eae4aed7ad09b2f54f31ec7a7df01 git	Not specified
CNA	Hexpm	Hex.pm	affected 2026-03-10 date	Not specified

References

Reference	Source	Link
github.com/hexpm/hexpm/commit/495f01607d3eae4aed7ad09b2f54f31ec7a7df01	6b3ad84c-e1a6-4bf7-a703-f496b71e49db	github.com
osv.dev/vulnerability/EEF-CVE-2026-23940	6b3ad84c-e1a6-4bf7-a703-f496b71e49db	osv.dev
github.com/hexpm/hexpm/security/advisories/GHSA-jp8w-gxf6-8hcr	6b3ad84c-e1a6-4bf7-a703-f496b71e49db	github.com
cna.erlef.org/cves/CVE-2026-23940.html	6b3ad84c-e1a6-4bf7-a703-f496b71e49db	cna.erlef.org
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

Vendor Comments And Credit

Discovery Credit

CNA: Joud Zakharia / zentrust partners GmbH (en)

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

Additional Advisory Data

Workarounds

CNA: * Prevent large package uploads by enforcing upload size limits at the reverse proxy or load balancer level.

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