# Improper Scope Enforcement in OAuth client_credentials Flow Allows Read-Only API Key to Escalate to Full Access

MITRE | NVD | CVE.ORG | Print: PDF

## Summary

| | |
|---|---|
| **CVE** | CVE-2026-21621 |
| **State** | PUBLISHED |
| **Assigner** | EEF |
| **Source Priority** | CVE Program / NVD first with legacy fallback |
| **Published** | 2026-03-05 20:16:12 UTC |
| **Updated** | 2026-04-06 17:17:07 UTC |
| **Description** | Incorrect Authorization vulnerability in hexpm hexpm/hexpm ('Elixir.HexpmWeb.API.OAuthController' module) allows Privile |

## Risk And Classification

**Primary CVSS:** v4.0 7 HIGH from 6b3ad84c-e1a6-4bf7-a703-f496b71e49db

CVSS:4.0/AV:N/AC:L/AT:P/PR:L/UI:N/VC:N/VI:H/VA:L/SC:N/SI:H/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-863 | CWE-863 CWE-863 Incorrect Authorization

| Version | Source | Type | Score | Severity | Vector |
|---|---|---|---|---|---|
| 4.0 | 6b3ad84c-e1a6-4bf7-a703-f496b71e49db | Secondary | 7 | HIGH | CVSS:4.0/AV:N/AC:L/AT:P/PR:L/UI:N/VC:N/VI:H/VA: |
| 4.0 | CNA | CVSS | 7 | HIGH | CVSS:4.0/AV:N/AC:L/AT:P/PR:L/UI:N/VC:N/VI:H/VA: |
| 3.1 | nvd@nist.gov | Primary | 5.3 | MEDIUM | CVSS:3.1/AV:N/AC:H/PR:L/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

Low

User Interaction

None

None

Confidentiality

None

Integrity

High

Availability

Low

Sub Conf.

None

Sub Integrity

High

Sub Availability

None

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

High

Privileges Required

Low

User Interaction

None

Scope

Unchanged

Confidentiality

None

Integrity

High

Availability

None

CVSS:3.1/AV:N/AC:H/PR:L/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 | Hexpm | All | All | All | All |

## Vendor Declared Affected Products

| Source | Vendor | Product | Version |
|---|---|---|---|
| CNA | Hexpm | Hexpm | affected 71829cb6f6559bcceb1ef4e43a2fb8cdd3af654b 71c127afebb7ed7cc637eb231b98feb802d62999 git |

| | | | |
|---|---|---|---|
| CNA | Hexpm | Hex.pm | affected 2025-08-18 2026-03-05 date |

## References

| Reference | Source | Link |
|---|---|---|
| osv.dev/vulnerability/EEF-CVE-2026-21621 | 6b3ad84c-e1a6-4bf7-a703-f496b71e49db | osv.dev |
| github.com/hexpm/hexpm/security/advisories/GHSA-739m-8727-j6w3 | 6b3ad84c-e1a6-4bf7-a703-f496b71e49db | github.com |
| github.com/hexpm/hexpm/commit/71c127afebb7ed7cc637eb231b98feb802d62999 | 6b3ad84c-e1a6-4bf7-a703-f496b71e49db | github.com |
| cna.erlef.org/cves/CVE-2026-21621.html | 6b3ad84c-e1a6-4bf7-a703-f496b71e49db | cna.erlef.or |
| CVE Program record | CVE.ORG | www.cve.or |
| NVD vulnerability detail | NVD | nvd.nist.gov |

## Vendor Comments And Credit

Discovery Credit

**CNA:** Michael Lubas / Paraxial.io (en)

**CNA:** Jonatan Männchen / EEF (en)

## Additional Advisory Data

Workarounds

**CNA:** * Revoke and reissue exposed API keys immediately if compromise is suspected. * Avoid relying on read-only API keys as a strict security boundary in high-risk environments. * Closely monitor audit logs for unexpected API key creation events. * Enforce strong 2FA hygiene and protect TOTP seeds carefully. There is no complete mitigation without upgrading, as the issue exists in server-side scope validation logic.

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