WPScan

WordPress Plugin Vulnerabilities

DeepL Pro API Translation < 1.7.5 - API Key Disclosure

Description

The plugin discloses sensitive information in its log files (which are publicly accessible), including DeepL API key.

Proof of Concept

```
https://example.com/wp-content/uploads/wpdeepl/2022-07-operation.log
https://example.com/wp-content/uploads/wpdeepl/2022-07-apiRequests.log
https://example.com/wp-content/uploads/wpdeepl/-request
```

Affects Plugins

wpdeepl

Fixed in version 1.7.5 - plugin closed ✓

References

CVE

CVE-2022-3691

Classification

WPScan

Type

SENSITIVE DATA DISCLOSURE

OWASP top 10

A3: Sensitive Data Exposure

CWE

CWE-200

Miscellaneous

Original Researcher

Raad Haddad of Cloudyrion GmbH

Submitter

Raad Haddad of Cloudyrion GmbH

Submitter twitter

raadfhaddad

Verified

Yes

WPVDB ID

4248a0af-1b7e-4e29-8129-3f40c1d0c560

Timeline

Publicly Published

2022-10-31 (about 25 days ago)

Added

2022-10-31 (about 25 days ago)

Last Updated

2022-10-31 (about 25 days ago)

Our Other Services

WPScan WordPress Security Plugin

For Developers

Status

API details

CLI scanner

Other

Privacy

Terms of service

Submission terms

Disclosure policy

In partnership with Jetpack

An endeavor

Work With Us