An Lárionad Náisiúnta Cibearshlándála
National Cyber Security Centre

NCSC #2412120165

NCSC Advisory

A Critical Vulnerability Exists in Peerigon Angular-Expressions (CVSS: 9.3)

12th, December 2024

STATUS: TLP:CLEAR

Recipients can spread this to the world, there is no limit on disclosure. Sources may use **TLP:CLEAR** when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules, TLP:CLEAR information may be shared without restriction.

For more information on the Traffic Light Protocol, see https://www.first.org/tlp/. Please treat this document in accordance with the TLP assigned.

An Roinn Comhshaoil, Aeráide agus Cumarsáide
Department of the Environment, Climate and Communications

Description

CVE ID: CVE-2024-54152

Published: 2024-12-10

Vendor: Peerigon

Product: Angular-Expressions

CVSS Score[1]: 9.3

Products affected

Product	Version
Angular-Expressions	<=1.4.2

Impact

Angular Expressions provides expressions for the Angular.JS web framework as a standalone module. Prior to version 1.4.3, an attacker can write a malicious expression that escapes the sandbox to execute arbitrary code on the system. With a more complex (undisclosed) payload, one can get full access to Arbitrary code execution on the system. The problem has been patched in version 1.4.3 of Angular Expressions. Two possible workarounds are available. One may either disable access to `__proto__` globally or make sure that one uses the function with just one argument.

Common Weakness Enumeration (CWE)[2]: CWE-94: Improper Control of Generation of Code ('Code Injection')

Known Exploited Vulnerability (KEV) catalog[3]: No

Used by Ransomware Operators: N/A

[1] https://www.first.org/cvss/v3.0/specification-document

[2] https://cwe.mitre.org

[3] https://www.cisa.gov/known-exploited-vulnerabilities-catalog

Recommedations

The NCSC strongly reccommends installing updates for vulnerable systems with the highest priority, after thorough testing. Affected organisations should review the latest release notes and install the relevant updates from Peerigon.

- https://nvd.nist.gov/vuln/detail/CVE-2024-54152
- https://www.cve.org/CVERecord?id=CVE-2024-54152
- https://github.com/peerigon/angular-expressions/security/advisories/GHSA-5462-4vcx-jh7j
- https://github.com/peerigon/angular-expressions/commit/97f7ad94006156eeb97fc942332578b6cfbf8eef