An Lárionad Náisiúnta Cibearshlándála
National Cyber Security Centre

NCSC #2412120143

NCSC Advisory

A Critical vulnerability exist in Apache Software Foundation, Arrow R package (CVSS: 9.8)

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-2024-52338

Published: 2024-11-28

Vendor: Apache Software Foundation

Product: Apache Arrow R package

CVSS3.0 Score[1]: 9.8

Products affected

Product	Version
Apache Arrow R package	4.0.0 <= 16.1.0

Impact

Deserialization of untrusted data in IPC and Parquet readers in the Apache Arrow R package versions 4.0.0 through 16.1.0 allows arbitrary code execution. An application is vulnerable if it reads Arrow IPC, Feather or Parquet data from untrusted sources (for example, user-supplied input files).

This vulnerability only affects the arrow R package, not other Apache Arrow implementations or bindings unless those bindings are specifically used via the R package (for example, an R application that embeds a Python interpreter and uses PyArrow to read files from untrusted sources is still vulnerable if the arrow R package is an affected version).

Common Weakness Enumeration (CWE)[2]: CWE-502 Deserialization of Untrusted Data

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 Apache Software Foundation.

- https://nvd.nist.gov/vuln/detail/CVE-2024-52338
- https://www.cve.org/CVERecord?id=CVE-2024-52338
- https://github.com/apache/arrow/commit/801de2fbcf5bcbce0c019ed4b35ff3fc863b141b
- https://lists.apache.org/thread/0rcbvj1gdp15lvm23zm601tjpq0k25vt