National Cyber Security Centre

2406270135-NCSC

Department of the Environment, Climate & Communications

NCSC Alert

Critical Vulnerability exists in Progress MOVEit Gateway (CVE-2024-5805)

Thursday 27th June, 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.

Description

Published: 2024-06-27T09:30:00
Vendor: Progress
Product: MOVEit Gateway
CVE ID: CVE-2024-5805
CVSS3.0 Score[1]**:** 9.1
EPSS[2]**:** 0.090800000
(For up to date EPSS score, click here: https://api.first.org/data/v1/epss?cve=CVE-2024-5805
Summary: Improper Authentication vulnerability in Progress MOVEit Gateway (SFTP modules) allows Authentication Bypass. This issue affects MOVEit Gateway 2024.0.0.

Products Affected

- Progress MOVEit Gateway: 2024.0.0

Impact

Common Weakness Enumeration (CWE)[3]**:** CWE-287 Improper Authentication

Present in CISA Known Exploited Vulnerability(KEV)[4] **catalog:** NO

Used by Ransomware Operators: Not Known

Recommendations

The NCSC strongly advises affected organisations to review the latest release notes and install the relevant updates from Progress. Upgrading to a patched release, using the full installer, is the only way to remediate this issue. Fixed version is 2024.0.1.

Additional recommendations and mitigation's for CVE-2024-5805 can be found in the respective links below:

- https://www.progress.com/moveit
- https://community.progress.com/s/article/MOVEit-Gateway-Critical-Security-Alert-Bulletin-June-2024-CVE-2024-5805

[1] https://www.first.org/cvss/v3.0/specification-document
[2] https://www.first.org/epss/articles/prob_percentile_bins
[3] https://cwe.mitre.org/
[4] https://www.cisa.gov/known-exploited-vulnerabilities-catalog

DISCLAIMER: This document is provided “as is” without warranty of any kind, expressed or implied, including, but not limited to, the implied warranty of fitness for a particular purpose. NCSC-IE does not endorse any commercial product or service, referenced in this document or otherwise.

National Cyber Security Centre
Tom Johnson House,
Beggars Bush,
Dublin, D04 A068,
Ireland
Tel: +353 (0)1 6782333
Mail: certreport@ncsc.gov.ie
Web: ncsc.gov.ie
Twitter: ncsc_gov_ie
LinkedIn: ncsc-ie

An Lárionad Náisiúnta
Cibearshlándála
National Cyber Security Centre