National Cyber Security Centre

2306010140-NCSC

A part of the **Department of the Environment, Climate & Communications**

NCSC Alert

Critical Vulnerability in MOVEit Transfer

Friday 2nd June, 2023

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

Progress have released details of a critical vulnerability in MOVEit Transfer which, if exploited, could lead to privilege escalation and unauthorised access.

As of yet there is no CVE for this vulnerability. Progress have made details of the vulnerability available from their website: https://community.progress.com/s/article/MOVEit-Transfer-Critical-Vulnerability-31May2023

Products Affected

- MOVEit Transfer 2023.0.0
- MOVEit Transfer 2022.1.x
- MOVEit Transfer 2022.0.x
- MOVEit Transfer 2021.1.x
- MOVEit Transfer 2021.0.x

Impact

Exploitation of this vulnerability could allow an attacker to escalate privileges and gain unauthorised access to the target environment.

Recommendations

The NCSC strongly advises users of affected versions of MOVEit Transfer to apply patches if available and to take immediate mitigation measures where patches are not available.

Progress are issuing patches for affected versions of the software and these will be downloadable from Progress as they are made available: https://community.progress.com/s/article/MOVEit-Transfer-Critical-Vulnerability-31May2023

Where patches are not yet available, Progress has included mitigation measures that affected customers can take. These are also available here: https://community.progress.com/s/article/MOVEit-Transfer-Critical-Vulnerability-31May2023

Progress also advises users of vulnerable versions of MOVEit Transfer to check their infrastructure for any signs of compromise over at least the past 30 days.

IOCs that can be checked for are also available from the Progress website using the above link.

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
29-31 Adelaide Road,
Dublin, D02 X285,
Ireland
Tel: +353 (0)1 6782333
Mail: certreport@decc.gov.ie
Web: ncsc.gov.ie
Twitter: ncsc_gov_ie
LinkedIn: ncsc-ie