National Cyber Security Centre

2306160102-NCSC

Department of the Environment, Climate & Communications

NCSC Alert

Critical Vulnerability in MOVEit Transfer - (CVE-2023-35708)

Friday 16th 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 discovered in MOVEit Transfer which, if exploited, could lead to privilege escalation and unauthorised access.

The details were published in an advisory on the vulnerability CVE-2023-35708 that includes information on recommended remediation, mitigation and workaround steps which MOVEit Transfer customers can take to address this latest vulnerability.

The advisory is available here:

https://community.progress.com/s/article/MOVEit-Transfer-Critical-Vulnerability-15June2023

Recently reported vulnerabilities in Moveit have been successfully exploited by malicious actors. The NCSC believes with high confidence that malicious actors will attempt to leverage this latest vulnerability in their campaigns.

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
- MOVEit Transfer 2020.1.x
- MOVEit Transfer 2020.0.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 all affected organisations of the latest MOVEit Transfer vulnerability to read the latest advisory from Progress, apply patches if available, and to immediately implement the mitigation measures where patches are not available.

Affected organisations should monitor the advisory for updates here:

https://community.progress.com/s/article/MOVEit-Transfer-Critical-Vulnerability-15June2023

Updated fixed version links, consolidated information can also be found on the the Progress Security Centre page.

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