National Cyber Security Centre

2306100106-NCSC

Department of the Environment, Climate & Communications

NCSC Alert

Critical SQL Injection Vulnerabilities in MOVEit Transfer

Saturday 10th 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 Software Corporation have released details of multiple SQL injection vulnerabilities in the MOVEit Transfer web application that could allow an un-authenticated attacker to gain unauthorised access to the MOVEit Transfer database.

All versions of MOVEit Transfer are affected by this vulnerability.

Patches for this vulnerability are available for supported versions. Progress have made details of the vulnerability available from their website: https://community.progress.com/s/article/MOVEit-Transfer-Critical-Vulnerability-CVE-Pending-Reserve-Status-June-9-2023

Products Affected

MOVEit transfer versions released before:

- 2021.0.7 (13.0.7)
- 2021.1.5 (13.1.5)
- 2022.0.5 (14.0.5)
- 2022.1.6 (14.1.6)
- 2023.0.2 (15.0.2)

Impact

Exploitation of this vulnerability could allow an attacker to submit a crafted payload to a MOVEit Transfer application endpoint which could result in modification and disclosure of MOVEit database content.

Recommendations

The NCSC strongly advises users of affected versions to apply patches where available or update to a supported version.

Progress have made patches for affected versions of the software available from their website: https://community.progress.com/s/article/MOVEit-Transfer-Critical-Vulnerability-CVE-Pending-Reserve-Status-June-9-2023

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