National Cyber Security Centre

2307060121-NCSC

Department of the Environment, Climate & Communications

NCSC Alert

Critical SQL Injection Vulnerability in MOVEit Transfer

Thursday 6th July, 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 a new critical SQL injection vulnerability in the MOVEit Transfer web application that could allow an unauthenticated attacker to gain unauthorised access to the MOVEit Transfer database. This new critical vulnerability is being tracked as CVE-2023-36934.

Before applying the new remediation steps, affected customers must ensure that they have already taken previously recommended remediation steps to address CVE-2023-34362 that was disclosed in May 2023.

Progress have also released details of two high severity vulnerabilities, tracked as CVE-2023-36932 and CVE-2023-36933 that also affect MOVEit Transfer.

Details of these new vulnerabilities and the remediation steps that organisations need to take to address them can be found here:

https://community.progress.com/s/article/MOVEit-Transfer-2020-1-Service-Pack-July-2023

Products Affected

CVE-2023-36934, CVE-2023-36932

MOVEit Transfer versions released before:

- 2023.0.4 (15.0.4)
- 2022.1.8 (14.1.8)
- 2022.0.7 (14.0.7)
- 2021.1.7 (13.1.7)
- 2021.0.9 (13.0.9)
- 2020.1.11 (12.1.11)

CVE-2023-36933

MOVEit Transfer versions released before:

- 2021.0.9 (13.0.9)
- 2021.1.7 (13.1.7)
- 2022.0.7 (14.0.7)
- 2022.1.8 (14.1.8)
- 2023.0.4 (15.0.4)

Impact

Exploitation of CVE-2023-36934 and CVE-2023-36932 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.

CVE-2023-36933 is a behavioral workflow vulnerability that could allow an attacker to invoke a method that results in an unhandled exception. Triggering this workflow would have an impact on the availability of the MOVEit Transfer application.

Recommendations

The NCSC strongly advises users of affected versions of MOVEit Transfer to follow the remediation steps outlined by Progress. Details of these steps are available from the Progress website here:

https://community.progress.com/s/article/MOVEit-Transfer-2020-1-Service-Pack-July-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