



To: Institutions of Higher Education
From: Chad May, Director of Research and Analysis
Justin Schaffer, Assistant Director of Research
Thomas Zimmerman, Research and Data Associate
Date: July 12, 2023
Subject: MOVEit Security Threat

Multiple public and private sector organizations were recently impacted by a cyberattack launched by the Clop ransomware group targeting vulnerable MOVEit servers. MOVEit is a widely-used file transfer software product developed by the Progress Software Company to securely transfer files between organizations and individuals. The New Jersey Office of Information Technology (NJ OIT), which supports and provides the MOVEit platform to state agencies, has shared the following message:

“As a number of New Jersey executive branch agencies also use the instance of MOVEit provided by the Office of Information Technology (OIT) to securely transfer files with their business partners, we are writing to let you know that at this time we have found no evidence of it being impacted. Since the first reports of a vulnerability were announced on May 31st, NJ OIT has been working with Progress Software to ensure all security patches and updates were applied.”

For more information on the attacks targeting the MOVEit vulnerability, please see the NJCCIC advisory posted at: <https://www.cyber.nj.gov/alerts-advisories/threat-actors-aggressively-exploiting-moveit-vulnerability>.

The Office of the Secretary of Higher Education (OSHE) has reviewed its MOVEit folders and accounts and found no evidence of a data breach or compromised files. However, with this recent vulnerability in MOVEit, we reviewed our procedures and have decided to institute a new process to increase security and minimize any potential data breach. Out of an abundance of caution, we have removed processed/submitted files from all institutional folders within the MOVEit application, and effective immediately, OSHE research team members will delete files after the files are processed into our secure SQL database. The SQL database is not accessible via the internet as it is located within the intranet of the Garden State Network. We expect that these measures will mitigate the risk of compromised data within the MOVEit platform.

OSHE continues to review our security policies and processes to align with best practices to ensure that any Personally Identifiable Information (PII) data is protected. We will also continue to monitor this evolving situation and work with our technology supports in the Division of Revenue and Enterprise Services and NJ OIT to ensure our data resources are secure, stable, and protected from misuse.

Thank you for your continued partnership and all that you do for your students and institutions.