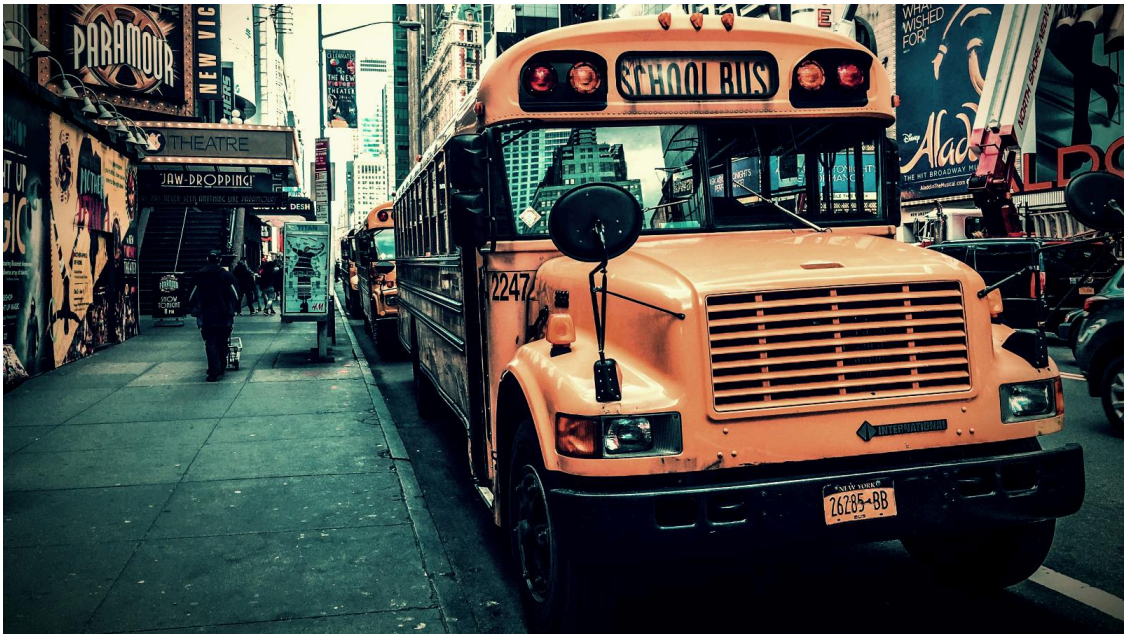
# Hackers steal data of 45,000 New York City students in MOVEit breach

By Sergiu Gatlan

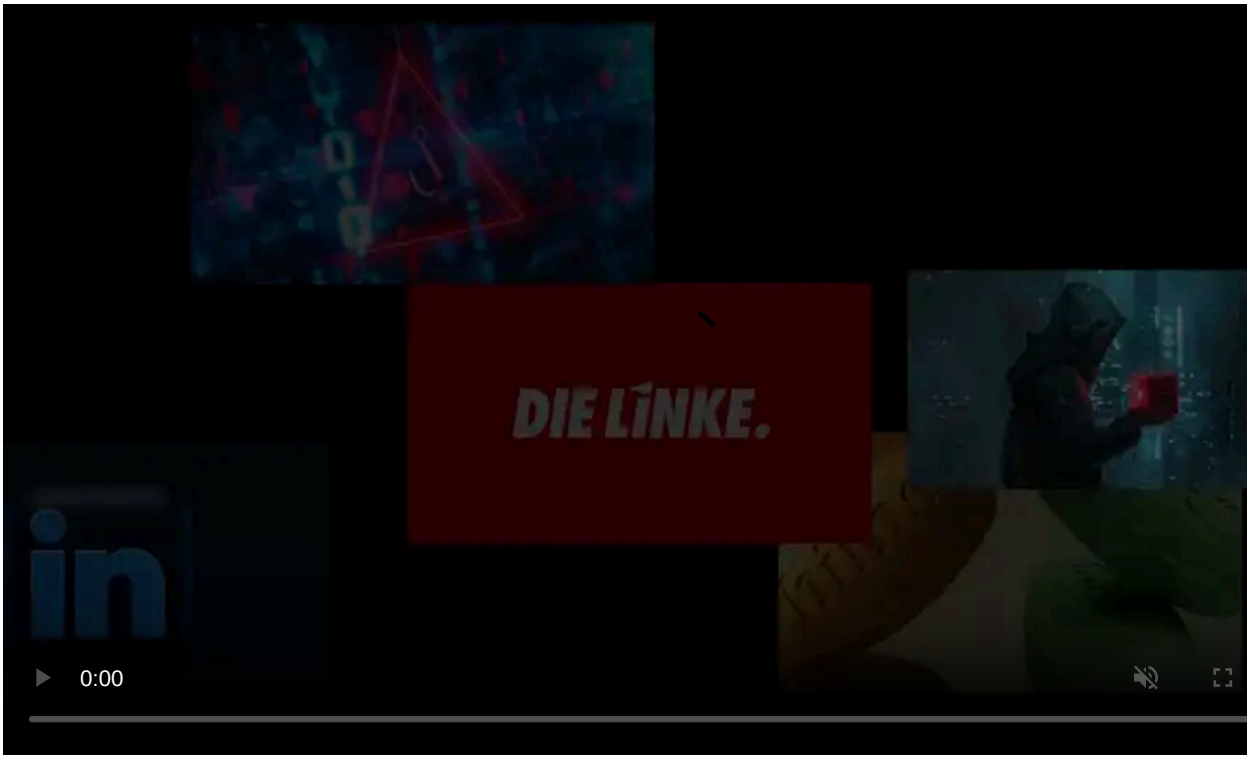
Published: 2023-06-26 · Archived: 2026-04-05 14:10:15 UTC




The New York City Department of Education (NYC DOE) says hackers stole documents containing the sensitive personal information of up to 45,000 students from its MOVEit Transfer server.

The managed file transfer (MFT) software was used by NYC DOE to securely transfer data and documents internally and externally to various vendors, including special education service providers.

NYC DOE patched the servers as soon as the developer disclosed info on the exploited vulnerability (CVE-2023-34362); however, the attackers were already abusing the bug in large-scale attacks as a zero-day before security updates were available.

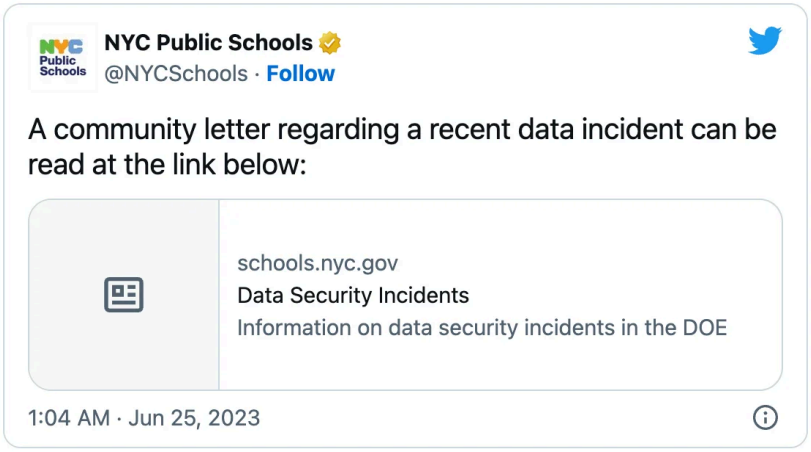

DIE LINKE.
0:00

The affected server was taken offline after the breach was discovered, and NYC DOE is working with NYC Cyber Command to address the incident.

"We also conducted an internal investigation, which revealed that certain DOE files were affected. Review of the impacted files is ongoing, but preliminary results indicate that approximately 45,000 students, in addition to DOE staff and related service providers, were affected," NYC DOE COO Emma Vadehra said in a statement issued over the weekend.

"Roughly 19,000 documents were accessed without authorization. The types of data impacted include Social Security Numbers and employee ID numbers (not necessarily for all impacted individuals; for example, approximately 9,000 Social Security Numbers were included).

"The FBI is investigating the broader breach that has impacted hundreds of entities; we are currently cooperating with both the NYPD and FBI as they investigate."




The Clop ransomware gang has claimed responsibility for the CVE-2023-34362 MOVEit Transfer attacks on June 5 in a statement shared with BleepingComputer, with the cybercrime gang saying it breached the MOVEit servers of "hundreds of companies."

Kroll also uncovered evidence that Clop had been actively testing exploits for the now-patched MOVEit zero-day since 2021 and researching methods to extract data from compromised servers since at least April 2022.

Clop's involvement in this extensive data theft campaign is part of a broader pattern of targeting MFT platforms.

Previous instances include the breach of Accellion FTA servers in December 2020, SolarWinds Serv-U servers in 2021, and the widespread exploitation of GoAnywhere MFT servers earlier this year in January.

## Clop already extorting impacted organizations

The Clop gang began extorting organizations affected by the MOVEit data theft attacks almost two weeks ago, on June 15, by publicly listing their names on Clop's dark web data leak site.

Shell, the University of Georgia (UGA) and University System of Georgia (USG), Heidelberger Druck, UnitedHealthcare Student Resources (UHSR), and Landal Greenparks are just some of the organizations that have confirmed to BleepingComputer that they were impacted.

Other victims that already disclosed breaches related to the MOVEit Transfer attacks include the U.S. state of Missouri, the U.S. state of Illinois, Zellis (along with its customers BBC, Boots, Aer Lingus, and Ireland's HSE), Ofcam, the government of Nova Scotia, the American Board of Internal Medicine, and Extreme Networks.

The U.S. Cybersecurity and Infrastructure Security Agency (CISA) disclosed that several U.S. federal agencies have also been compromised, as reported by CNN. Federal News Network said the attacks also impacted two U.S. Department of

Energy (DOE) entities.

Progress warned MOVEit Transfer customers last week to restrict HTTP access to their servers after info on a new SQL injection (SQLi) security flaw (CVE-2023-35708) was published online.

That warning came after another advisory disclosed several other critical SQL injection vulnerabilities collectively tracked as CVE-2023-35036.



---

Source: https://www.bleepingcomputer.com/news/security/hackers-steal-data-of-45-000-new-york-city-students-in-moveit-breach/