Colorado warns 4 million of data stolen in IBM MOVEit breach

By Bill Toulas

Published: 2023-08-14 · Archived: 2026-04-05 17:03:56 UTC

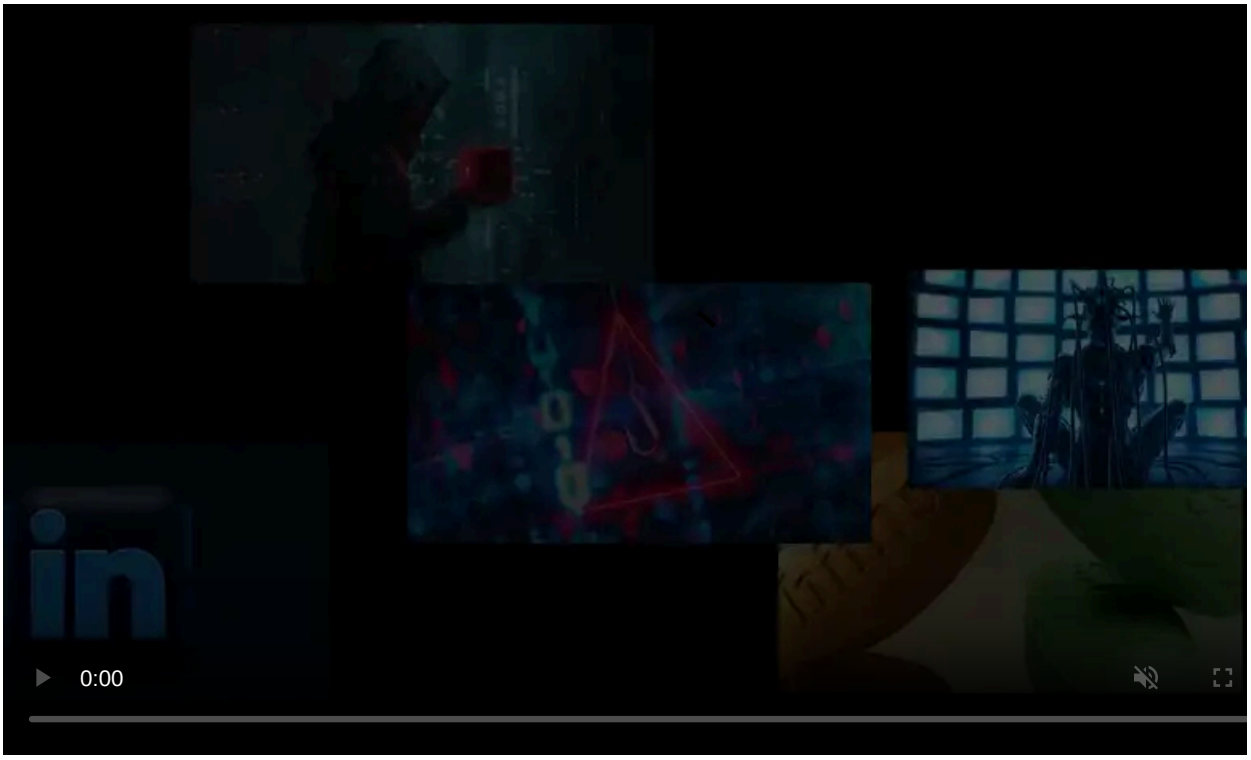
Image: Midjourney

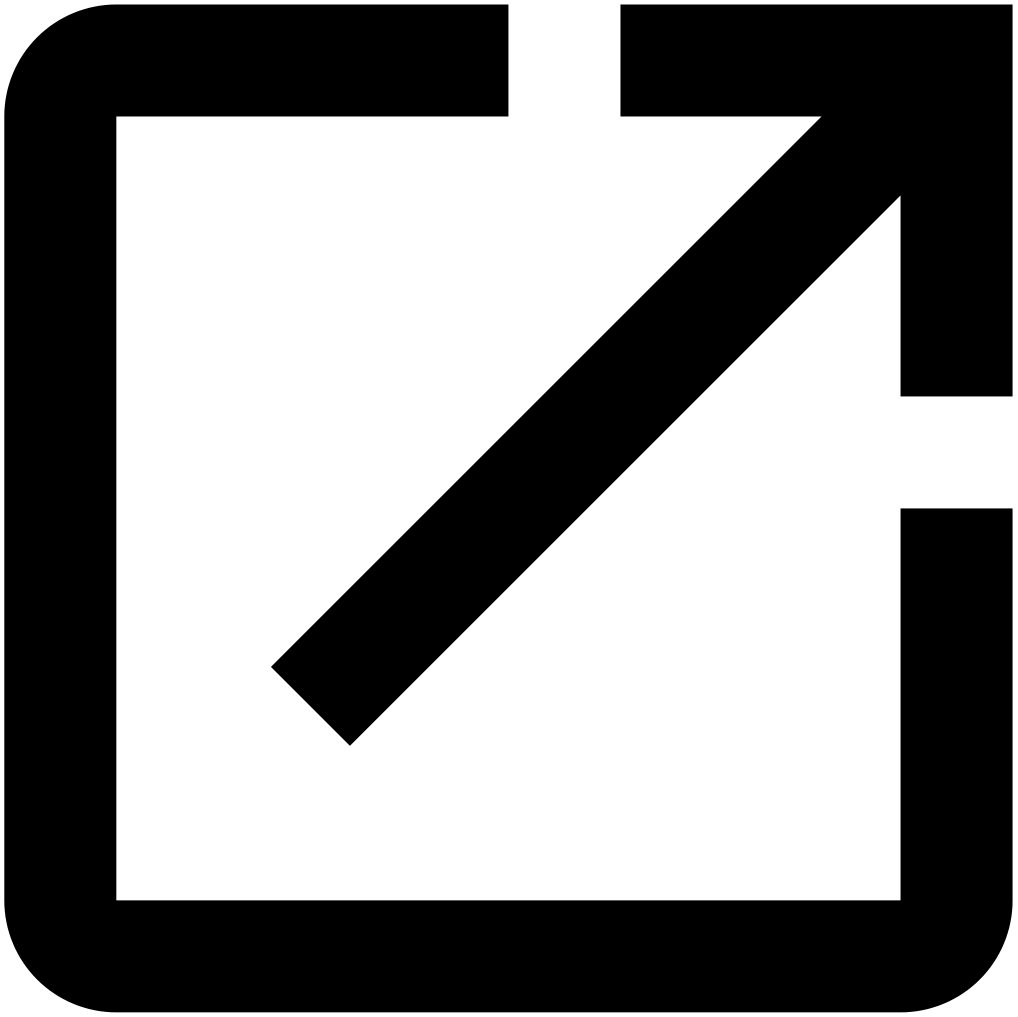
The Colorado Department of Health Care Policy & Financing (HCPF) is alerting more than four million individuals of a data breach that impacted their personal and health information.

Colorado HCPF is a state government agency that manages the Health First Colorado (Medicaid) and Child Health Plan Plus programs, and provides support for low-income families, the elderly, and citizens with disabilities.

The data breach was possible after Clop ransomware exploited the MOVEit Transfer zero-day (CVE-2023-34362) in a hacking campaign that impacted hundreds of organizations worldwide.

HCPF clarifies that while their systems weren't directly compromised, the data exposure occurred through IBM, their contractor, which utilized the MOVEit software.


0:00



"After IBM notified HCPF that it was impacted by the MOVEit incident, HCPF launched an investigation right away to understand whether the incident impacted its own systems, and to determine whether Health First Colorado or CHP+ members' protected health information was accessed by an unauthorized party," reads the notice.

"While HCPF confirmed that no other HCPF systems or databases were impacted, on June 13, 2023, the investigation identified that certain HCPF files on the MOVEit application used by IBM were accessed by the unauthorized actor on or about May 28, 2023" - Colorado Department of Health Care Policy & Financing

The investigation revealed that the threat actors managed to access and likely exfiltrated files that contained certain Health First Colorado and CHP+ members' information, including:

- Full names
- Social Security Numbers (SSNs)
- Medicaid ID number
- Medicare ID number
- Date of Birth
- Home address
- Contact information
- Income information
- Demographic data
- Clinical data (diagnosis, lab results, treatment, medication)
- Health insurance information

The above data can be utilized to launch effective phishing or social engineering attacks, and can help with identity or bank fraud activity.

In total, data of 4,091,794 people has been exposed. For all individuals that received the data breach notification, HPCF provides two years of credit monitoring services via Experian to help counteract fraud attempts.

This disclosure comes only a week after another large state organization in Colorado, the Department of Higher Education (CDHE), disclosed that a massive data breach caused by a ransomware attack had impacted a large number of students and teachers.

The CDHE said the threat actors leveraged the stolen data to perform double extortion and encrypted network computers; however, it did not clarify how the hackers obtained access to the network.

In July 2023, the Colorado State University disclosed a data breach resulting from its use of the vulnerable MOVEit Transfer software, impacting tens of thousands of students and academic staff.

Source: https://www.bleepingcomputer.com/news/security/colorado-warns-4-million-of-data-stolen-in-ibm-moveit-breach/