Radisson Hotels, major insurance firms become latest MOVEit victims to disclose breaches

By Jonathan Greig

Published: 2023-07-11 · Archived: 2026-04-05 19:48:43 UTC

The number of organizations affected by a recently exploited vulnerability in a popular file transfer tool surpassed 250 on Monday as major corporations like Radisson Hotels and two major insurance companies confirmed that their data was accessed by hackers exploiting a vulnerability in the software.

Choice Hotels – the company that purchased global hotel chain Radisson Hotels last year – confirmed to Recorded Future News that guest records were involved in the data breach.

“Unfortunately, we have confirmed that MOVEit software, from our vendor, had a vulnerability that was exploited by bad actors, resulting in data breaches affecting many of their customers including Radisson Hotels Americas,” a spokesperson said.

“While our investigation is still ongoing, we have identified a limited number of guest records that were accessed by these bad actors. In an abundance of caution, we are in the process of notifying the affected guests.”

The hotel chain did not say how many guests have been identified so far. It operates more than 1,700 properties in 120 countries.

The Choice Hotels spokesperson said they are dedicating “significant resources” to monitoring the cyber landscape in light of the incident and are coordinating with regulators about the incident.

American National Insurance Company, one of the biggest in the U.S., also confirmed that Progress Software is one of its vendors and that an investigation has been started into what data may have been accessed by the Clop ransomware group – which has been the primary gang of hackers exploiting the MOVEit vulnerability and extorting victims.

“On July 7, 2023, we became aware that American National’s name has been listed on a website outside the confines of the public Internet. We are working as thoroughly and expeditiously as possible to validate and review any data that may have been impacted to determine if any individuals’ or organizations’ information was involved,” the company told Recorded Future News.

“If we determine that an individual’s sensitive data was involved, we will provide notification to the individual along with resources to help protect their information.”

Sun Life, one of Canada’s largest insurance providers, said on Saturday that data belonging to some of its U.S. customers was compromised after one of its vendors — Pension Benefit Information (PBI) — had a server “accessed by an unauthorized third party as part of the global attack.”

There has been a steady stream of announcements from dozens of the biggest schools, banks and companies in the world confirming their exposure to the MOVEit issue – the third file transfer vulnerability exploited by the Clop ransomware group in the last two years.

Over the last week, TD Ameritrade, law firms Kirkland & Ellis, Proskauer Rose and K&L Gates have come forward to confirm that they were affected.

Emsisoft ransomware expert Brett Callow, who has kept a running tally of victims, said the number has now reached 254, with the information of at least 17.7 million people exposed.

Many of the victims are coming from governments or universities – most of which are involved in the incident due to their connection to PBI Research Services, the National Student Clearinghouse (NSC) or the Teachers Insurance and Annuity Association of America (TIAA).

Officials from the University of Illinois told Recorded Future News that they are communicating with students, faculty and staff about the incident after discovering information from their school was involved.

“We don’t know how many students’ data was compromised at the National Student Clearinghouse. NSC notified the numerous higher education institutions that use NSC in early June that it was impacted by the MOVEit breach and that it was investigating,” the school said.

“On June 26 the U of I System was notified by NSC that some of our students’ data was possibly part of that breach, but NSC did not provide details on which students might be affected or what data was breached. We notified all students on July 3 that the personal data of some of our students was accessed, but we do not know which students. NSC has said it is continuing to investigate and will send notices directly to anyone whose data was accessed.”

The University of Louisville also explained to Recorded Future News that a small number of its UofL Health medical practices used MOVEit to transfer files to third party vendors.

The school is now working with forensic security consultants to determine what information was accessed by the hackers. The University of Utah released a similar message to its students last Friday.

The federal government warned on Friday that three new vulnerabilities have been discovered in the MOVEit file transfer software – the fourth, fifth and sixth problems found in the software since the fiasco began at the end of May.

No previous article

No new articles

Jonathan Greig

is a Breaking News Reporter at Recorded Future News. Jonathan has worked across the globe as a journalist since 2014. Before moving back to New York City, he worked for news outlets in South Africa, Jordan and Cambodia. He previously covered cybersecurity at ZDNet and TechRepublic.
