Medical files of 8M-plus people fall into hands of Clop via MOVEit mega-bug

By Jessica Lyons

Published: 2023-07-27 · Archived: 2026-04-05 23:40:28 UTC

Accounting giant Deloitte, pizza and birthday party chain Chuck E. Cheese, government contractor Maximus, and the Hallmark Channel are among the latest victims that the Russian ransomware crew Clop claims to have compromised via the MOVEit vulnerability.

Deloitte confirmed an intrusion but declined to answer *The Register*'s questions about how much and what type of data was accessed in the incident. The biz now joins PwC and Ernst and Young – all three big accounting firms – among the hundreds of organizations compromised by Clop via a security hole in vulnerable deployments of the file-transfer tool MOVEit.

"Immediately upon becoming aware of this zero-day vulnerability, Deloitte applied the vendor's security updates and performed mitigating actions in accordance with the vendor's guidance," a Deloitte Global spokesperson explained.

"Our analysis determined that our global network use of the vulnerable MOVEit Transfer software is limited. Having conducted our analysis, we have seen no evidence of impact to client data."

8m-11m patients' healthcare data accessed

Meanwhile, in a US Securities and Exchange Commission filing on Wednesday, Maximus, which does the admin for US government programs like Medicaid and Medicare, disclosed that the personal information of as many as 11 million individuals' was "accessed" by Clop.

"Based on the review of impacted files to date, the company believes those files contain personal information, including social security numbers, protected health information and/or other personal information, of at least 8 to 11 million individuals to whom the company anticipates providing notice of the incident," Maximus's 8-K filing to the SEC stated.

In a statement provided to *The Register*, a spokesperson said Maximus responded "quickly" to mitigate the MOVEit vulnerability, and is continuing investigating the incident. The company will record an expense of up to $15 million to cover the cost of cleaning up.

"To be clear, we have not identified any impact from the MOVEit vulnerability on other parts of our corporate network and remain confident in the integrity of the network," the Maximus spokesperson said.

"We have been working with the subset of our customers who were using MOVEit as part of their workflows and continue to provide updates and support to them as our investigation proceeds. We continue to closely monitor our systems for any unusual activity."

Neither Chuck E. Cheese nor the Hallmark Channel immediately responded to *The Register*'s inquiries after Clop listed both on its leak site.

514 compromised organizations and counting

The new additions to the victims' list bring the headcount to 514 organizations and more than 36 million individuals, according to Emsisoft threat researchers.

The team has been scouring state breach notifications, SEC filings, other public disclosures, and Clop's website to update their list of affected orgs and people at least every 24 hours since the fiasco started.

"How many organizations and individuals have been impacted by this incident remains to be seen," Emsisoft Threat Analyst Brett Callow told *The Register*. "Given the complexity of the upstream/downstream, it's highly likely that some of the organizations which have been impacted don't yet realize they've been impacted."

"It will likely take months if not years for the full impact and costs to become clear as the legal proceedings will not play out quickly," he added.

Progress Software, which makes the MOVEit file transfer suite, is facing multiple class-action lawsuits stemming from the vulnerability. So are some of Progress Software's customers, including Johns Hopkins University and Johns Hopkins Health System.

The latter two lawsuits allege that the university and health-care provider failed to properly secure patients' protected health information that was accessed in the breach.

- MOVEit body count closes in on 400 orgs, 20M+ individuals
- US government hit by Russia's Clop in MOVEit mass attack
- Crooks pwned your servers? You've got four days to tell us, SEC tells public companies
- Ivanti plugs critical bug – but not before it was used against Norwegian government

Also interesting are the organizations that were listed, and then removed, from Clop's leak site. This potentially indicates the ransomware gang was bluffing, or the companies decided to negotiate with the extortionists and pay up, or the crew gave the businesses a break.

According to Callow, recently delisted firms include the aforementioned Maximus, TD Ameritrade, Global University Systems (GUS) Canada, Greenshield, National Student Clearinghouse, and security biz Telos Corporation.

Progress Software initially disclosed the first MOVEit bug, a SQL injection vulnerability tracked as CVE-2023-34362, on May 31 and patched it the next day.

Since then, bug hunters have spotted other vulnerabilities and reported them to Progress, bringing the total number to six as of July 5. All of these have since been fixed, and Progress has said none of the vulnerabilities discovered after the first bug on May 31 have been exploited. ®

Source: https://www.theregister.com/2023/07/27/maximus_deloitte_moveit_hack/