COSMOS
Navigate the Compliance Universe

Report on Patient Privacy Volume 23, Number 7. July 13, 2023 Patch MOVEit Vulnerability Immediately to Avoid a Breach, Cybersecurity Officials Warn

By Jane Anderson

Federal cybersecurity officials are warning health care organizations to take immediate steps to secure their systems against a critical vulnerability in the commonly used MOVEit Transfer software, as multiple entities—including federal and state government agencies, large hospital systems and insurers—report related breaches.

The software, from Progress Software—formerly IPSwitch—is used by many organizations in the health care sector, including hospitals, clinics and health insurers, according to the federal Health Sector Cybersecurity Coordination Center (HC3). "This zero-day vulnerability could allow an attacker to escalate privileges and gain unauthorized access to the healthcare environment, potentially compromising any number of victims," HC3 said.[1]

The likely Russian-affiliated ransomware group known as CLoP is reportedly behind at least some of the attacks, including the attacks on federal agencies.

"This is probably the most well-coordinated, most well-planned campaign I've seen in a long time," Fred Langston, founder and chief product officer at Critical Insight, said during a webinar on the vulnerability's impact.[2]