New MOVEit Transfer Vulnerability Under Active Exploitation

Progress Software MOVEit Transfer, a popular file transfer software, is under attack again. A critical security flaw (CVE-2024-5806) has been discovered that allows attackers to bypass authentication and gain access to systems. This vulnerability affects multiple versions of MOVEit Transfer and Gateway.

This flaw is rated critical (CVSS score: 9.1) because it can be easily exploited and has serious consequences. Attackers are already trying to take advantage of this vulnerability, so it's important to act immediately. Last year, another flaw (CVE-2023-34362) was exploited impacting 2,500 organizations and an estimated 66 million individuals. Threat actors utilized the flaw in a series of ransomware attacks with an estimated cost in the billions of dollars. Because of this history, it's important to prioritize patching this latest vulnerability to avoid a similar situation

Here's what you need to do: Update MOVEit Transfer and Gateway to the latest versions as soon as possible. Additionally, you should block public access to MOVEit Transfer servers and restrict outbound traffic to only trusted destinations.

CRITICALSTART® offers a pioneering solution to modern organizational challenges in aligning cyber protection with risk appetite through its Cyber Operations Risk & Response™ platform, award-winning Managed Detection and Response (MDR) services, and a dedicated human-led risk and security team. By providing continuous monitoring, mitigation, maturity assessments, and comprehensive threat intelligence research, they enable businesses to proactively protect critical assets with measurable ROI. Critical Start's comprehensive approach allows organizations to achieve the highest level of cyber risk reduction for every dollar invested, aligning with their desired levels of risk tolerance.