PUBLICATION

MOVEit Transfer Zero-Day Vulnerability: What Companies Need to Know

Authors: Alisa L. Chestler, Layna S. Cook Rush, Matthew George White
June 07, 2023

On May 31, 2023, renowned managed file transfer solution provider Ipswitch, Inc. revealed a zero-day vulnerability in its flagship solution, MOVEit Transfer, that can enable mass data theft from thousands of organizations. File transfer services play crucial roles in securing business and government operations, but companies must be aware of the inherent risks and adopt mitigations to safeguard against those risks.

Cybersecurity risks rise exponentially when an application or a service that an organization relies on develops a previously unknown security vulnerability. Such vulnerabilities, known as zero-day vulnerabilities because mitigations have not yet been developed to respond to them, can lead to unauthorized system access, data breaches, and financial and reputational harm. Malicious cyber actors – in this case, ransomware gangs seeking financial gain – are quick to exploit these vulnerabilities, targeting corporate networks and data stores. The recently discovered zero-day in MOVEit Transfer provides such a vulnerability for threat actors to exploit.

MOVEit Transfer is used to mitigate risk by securing file exchanges between businesses, partners, and customers, through protocols such as SFTP, SCP, and HTTP-based uploads. The solution is used widely by organizations in the healthcare, financial, and defense sectors to securely transfer protected health information (PHI), payment card information (PCI), and personally identifiable information (PII). As a result, a breach in MOVEit Transfer can have a far-reaching impact on compliance with the Health Insurance Portability and Accountability Act (HIPAA), Payment Card Information Data Security Standard (PCI-DSS), Federal Acquisition Regulation (FAR), and individual state breach notification requirements, among others.

The MOVEit Transfer Vulnerability

Threat researchers have identified a structured query language (SQL) injection vulnerability in the MOVEit Transfer web application that permits unauthenticated access to MOVEit Transfer's database. This SQL injection vulnerability allows for further compromise, such as arbitrary code execution, which can be used to deploy ransomware, escalate privileges, or enable other malicious activity in MOVEit Transfer environments.

Threat actors can exploit this vulnerability to gain access to an extensive database of files and potentially sensitive data. The vulnerability allows for unauthorized data access and control, including access to Azure Storage Blob credentials, providing the attackers with the means to steal data directly from a victim's Azure Blob Storage containers. This situation is particularly alarming because, with a copy of the database, threat actors can continuously attempt to access even encrypted data, posing a severe threat to organizational security.

With more than 1,700 software companies and 3.5 million users worldwide relying on its services, MOVEit Transfer is a key player in the managed file transfer ecosystem. The software's vulnerability has already been exploited by several unidentified threat actor groups worldwide. Initial reports suggest unauthorized access and mass downloading of data, with large downloads or unexpected backups as key indicators of a data breach in progress.

Securing Data

In response to this threat, all organizations using MOVEit Transfer should take immediate action.

1. **Modify Traffic to the MOVEit Transfer Environment**: Affected companies should temporarily disable all HTTP and HTTPS traffic to the MOVEit Transfer environment. This involves changing firewall rules to deny this type of traffic on ports 80 and 443.
2. **Evaluate System**: Examine affected systems and delete any unauthorized files, user accounts, and specific instances of script files. Thoroughly review logs for any unexpected or large file downloads. If using Azure, monitor logs for any unauthorized access and change any potentially compromised keys. Finally, reset all credentials for affected systems and the MOVEit Service Account.
3. **Confirm Settings**: Review and ensure usernames, passwords, and applicable configurations are not the vendor's default. Shodan, a search engine for publicly exposed devices and databases, showed that more than 2,500 MOVEit Transfer servers were discoverable on the internet.
4. **Patch**: Apply patches to all supported versions of MOVEit Transfer. These patches are now available and should be applied according to the version in use.
5. **Continuous Monitoring**: Regularly monitor your network, endpoints, and logs for any indicators of compromise.
6. **Security Measures**: Employ additional security measures, such as updating firewall rules to only allow connections from trusted IP addresses, removing any unauthorized accounts, restricting remote access, and enabling multi-factor authentication (MFA).

Even if your organization does not use MOVEit Transfer directly, the ripple effects of this breach may still pose a risk. Companies should conduct a thorough audit of their data and file-sharing practices, including all individual user accounts, administrative accounts, network devices, cloud-based services, and shared files. Any obsolete accounts or services should be promptly suspended.

In addition to these mitigations, affected companies should immediately contact outside counsel to understand how this vulnerability could affect their regulatory and statutory compliance and legal requirements related to reporting and notification. Because these services are attractive targets for threat actors, breaches to secure data transfers solutions are likely to continue. To mitigate this risk, companies in every industry should develop and implement cybersecurity incident response plans, conduct annual tabletop exercises, and perform regular security audits.

The potential severity of this incident underscores the importance of ensuring your vendor agreements are regularly reviewed and contain the appropriate provisions to protect your organization. In these types of agreements, it is important to include provisions obligating the vendor to notify you of any actual or attempted security incident within a reasonable time period. It is also critical that these agreements include requirements for the vendor to keep you informed about findings related to any incident and provisions detailing which party bears the costs associated with forensic investigation, remediation, and individual notifications. Other key provisions include allocating risk between the parties, such as indemnification obligations, limitations of liability, and cyber insurance requirements. Finally, vendor agreements must provide you with the opportunity to reasonably audit the vendor's security measures and protocols with appropriate regularity.

For any questions about how the MOVEit Transfer vulnerability might affect your business or your clients, or how you can prepare for these types of threats, please contact one of the authors or any member of the Baker Donelson Data Protection, Privacy and Cybersecurity Team.