



Progress MOVEit Transfer SQL Injection Vulnerability

Zero-day vulnerability exploited in data theft attacks

<https://community.progress.com/s/article/MOVEit-Transfer-Critical-Vulnerability-31May2023>
CVEs: [CVE-2023-34362](#), [CVE-2023-35708](#), [CVE-2023-35036](#)

A SQL injection vulnerability has been found in the MOVEit Transfer web application that could allow an unauthenticated attacker to gain access to MOVEit Transfer's database. According to the vendor, depending on the database engine being used (MySQL, Microsoft SQL Server, or Azure SQL), an attacker may be able to gather information about the structure and contents of the database and execute SQL statements that can change or delete database elements..

Background	MOVEit Transfer is a managed file transfer (MFT) solution developed by Ipswitch, a subsidiary of Progress Software Corporation, that allows the enterprise to securely transfer files between business partners and customers using SFTP, SCP, and HTTP-based uploads. Previously during Feb of this year, we saw a different MFT solution, Fortra GoAnywhere MFT exploited by attackers for ransomware attacks on various organizations which shows file transfer solution remain a target for ransomware attacks. To read the full Outbreak Report, go to Additional Resources section below.
Announced	May 31, 2023: Vulnerability was announced by Progress Software Corporation. https://community.progress.com/s/article/MOVEit-Transfer-Critical-Vulnerability-31May2023 June 2, 2023: CISA added CVE-2023-34362 to its Known Exploited Vulnerability catalog (KEV)
Latest Developments	June 2, 2023: FortiGuard Labs released a Threat Signal on Progress MOVEit Transfer SQL Injection Vulnerability. https://www.fortiguard.com/threat-signal-report/5174 June 4, 2023: Microsoft links attacks exploiting the CVE-2023-34362 MOVEit Transfer 0-day vulnerability to Lace Tempest aka ClOp ransomware group. https://twitter.com/MsfSecIntel/status/1665537730946670595 June 7, 2023: CISA released a Cybersecurity Advisory, "Ransomware Gang Exploits CVE-2023-34362 MOVEit Vulnerability" https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-158a June 8, 2023: FortiGuard Threat Labs released a detailed blog on CVE-2023-34362 https://www.fortinet.com/blog/threat-research/moveit-transfer-critical-vulnerability-cve-2023-34362-exploited-as-a-0-day June 9, 2023: Another SQL injection vulnerability (CVE-2023-35036) have been identified in the MOVEit Transfer web application that could allow an un-authenticated attacker to gain unauthorized access to the MOVEit Transfer database. https://community.progress.com/s/article/MOVEit-Transfer-Critical-Vulnerability-CVE-2023-35036-June-9-2023 June 15, 2023: Progress discovered a vulnerability (CVE-2023-35708) in MOVEit Transfer that could lead to escalated privileges and potential unauthorized access to the environment. https://community.progress.com/s/article/MOVEit-Transfer-Critical-Vulnerability-15June2023 May, 2024: The University System of Georgia (USG) is sending data breach notifications to 800,000 individuals whose data was exposed in the 2023 ClOp MOVEit attacks. https://apps.web.maine.gov/online/a/viewer/ME/40/5b9aff63-0dc1-429a-a5e4-6b8e6c859f02.shtml

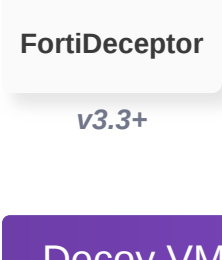
PROTECT

Countermeasures across the security fabric for protecting assets, data and network from cybersecurity events:

Reconnaissance

Lure

Detects attack attempts related to Progress MOVEit Transfer SQL Injection Vulnerability and prevents lateral movement on the network segment



v3.3+

Decoy VM

Detects attack attempts related to Progress MOVEit Transfer SQL Injection Vulnerability and prevents lateral movement on the network segment



v3.3+

Weaponization

Delivery

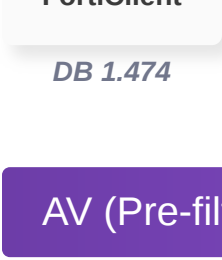
AV

Detects known malware related to Progress MOVEit Transfer vulnerability campaign



Vulnerability

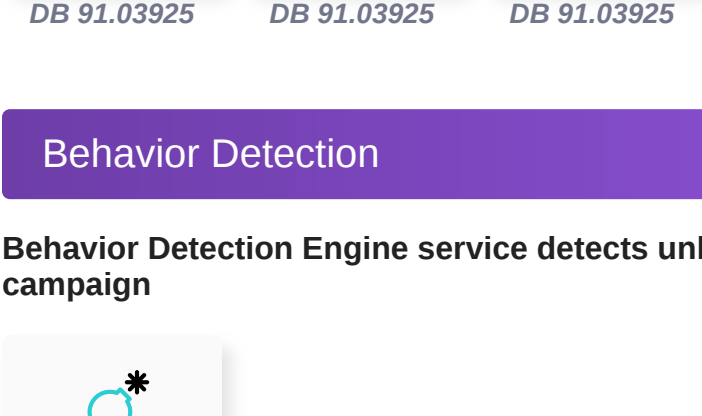
Detects windows device instances running vulnerable Progress MOVEit application



DB 1.474

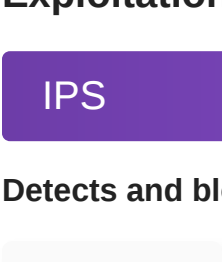
AV (Pre-filter)

Detects known malware related to Progress MOVEit Transfer vulnerability campaign



Behavior Detection

Behavior Detection Engine service detects unknown malware related to Progress MOVEit Transfer vulnerability campaign

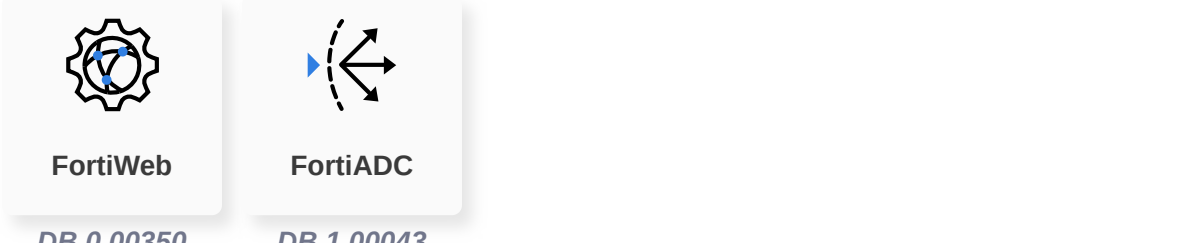


v4.0+

Exploitation

IPS

Detects and blocks attack attempts leveraging vulnerable MOVEit Transfer Web Application vulnerabilities



Web App Security

Detects and blocks attack attempts leveraging vulnerable MOVEit Transfer Web Application vulnerabilities (CVE-2023-34362, CVE-2023-35708, CVE-2023-35036)



Installation

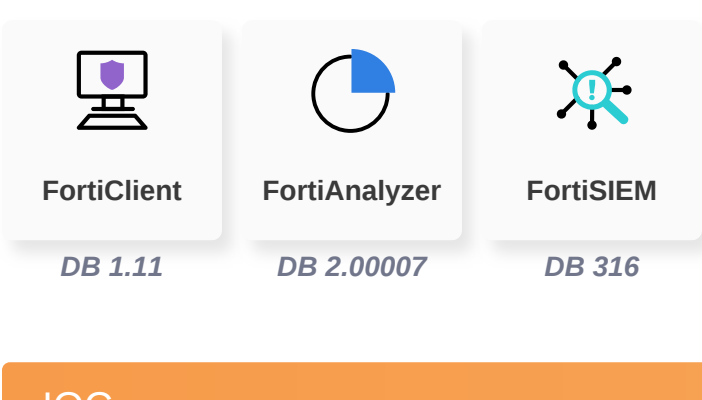
C2

Action

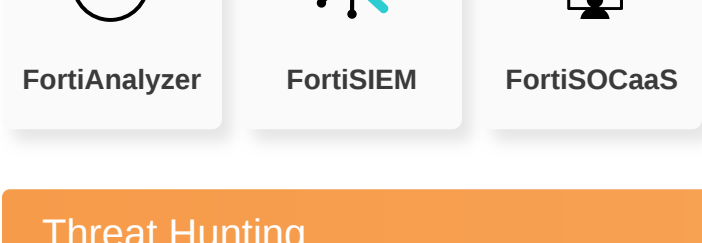
DETECT

Find and correlate important information to identify an outbreak, the following updates are available to raise alert and generate reports:

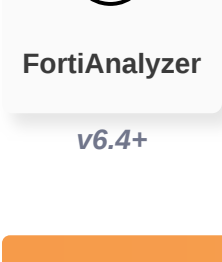
Outbreak Detection



IOC

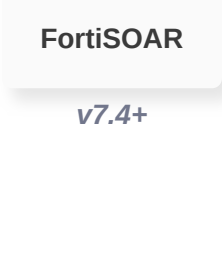


Threat Hunting



v6.4+

Playbook



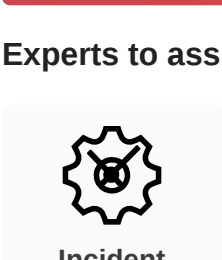
v7.4+

RESPOND

Develop containment techniques to mitigate impacts of security events:

Automated Response

Services that can automatically respond to this outbreak.



Assisted Response Services

Experts to assist you with analysis, containment and response activities.



RECOVER

Improve security posture and processes by implementing security awareness and training, in preparation for (and recovery from) security incidents:

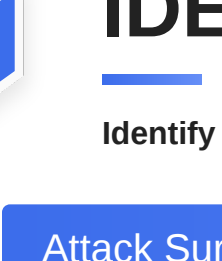
NOC/SOC Training

Train your network and security professionals and optimize your incident response to stay on top of the cyberattacks.



End-User Training

Raise security awareness to your employees that are continuously being targetted by phishing, drive-by download and other forms of cyberattacks.

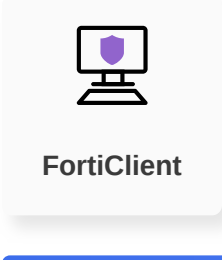


IDENTIFY

Identify processes and assets that need protection:

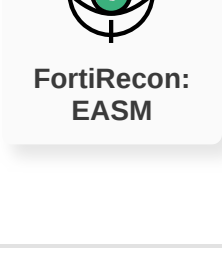
Attack Surface Hardening

Check Security Fabric devices to build actionable configuration recommendations and key indicators.



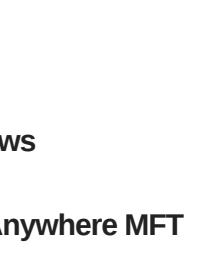
Vulnerability Management

Reduce the attack surface on software vulnerabilities via systematic and automated patching.



Business Reputation

Know attackers next move to protect against your business branding.



Additional Resources

Bleeping Computer	https://www.bleepingcomputer.com/news/security/microsoft-links-clop-ransomware-gang-to-moveit-data-theft-attacks/
SecurityWeek	https://www.securityweek.com/ransomware-group-used-moveit-exploit-to-steal-data-from-dozens-of-organizations/
The Hacker News	https://thehackernews.com/2023/06/moveit-transfer-under-attack-zero-day.html
Outbreak: GoAnywhere MFT RCE	https://www.fortiguard.com/outbreak-alert/goanywhere-mft-rce
FortiGuard Threat Signal	https://www.fortiguard.com/threat-signal-report/5174
Bleeping Computer	https://www.bleepingcomputer.com/news/security/millions-of-oregon-louisiana-state-ids-stolen-in-moveit-breach/

Learn more about [FortiGuard Outbreak Alerts](#)