# Memo

**To:** ITS Department, Marymount University

**From:** Abdulla

**Subject:** Software Vulnerabilities Exploited in 2024 and Their Impact

## This memo provides details about two major software vulnerabilities that were exploited in 2024. These vulnerabilities led to significant data breaches, affecting companies and individuals.

**1. MOVEit Transfer Vulnerability**

**Description:**  
MOVEit Transfer is a widely used file transfer tool for securely sharing sensitive data. In mid-2024, a critical vulnerability (CVE-2024-5806) was discovered. Attackers exploited a SQL injection flaw in the software, allowing them to access stored files without authorization. The vulnerability arose due to improper validation of user inputs, enabling attackers to manipulate SQL queries and extract confidential data.

**How It Was Exploited:**  
Hackers used automated scripts to find systems running MOVEit Transfer. Once they identified vulnerable systems, they then executed malicious SQL commands to extract data. This attack was primarily carried out by a ransomware group that demanded payments from affected companies.

**Impact:**

* Over 50 organizations worldwide were affected including financial institutions and government agencies.
* Millions of sensitive records, such as customer banking details and personally identifiable information (PII) were exposed.
* Some companies had to pay ransom to prevent their data from being publicly leaked on dark web forums.
* Organizations suffered financial losses, reputational damage and faced potential legal consequences due to compliance violations.

**2. Ivanti VPN Vulnerability**

**Description:**  
Ivanti VPN is a popular remote access tool used by businesses and government agencies to enable secure remote connections. In early 2024, a zero day vulnerability (CVE-2024-21887) was discovered, which allowed attackers to bypass authentication mechanisms and gain full access to internal networks of affected organizations. The flaw originated from insufficient input validation in the authentication process.

**How It Was Exploited:**  
Threat actors targeted government agencies and major corporations using this flaw. They then accessed sensitive data, installed malware and created backdoors to maintain long term access. Some attacks were linked to state sponsored hacking groups.

**Impact:**

* Government agencies and multinational corporations suffered severe data breaches leading to exposure of classified information.
* Critical infrastructure sectors, including healthcare and financial services, were compromised, putting millions of users at risk.
* Attackers exfiltrated sensitive data for espionage, financial fraud and further cyber attacks.
* Businesses had to spend millions of dollars on incident response, forensic investigations, and security upgrades.

**Sources**

<https://www.tenable.com/blog/cve-2024-5806-progress-moveit-transfer-authentication-bypass-vulnerability?utm_source=chatgpt.com>

[https://www.paloaltonetworks.com/cyberpedia/ivanti-VPN-vulnerability-what-you-need-to-know](https://www.tenable.com/blog/cve-2024-5806-progress-moveit-transfer-authentication-bypass-vulnerability?utm_source=chatgpt.com)

**Abdulla**  
ITS Intern  
Marymount University.