

CVE-2023-34362

Progress MOVEit Transfer SQL Injection Vulnerability

Exigent

CISA KEV since Jun 2, 2023

Actively exploited

Ransomware use known

Public exploit module (Metasploit)

In Progress MOVEit Transfer before 2021.0.6 (13.0.6), 2021.1.4 (13.1.4), 2022.0.4 (14.0.4), 2022.1.5 (14.1.5), and 2023.0.1 (15.0.1), 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. Depending on the database engine being used (MySQL, Microsoft SQL Server, or Azure SQL), an attacker may be able to infer information about the structure and contents of the database, and execute SQL statements

EVRS

94/100

Immediate priority

CVSS V3.1

9.8

Critical · NVD

EPSS

0.999

99.97th percentile · FIRST

CISA DEADLINE

Jun 23, 2023

KEV since 2023 · listed over a year

Signals behind the score

☒ counted in the score ☐ not counted

evidence for 6 of 8 signals

☒ CISA KEV	Listed in the catalog	☐ Vendor exploitation	Confirmed exploitation in the wild
☒ Ransomware	Known ransomware campaigns	☐ KEV recency	On the CISA KEV catalog for over two years
☒ EPSS	0.999 probability	☐ Pre-patch disclosure	Disclosure status unavailable
☒ CVSS	Base score 9.8	☐ Microsoft Exploitability Index	Not a Microsoft CVE

Remediation

Out-of-band / urgent Patch or fixed version identified**CISA required action:** Apply updates per vendor instructions.

Basis: CISA KEV required action

that alter or delete database elements. NOTE: this is exploited in the wild in May and June 2023; exploitation of unpatched systems can occur via HTTP or HTTPS. All versions (e.g., 2020.0 and 2019x) before the five explicitly mentioned versions are affected, including older unsupported versions.

Affected and fixed versions

PACKAGE	AFFECTED	FIXED IN	SOURCE
moveit cloud	< 14.0.5.45 ≥ 14.1.0.0 < 14.1.6.97 ≥ 15.0.0.0 < 15.0.2.39	14.0.5.45 · 14.1.6.97 · 15.0.2.39	NVD
moveit transfer	< 2021.0.7 ≥ 2021.1.0 < 2021.1.5 ≥ 2022.0.0 < 2022.0.5 ≥ 2022.1.0 < 2022.1.6 ≥ 2023.0.0 < 2023.0.2	2021.0.7 · 2021.1.5 · 2022.0.5	NVD

Sources

Vendor guidance	github.com/advisories/GHSA-hq22-q5g8-577g	Additional guidance	community.progress.com/s/article/MOVEit-Transfer-Critical-Vulnerability-31May2023
This CVE has a CISA AA located here	cisa.gov/news-events/cybersecurity-advisories/aa23-158a . Please see the AA for associated IOCs. Additional information is available at: https://community.progress.com/s/article/MOVEit-Transfer-Critical-Vulnerability-31May2023	NVD	nvd.nist.gov/vuln/detail/CVE-2023-34362
CISA KEV	cisa.gov/known-exploited-vulnerabilities-catalog	ENISA EUVD	euvd.enisa.europa.eu/vulnerability/EUVD-2023-38442
Current data	evulnable.com/vulnerability-management/cve/CVE-2023-34362		

Snapshot at generation time. EPSS can move quickly. A public exploit module is not evidence of active exploitation.