Published:2026/04/08 Last Updated:2026/04/08

JVN#66473735
Multiple vulnerabilities in Movable Type

JVN
HOME
What is JVN ?
Instructions
List of Vulnerability Report
VN_JP
VN_JP(Unreachable)
VN_VU
TA
TRnotes
JVN iPedia
MyJVN
JVNJS/RSS
Vendor List
List of unreachable developers
Contact

Overview

Movable Type provided by Six Apart Ltd. contains multiple vulnerabilities.

Products Affected

- Movable Type / Movable Type Advanced
  - 9.1.0 and earlier (9.1 series)
  - 9.0.6 and earlier (9.0 series)
  - 8.8.2 and earlier (8.8 series)
  - 8.0.9 and earlier (8.0 series)
- Movable Type Premium / Movable Type Premium Advanced Edition
  - 9.1.0 and earlier (9.1 series)
  - 9.0.6 and earlier (9.0 series)
- Movable Type Premium / Movable Type Premium Advanced Edition / Movable Type Premium (MT8-based)
  - 2.14 and earlier

The vulnerabilities affect Movable Type instances where the Listing Framework is enabled in the administrative console or where the Data API is available. Therefore, the following end-of-support products are also affected.

- Movable Type 5.1 to 5.18（all 5.1 series）
- Movable Type 5.2, 5.2.1 to 5.2.13（all 5.2 series）
- Movable Type 6.0, 6.0.1 to 6.8.8（all 6 series）
- Movable Type 7 r.4207 to r.5510（all 7 series）
- Movable Type 8.4.0 to 8.4.4（all 8.4 series）
- Movable Type Premium 1.0 to 1.68（all MTP 1 series）

Description

The Listing Framework of Movable Type provided by Six Apart Ltd. contains multiple vulnerabilities listed below.

- **Code injection (CWE-94)**
  - CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N Base Score 9.3
  - CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H Base Score 9.8

    - CVE-2026-25776

- **SQL injection (CWE-89)**
    - CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:L/VI:L/VA:L/SC:N/SI:N/SA:N Base Score 6.9
    - CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L Base Score 7.3
    - CVE-2026-33088

Impact

- An attacker could execute arbitrary Perl script (CVE-2026-25776)
- An attacker could execute an arbitrary SQL statement (CVE-2026-33088)

Solution

Update the Software

Update the affected product to the latest version according to the information provided by the developer.
The developer has released the following updates that contain fixes for the vulnerabilities.

- Movable Type
    - 9.1.1 (for cloud version)
    - 9.0.7
    - 8.8.3
    - 8.0.10

- Movable Type Premium
    - 9.1.1 / 9.0.7
    - 2.15

Apply workaround

Attacks via the Data API can be mitigated by disabling its use through the following measures:

- Delete `mt-data-api.cgi` (for CGI environments)
- Set `data_api` in the Movable Type environment variable `RestrictedPSGIApp` (for PSGI, MT 6.2 and later)
- Set an unguessable string in the Movable Type environment variable `DataAPIScript` (for MT 6.0, 6.1)

For more details, refer to the information provided by the developer.

Vendor Status

Vendor	Status	Last Update	Vendor Notes
Six Apart Ltd.	Vulnerable	2026/04/08	Six Apart Ltd. website

References

JPCERT/CC Addendum

Vulnerability Analysis by JPCERT/CC

Credit

CVE-2026-25776
Sho Odagiri of GMO Cybersecurity by Ierae, Inc. reported this vulnerability to Six Apart Ltd. and coordinated. After the coordination was completed, Six Apart Ltd. reported the case to JPCERT/CC to notify users of the solution through JVN.

CVE-2026-33088
Six Apart Ltd. reported this vulnerability to JPCERT/CC to notify users of its solution through JVN. JPCERT/CC and Six Apart Ltd. coordinated under the Information Security Early Warning Partnership.

Other Information

JPCERT Alert	
JPCERT Reports	
CERT Advisory	
CPNI Advisory	
TRnotes	
CVE	CVE-2026-25776
	CVE-2026-33088
JVN iPedia	JVNDB-2026-000050