



# CVE-2026-25776

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#) 

## Summary

<b>CVE</b>	CVE-2026-25776
<b>State</b>	PUBLISHED
<b>Assigner</b>	jpcert
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2026-04-08 09:16:20 UTC
<b>Updated</b>	2026-04-20 17:21:58 UTC
<b>Description</b>	Movable Type provided by Six Apart Ltd. contains a code injection vulnerability which may allow an attacker to execute arbitrary code.

## Risk And Classification

**Primary CVSS:** v4.0 9.3 CRITICAL from vultures@jpcert.or.jp

**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/E:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSX/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/UX

**EPSS:** 0.000640000 probability, percentile 0.199350000 (date 2026-04-14)

**Problem Types:** CWE-94 | CWE-94 Code injection

Version	Source	Type	Score	Severity	Vector
4.0	vultures@jpcert.or.jp	Secondary	9.3	CRITICAL	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/E:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSX/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/UX
4.0	CNA	CVSS	9.3	CRITICAL	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
3.0	vultures@jpcert.or.jp	Secondary	9.8	CRITICAL	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
3.0	CNA	CVSS	9.8	CRITICAL	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

## CVSS v4.0 Breakdown

Attack Vector

**Network**

Attack Complexity

**Low**

Attack Requirements

**None**

Privileges Required

**None**

User Interaction

**None**

None

Confidentiality

High

Integrity

High

Availability

High

Sub Conf.

None

Sub Integrity

None

Sub Availability

None

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/E:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSX/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

### CVSS v3.0 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

High

Integrity

High

Availability

High

CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

### NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Sixapart	Movable Type	All	All	All	All
Application	Sixapart	Movable Type	9.0.5	All	All	All
Application	Sixapart	Movable Type	9.0.6	All	All	All
Application	Sixapart	Movable Type	9.1.0	All	All	All

Application	Sixapart	Movable Type	All	All	All	All
-------------	----------	--------------	-----	-----	-----	-----

## Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Six Apart Ltd.	Movable Type	affected 9.1.0 and earlier	Not specified
CNA	Six Apart Ltd.	Movable Type	affected 9.0.6 and earlier	Not specified
CNA	Six Apart Ltd.	Movable Type	affected 8.8.2 and earlier	Not specified
CNA	Six Apart Ltd.	Movable Type	affected 8.0.9 and earlier	Not specified
CNA	Six Apart Ltd.	Movable Type Advanced	affected 9.1.0 and earlier	Not specified
CNA	Six Apart Ltd.	Movable Type Advanced	affected 9.0.6 and earlier	Not specified
CNA	Six Apart Ltd.	Movable Type Advanced	affected 8.8.2 and earlier	Not specified
CNA	Six Apart Ltd.	Movable Type Advanced	affected 8.0.9 and earlier	Not specified
CNA	Six Apart Ltd.	Movable Type Premium	affected 9.1.0 and earlier	Not specified
CNA	Six Apart Ltd.	Movable Type Premium	affected 9.0.6 and earlier	Not specified
CNA	Six Apart Ltd.	Movable Type Premium Advanced Edition	affected 9.1.0 and earlier	Not specified
CNA	Six Apart Ltd.	Movable Type Premium Advanced Edition	affected 9.0.6 and earlier	Not specified
CNA	Six Apart Ltd.	Movable Type Premium	affected 2.14 and earlier	Not specified
CNA	Six Apart Ltd.	Movable Type Premium Advanced Edition	affected 2.14 and earlier	Not specified
CNA	Six Apart Ltd.	Movable Type Premium MT8-based	affected 2.14 and earlier	Not specified
CNA	Six Apart Ltd.	Movable Type	affected 5.1 to 5.18	Not specified
CNA	Six Apart Ltd.	Movable Type	affected 5.2	Not specified
CNA	Six Apart Ltd.	Movable Type	affected 5.2.1 to 5.2.13	Not specified
CNA	Six Apart Ltd.	Movable Type	affected 6.0	Not specified
CNA	Six Apart Ltd.	Movable Type	affected 6.0.1 to 6.8.8	Not specified
CNA	Six Apart Ltd.	Movable Type	affected 7 r.4207 to r.5510	Not specified
CNA	Six Apart Ltd.	Movable Type	affected 8.4.0 to 8.4.4	Not specified
CNA	Six Apart Ltd.	Movable Type	affected 1.0 to 1.68	Not specified

## References

Reference	Source	Link	Tags
<a href="https://jvn.jp/en/jp/JVN66473735">jvn.jp/en/jp/JVN66473735</a>	<a href="mailto:vultures@jpcert.or.jp">vultures@jpcert.or.jp</a>	<a href="https://jvn.jp">jvn.jp</a>	Third Party Advisory
<a href="https://www.sixapart.jp/movabletype/news/2026/04/08-1100.html">www.sixapart.jp/movabletype/news/2026/04/08-1100.html</a>	<a href="mailto:vultures@jpcert.or.jp">vultures@jpcert.or.jp</a>	<a href="https://www.sixapart.jp">www.sixapart.jp</a>	Vendor Advisory
<a href="https://movabletype.org/news/2026/04/mt-907-released.html">movabletype.org/news/2026/04/mt-907-released.html</a>	<a href="mailto:vultures@jpcert.or.jp">vultures@jpcert.or.jp</a>	<a href="https://movabletype.org">movabletype.org</a>	Vendor Advisory
CVE Program record	CVE.ORG	<a href="https://www.cve.org">www.cve.org</a>	canonical
NVD vulnerability detail	NVD	<a href="https://nvd.nist.gov">nvd.nist.gov</a>	canonical, analysis

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

**Free CVE JSON API** [cve.report/api](#)

**CVE.report and Source URL Uptime Status** [status.cve.report](#)