CVE-2026-25776

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

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

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/MSC:X/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

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:
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

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/MSC:X/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
jvn.jp/en/jp/JVN66473735	vultures@jpcert.or.jp	jvn.jp	Third Party Advisory
www.sixapart.jp/movabletype/news/2026/04/08-1100.html	vultures@jpcert.or.jp	www.sixapart.jp	Vendor Advisory
movabletype.org/news/2026/04/mt-907-released.html	vultures@jpcert.or.jp	movabletype.org	Vendor Advisory
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

No vendor comments have been submitted for this CVE.

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

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status **status.cve.report**