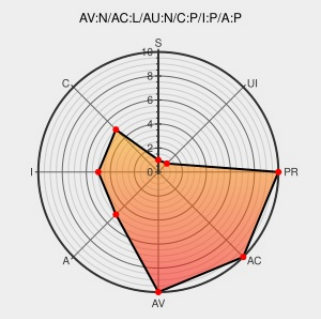
CVE-2014-9057

Published on: 12/16/2014 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:25:59 PM UTC

CVE-2014-9057

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Debian Linux from Debian contain the following vulnerability:

SQL injection vulnerability in the XML-RPC interface in Movable Type before 5.18, 5.2.x before 5.2.11, and 6.x before 6.0.6 allows remote attackers to execute arbitrary SQL commands via unspecified vectors.

CVE-2014-9057 has been assigned by cve@mitre.org to track the vulnerability

CVSS2 Score: 7.5 - HIGH

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
Debian -- Security Information -- DSA-3183-1 movabletype-opensource	www.debian.org, Depreciated Link, text/html	DEBIAN DSA-3183
MovableType.org – Documentation: Movable Type 6.0.6 release notes	Vendor Advisory, movabletype.org, text/html	CONFIRM movabletype.org/documentation/appendices/release-notes/6.0.6.html
Security Advisory SA61227 - Movable Type XML-RPC Interface SQL Injection Vulnerability - Secunia	web.archive.org, text/html	SECUNIA 61227
MovableType.org – News: Movable Type 6.0.6 released	Vendor Advisory, movabletype.org, text/html	CONFIRM movabletype.org/news/2014/12/6.0.6.html

are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Debian	Debian Linux	7.0	All	All	All
Operating System	Debian	Debian Linux	7.0	All	All	All
Application	Sixapart	Movable Type	5.2	All	All	All
Application	Sixapart	Movable Type	5.2.10	All	All	All
Application	Sixapart	Movable Type	5.2.2	All	All	All
Application	Sixapart	Movable Type	5.2.3	All	All	All
Application	Sixapart	Movable Type	5.2.4	All	All	All
Application	Sixapart	Movable Type	5.2.5	All	All	All
Application	Sixapart	Movable Type	5.2.6	All	All	All
Application	Sixapart	Movable Type	5.2.7	All	All	All
Application	Sixapart	Movable Type	5.2.8	All	All	All
Application	Sixapart	Movable Type	5.2.9	All	All	All
Application	Sixapart	Movable Type	6.0	All	All	All
Application	Sixapart	Movable Type	6.0.1	All	All	All
Application	Sixapart	Movable Type	6.0.2	All	All	All
Application	Sixapart	Movable Type	6.0.3	All	All	All
Application	Sixapart	Movable Type	6.0.4	All	All	All
Application	Sixapart	Movable Type	6.0.5	All	All	All
Application	Sixapart	Movable Type	5.2	All	All	All
Application	Sixapart	Movable Type	5.2.10	All	All	All
Application	Sixapart	Movable Type	5.2.2	All	All	All
Application	Sixapart	Movable Type	5.2.3	All	All	All
Application	Sixapart	Movable Type	5.2.4	All	All	All
Application	Sixapart	Movable Type	5.2.5	All	All	All
Application	Sixapart	Movable Type	5.2.6	All	All	All
Application	Sixapart	Movable Type	5.2.7	All	All	All
Application	Sixapart	Movable Type	5.2.8	All	All	All
Application	Sixapart	Movable Type	5.2.9	All	All	All

Application	Sixapart	Movable Type	6.0	All	All	All
Application	Sixapart	Movable Type	6.0.1	All	All	All
Application	Sixapart	Movable Type	6.0.2	All	All	All
Application	Sixapart	Movable Type	6.0.3	All	All	All
Application	Sixapart	Movable Type	6.0.4	All	All	All
Application	Sixapart	Movable Type	6.0.5	All	All	All
Application	Sixapart	Movable Type	All	All	All	All

cpe:2.3:o:debian:debian_linux:7.0:*:*:*:*:*:*:*:

cpe:2.3:o:debian:debian_linux:7.0:*:*:*:*:*:*:*:

cpe:2.3:a:sixapart:movable_type:5.2:*:*:*:*:*:*:*:

cpe:2.3:a:sixapart:movable_type:5.2.10:*:*:*:*:*:*:*:

cpe:2.3:a:sixapart:movable_type:5.2.2:*:*:*:*:*:*:*:

cpe:2.3:a:sixapart:movable_type:5.2.3:*:*:*:*:*:*:*:

cpe:2.3:a:sixapart:movable_type:5.2.4:*:*:*:*:*:*:*:

cpe:2.3:a:sixapart:movable_type:5.2.5:*:*:*:*:*:*:*:

cpe:2.3:a:sixapart:movable_type:5.2.6:*:*:*:*:*:*:*:

cpe:2.3:a:sixapart:movable_type:5.2.7:*:*:*:*:*:*:*:

cpe:2.3:a:sixapart:movable_type:5.2.8:*:*:*:*:*:*:*:

cpe:2.3:a:sixapart:movable_type:5.2.9:*:*:*:*:*:*:*:

cpe:2.3:a:sixapart:movable_type:6.0:*:*:*:*:*:*:*:

cpe:2.3:a:sixapart:movable_type:6.0.1:*:*:*:*:*:*:*:

cpe:2.3:a:sixapart:movable_type:6.0.2:*:*:*:*:*:*:*:

cpe:2.3:a:sixapart:movable_type:6.0.3:*:*:*:*:*:*:*:

cpe:2.3:a:sixapart:movable_type:6.0.4:*:*:*:*:*:*:*:

cpe:2.3:a:sixapart:movable_type:6.0.5:*:*:*:*:*:*:*:

cpe:2.3:a:sixapart:movable_type:5.2:*:*:*:*:*:*:*:

cpe:2.3:a:sixapart:movable_type:5.2.10:*:*:*:*:*:*:*:

cpe:2.3:a:sixapart:movable_type:5.2.2:*:*:*:*:*:*:*:

cpe:2.3:a:sixapart:movable_type:5.2.3:*:*:*:*:*:*:*:

cpe:2.3:a:sixapart:movable_type:5.2.4:*:*:*:*:*:*:*:

cpe:2.3:a:sixapart:movable_type:5.2.5:*:*:*:*:*:*:*:

cpe:2.3:a:sixapart:movable_type:5.2.6:*:*:*:*:*:*:*:

cpe:2.3:a:sixapart:movable_type:5.2.7:*:*:*:*:*:*:*:

cpe:2.3:a:sixapart:movable_type:5.2.8:*:*:*:*:*:*:*:

cpe:2.3:a:sixapart:movable_type:5.2.9:*:*:*:*:*:*:*:

cpe:2.3:a:sixapart:movable_type:6.0:*:*:*:*:*:*:*:

cpe:2.3:a:sixapart:movable_type:6.0.1:*:*:*:*:*:*:*:

cpe:2.3:a:sixapart:movable_type:6.0.2:*:*:*:*:*:*:*:

cpe:2.3:a:sixapart:movable_type:6.0.3:*:*:*:*:*:*:*:

cpe:2.3:a:sixapart:movable_type:6.0.4:*:*:*:*:*:*:*:

cpe:2.3:a:sixapart:movable_type:6.0.5:*:*:*:*:*:*:*:

cpe:2.3:a:sixapart:movable_type:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→