



# CVE-2012-2998

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064\_img.jpg\)](#)

## Summary

<b>CVE</b>	CVE-2012-2998
<b>State</b>	PUBLIC
<b>Assigner</b>	cert@cert.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2012-09-28 10:40:00 UTC
<b>Updated</b>	2013-02-14 04:53:00 UTC
<b>Description</b>	SQL injection vulnerability in the ad hoc query module in Trend Micro Control Manager (TMCM) before 5.5.0.1823 and 6.0.0.1823

## Risk And Classification

**Problem Types:** CWE-89

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Trend Micro	Control Manager	2.0	All	All	All
Application	Trend Micro	Control Manager	2.1	All	All	All
Application	Trend Micro	Control Manager	2.5	All	All	All
Application	Trend Micro	Control Manager	3.0	All	ent_ed	All
Application	Trend Micro	Control Manager	3.0	All	std_ed	All
Application	Trend Micro	Control Manager	3.5	All	ent_ed	All
Application	Trend Micro	Control Manager	3.5	All	std_ed	All
Application	Trend Micro	Control Manager	5.0	All	adv_ed	All
Application	Trend Micro	Control Manager	5.0	All	std_ed	All
Application	Trend Micro	Control Manager	5.5	All	adv_ed	All
Application	Trend Micro	Control Manager	6.0	All	All	All
Application	Trend Micro	Control Manager	2.0	All	All	All
Application	Trend Micro	Control Manager	2.1	All	All	All
Application	Trend Micro	Control Manager	2.5	All	All	All
Application	Trend Micro	Control Manager	3.0	All	ent_ed	All
Application	Trend Micro	Control Manager	3.0	All	std_ed	All
Application	Trend Micro	Control Manager	3.5	All	ent_ed	All

Application	<a href="#">Trend Micro</a>	<a href="#">Control Manager</a>	3.5	All	std_ed	All
Application	<a href="#">Trend Micro</a>	<a href="#">Control Manager</a>	5.0	All	adv_ed	All
Application	<a href="#">Trend Micro</a>	<a href="#">Control Manager</a>	5.0	All	std_ed	All
Application	<a href="#">Trend Micro</a>	<a href="#">Control Manager</a>	5.5	All	adv_ed	All
Application	<a href="#">Trend Micro</a>	<a href="#">Control Manager</a>	6.0	All	All	All
Application	<a href="#">Trend Micro</a>	<a href="#">Control Manager</a>	All	All	std_ed	All

## References

Reference	S
US-CERT Vulnerability Note VU#950795 - Trend Micro Control Manager adhoc query vulnerability	C
<a href="http://www.trendmicro.com/ftp/documentation/readme/readme_critical_patch_TMCM55_1823.txt">www.trendmicro.com/ftp/documentation/readme/readme_critical_patch_TMCM55_1823.txt</a>	C
Trend Micro Control Manager SQL Injection Vulnerability   Spentera	M
JVN#42014489: Trend Micro Control Manager vulnerable to SQL injection	J
<a href="http://www.trendmicro.com/ftp/documentation/readme/readme_critical_patch_tmcm60_patch1_...">www.trendmicro.com/ftp/documentation/readme/readme_critical_patch_tmcm60_patch1_...</a>	C
SQL injection vulnerability - Control Manager	C
JVNDB-2012-000090	J
Trend Micro Control Manager Input Validation Flaw in Ad Hoc Query Module Lets Remote Users Inject SQL Commands - SecurityTracker	S
CVE Program record	C
NVD vulnerability detail	M

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](#).

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