



# CVE-2014-4189

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

## Summary

<b>CVE</b>	CVE-2014-4189
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2014-06-17 14:55:00 UTC
<b>Updated</b>	2015-09-02 17:05:00 UTC
<b>Description</b>	Cross-site scripting (XSS) vulnerability in Hitachi Tuning Manager before 7.6.1-06 and 8.x before 8.0.0-04 and JP1/Perform

## Risk And Classification

### Problem Types: CWE-79

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Hitachi	Jp1/performance Management-manager Web Option	07-00	All	All	All
Application	Hitachi	Jp1/performance Management-manager Web Option	07-00	All	All	All
Application	Hitachi	Jp1/performance Management-manager Web Option	07-54	All	All	All
Application	Hitachi	Jp1/performance Management-manager Web Option	07-54	All	All	All
Application	Hitachi	Jp1/performance Management-manager Web Option	07-00	All	All	All
Application	Hitachi	Jp1/performance Management-manager Web Option	07-00	All	All	All
Application	Hitachi	Jp1/performance Management-manager Web Option	07-54	All	All	All
Application	Hitachi	Jp1/performance Management-manager Web Option	07-54	All	All	All
Application	Hitachi	Jp1/performance Management-manager Web Option	07-00	All	All	All
Application	Hitachi	Jp1/performance Management-manager Web Option	07-00	All	All	All
Application	Hitachi	Jp1/performance Management-manager Web Option	07-54	All	All	All
Application	Hitachi	Jp1/performance Management-manager Web Option	07-54	All	All	All
Application	Hitachi	Tuning Manager	6.0.0	All	All	All
Application	Hitachi	Tuning Manager	6.0.0	All	All	All
Application	Hitachi	Tuning Manager	7.1.0	All	All	All
Application	Hitachi	Tuning Manager	7.6.1	All	All	All
Application	Hitachi	Tuning Manager	7.6.1	05	All	All

Application	Hitachi	Tuning Manager	8.0.0	All	All	All
Application	Hitachi	Tuning Manager	8.0.0	All	All	All
Application	Hitachi	Tuning Manager	8.0.0	03	All	All
Application	Hitachi	Tuning Manager	8.0.0	03	All	All
Application	Hitachi	Tuning Manager	6.0.0	All	All	All
Application	Hitachi	Tuning Manager	6.0.0	All	All	All
Application	Hitachi	Tuning Manager	7.1.0	All	All	All
Application	Hitachi	Tuning Manager	7.6.1	All	All	All
Application	Hitachi	Tuning Manager	7.6.1	05	All	All
Application	Hitachi	Tuning Manager	8.0.0	All	All	All
Application	Hitachi	Tuning Manager	8.0.0	All	All	All
Application	Hitachi	Tuning Manager	8.0.0	03	All	All
Application	Hitachi	Tuning Manager	8.0.0	03	All	All

## References

### Reference

Security Advisory SA58899 - Hitachi Tuning Manager Cross-Site Scripting and Request Forgery Vulnerabilities - Secunia

Multiple Vulnerabilities in Hitachi Tuning Manager, and JP1/Performance Management - Manager Web Option: Software Vulnerability Informa

Security Advisory SA58528 - Hitachi Tuning Manager / JP1/Performance Management Two Vulnerabilities - Secunia

Multiple Hitachi Products Cross Site Scripting and Cross Site Request Forgery Vulnerabilities

CVE Program record

NVD vulnerability detail

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](#)