



# CVE-2009-1291

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

## Summary

<b>CVE</b>	CVE-2009-1291
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2009-04-30 20:30:00 UTC
<b>Updated</b>	2017-08-17 01:30:00 UTC
<b>Description</b>	Stack-based buffer overflow in TIBCO SmartSockets before 6.8.2, SmartSockets Product Family (aka RTworks) before 4.0.

## Risk And Classification

**Problem Types:** CWE-119

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	<a href="#">Tibco</a>	<a href="#">Enterprise Message Service</a>	4.0.0	All	All	All
Application	<a href="#">Tibco</a>	<a href="#">Enterprise Message Service</a>	4.1.0	All	All	All
Application	<a href="#">Tibco</a>	<a href="#">Enterprise Message Service</a>	4.2.0	All	All	All
Application	<a href="#">Tibco</a>	<a href="#">Enterprise Message Service</a>	4.3.0	All	All	All
Application	<a href="#">Tibco</a>	<a href="#">Enterprise Message Service</a>	4.4.1	All	All	All
Application	<a href="#">Tibco</a>	<a href="#">Enterprise Message Service</a>	4.4.2	All	All	All
Application	<a href="#">Tibco</a>	<a href="#">Enterprise Message Service</a>	4.0.0	All	All	All
Application	<a href="#">Tibco</a>	<a href="#">Enterprise Message Service</a>	4.1.0	All	All	All
Application	<a href="#">Tibco</a>	<a href="#">Enterprise Message Service</a>	4.2.0	All	All	All
Application	<a href="#">Tibco</a>	<a href="#">Enterprise Message Service</a>	4.3.0	All	All	All
Application	<a href="#">Tibco</a>	<a href="#">Enterprise Message Service</a>	4.4.1	All	All	All
Application	<a href="#">Tibco</a>	<a href="#">Enterprise Message Service</a>	4.4.2	All	All	All
Application	<a href="#">Tibco</a>	<a href="#">Enterprise Message Service</a>	All	All	All	All
Application	<a href="#">Tibco</a>	<a href="#">Rtworks</a>	4.0.3	All	All	All
Application	<a href="#">Tibco</a>	<a href="#">Rtworks</a>	4.0.4	All	All	All
Application	<a href="#">Tibco</a>	<a href="#">Rtworks</a>	4.0.3	All	All	All
Application	<a href="#">Tibco</a>	<a href="#">Rtworks</a>	4.0.4	All	All	All

Application	<a href="#">Tibco</a>	<a href="#">Smartsockets</a>	6.8.0	All	All	All
Application	<a href="#">Tibco</a>	<a href="#">Smartsockets</a>	6.8.1	All	All	All
Application	<a href="#">Tibco</a>	<a href="#">Smartsockets</a>	6.8.0	All	All	All
Application	<a href="#">Tibco</a>	<a href="#">Smartsockets</a>	6.8.1	All	All	All
Application	<a href="#">Tibco</a>	<a href="#">Smartsockets Rtserver</a>	6.8.0	All	All	All
Application	<a href="#">Tibco</a>	<a href="#">Smartsockets Rtserver</a>	6.8.0	All	All	All
Application	<a href="#">Tibco</a>	<a href="#">Smartsockets Rtserver</a>	All	All	All	All

## References

Reference
<a href="#">Public Advisory: 04.28.09 // iDefense Labs</a>
<a href="#">IBM X-Force Exchange</a>
<a href="#">Webmail : Solution de messagerie professionnelle - OVHcloud- OVH</a>
<a href="#">404 Not Found</a>
<a href="#">TIBCO   TIBCO Security Advisory FAQ: SmartSockets, SmartSockets Product Family Modules (formerly RTworks), Enterprise Message Servi</a>
<a href="#">TIBCO   Security Advisories for TIBCO Products</a>
<a href="#">404 Not Found</a>
<a href="#">404 Not Found</a>
<a href="#">TIBCO SmartSockets Buffer Overflow Vulnerability - Secunia Advisories - Vulnerability Information - Secunia.com</a>
<a href="#">TIBCO SmartSockets Stack Overflow in RTserver Lets Remote Users Execute Arbitrary Code - SecurityTracker</a>
<a href="#">TIBCO SmartSockets RTserver Stack Buffer Overflow Vulnerability</a>
<a href="#">Harmony Security : Blog</a>
<a href="#">CVE Program record</a>
<a href="#">NVD vulnerability detail</a>

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](#)