



CVE-2009-2898

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

Summary

CVE	CVE-2009-2898
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2009-10-13 10:30:00 UTC
Updated	2018-10-10 19:42:00 UTC
Description	Cross-site scripting (XSS) vulnerability in the Alerts list feature in the web interface in SpringSource Hyperic HQ 3.2.x before

Risk And Classification

Problem Types: CWE-79

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Springsource	Application Management Suite	2.0.0	sr3	All	All
Application	Springsource	Application Management Suite	2.0.0	sr3	All	All
Application	Springsource	Hyperic Hq	3.2	beta_1	All	All
Application	Springsource	Hyperic Hq	3.2.0	All	All	All
Application	Springsource	Hyperic Hq	3.2.1	All	All	All
Application	Springsource	Hyperic Hq	3.2.2	All	All	All
Application	Springsource	Hyperic Hq	3.2.3	All	All	All
Application	Springsource	Hyperic Hq	3.2.4	All	All	All
Application	Springsource	Hyperic Hq	3.2.5	All	All	All
Application	Springsource	Hyperic Hq	3.2.6	All	All	All
Application	Springsource	Hyperic Hq	4.0.0	All	All	All
Application	Springsource	Hyperic Hq	4.0.1	All	All	All
Application	Springsource	Hyperic Hq	4.0.2	All	All	All
Application	Springsource	Hyperic Hq	4.0.3	All	All	All
Application	Springsource	Hyperic Hq	4.1.0	All	All	All
Application	Springsource	Hyperic Hq	4.1.1	All	All	All
Application	Springsource	Hyperic Hq	4.1.2	All	All	All

Application	Springsource	Hyperic Hq	4.2	beta_1	All	All
Application	Springsource	Hyperic Hq	3.2	beta_1	All	All
Application	Springsource	Hyperic Hq	3.2.0	All	All	All
Application	Springsource	Hyperic Hq	3.2.1	All	All	All
Application	Springsource	Hyperic Hq	3.2.2	All	All	All
Application	Springsource	Hyperic Hq	3.2.3	All	All	All
Application	Springsource	Hyperic Hq	3.2.4	All	All	All
Application	Springsource	Hyperic Hq	3.2.5	All	All	All
Application	Springsource	Hyperic Hq	3.2.6	All	All	All
Application	Springsource	Hyperic Hq	4.0.0	All	All	All
Application	Springsource	Hyperic Hq	4.0.1	All	All	All
Application	Springsource	Hyperic Hq	4.0.2	All	All	All
Application	Springsource	Hyperic Hq	4.0.3	All	All	All
Application	Springsource	Hyperic Hq	4.1.0	All	All	All
Application	Springsource	Hyperic Hq	4.1.1	All	All	All
Application	Springsource	Hyperic Hq	4.1.2	All	All	All
Application	Springsource	Hyperic Hq	4.2	beta_1	All	All
Application	Springsource	Tc Server	6.0.20	b	All	All
Application	Springsource	Tc Server	6.0.20	b	All	All

References

Reference	Source	Link	Tags
SecurityFocus	BUGTRAQ	www.securityfocus.com	
jira.hyperic.com/browse/HHQ-3390	CONFIRM	jira.hyperic.com	
Core Security Technologies	MISC	www.coresecurity.com	Patch
SecurityFocus	BUGTRAQ	www.securityfocus.com	
IBM X-Force Exchange	XF	exchange.xforce.ibmcloud.com	
58611	OSVDB	www.osvdb.org	
Hyperic HQ Known Vulnerabilities SpringSource	CONFIRM	www.springsource.com	Patch, Vendor
Corelabs site	MISC	corelabs.coresecurity.com	Exploit, PoC
Hyperic HQ Cross-Site Scripting and Script Insertion Vulnerabilities - Secunia.com	SECUNIA	secunia.com	Vendor Advisory
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical

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](#).

Free CVE JSON API [cve.report/api](#)

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