

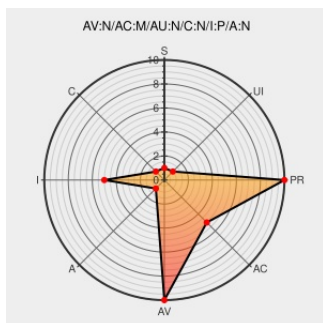


CVE-2009-3892

Published on: 11/17/2009 12:00:00 AM UTC

Last Modified on: 02/13/2023 01:17:00 AM UTC

CVE-2009-3892

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

Certain versions of [Rt](#) from [Bestpractical](#) contain the following vulnerability:

Cross-site scripting (XSS) vulnerability in Best Practical Solutions RT 3.6.x before 3.6.9, 3.8.x before 3.8.5, and other 3.4.6 through 3.8.4 versions allows remote attackers to inject arbitrary web script or HTML via certain Custom Fields.

CVE-2009-3892 has been assigned by secalert@redhat.com to track the vulnerability

CVSS2 Score: **4.3 - MEDIUM**

Access
Vector

NETWORK

Access
Complexity

MEDIUM

Authentication

NONE

Confidentiality
Impact

NONE

Integrity
Impact

PARTIAL

Availability
Impact

NONE

CVE References

Description

Tags

Link

oss-security - Re: CVE Id request: request-tracker

[www.openwall.com
text/html](http://www.openwall.com/text/html)

[MLIST \[oss-security\] 20091116 Re: CVE Id request: request-tracker](#)

oss-security - CVE Id request: request-tracker

[www.openwall.com
text/html](http://www.openwall.com/text/html)

[MLIST \[oss-security\] 20091115 CVE Id request: request-tracker](#)

#546778 - request-tracker3.6: XSS vulnerability when displaying Custom Field values - Debian Bug report logs

[bugs.debian.org
text/html](http://bugs.debian.org/text/html)

CONFIRM bugs.debian.org/cgi-bin/bugreport.cgi?bug=546778

538173 - (CVE-2009-3892) CVE-2009-3892 Request Tracker XSS flaw

[bugzilla.redhat.com
text/html](http://bugzilla.redhat.com/text/html)

[MISC bugzilla.redhat.com/show_bug.cgi?id=538173](#)

[Rt-announce] RT 3.8.5 Released

[Patch lists.bestpractical.com
text/html](#)

[MLIST \[rt-announce\] 20090914 RT 3.8.5 Released](#)

[Rt-announce] RT 3.6.9 Released

Patch

lists.bestpractical.com

text/html

 [MLIST \[rt-announce\] 20090914 RT 3.6.9 Released](#)

Red Hat Customer Portal - Access to 24x7 support and knowledge

access.redhat.com

text/html

 **MISC**
access.redhat.com/security/cve/CVE-2009-3892

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that 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
Application	Bestpractical	Rt	3.4.6	All	All	All
Application	Bestpractical	Rt	3.6.0	All	All	All
Application	Bestpractical	Rt	3.6.1	All	All	All
Application	Bestpractical	Rt	3.6.2	All	All	All
Application	Bestpractical	Rt	3.6.3	All	All	All
Application	Bestpractical	Rt	3.6.4	All	All	All
Application	Bestpractical	Rt	3.6.5	All	All	All
Application	Bestpractical	Rt	3.6.6	All	All	All
Application	Bestpractical	Rt	3.6.7	All	All	All
Application	Bestpractical	Rt	3.6.8	All	All	All
Application	Bestpractical	Rt	3.8.0	All	All	All
Application	Bestpractical	Rt	3.8.1	All	All	All
Application	Bestpractical	Rt	3.8.2	All	All	All
Application	Bestpractical	Rt	3.8.3	All	All	All
Application	Bestpractical	Rt	3.8.4	All	All	All
Application	Bestpractical	Rt	3.4.6	All	All	All
Application	Bestpractical	Rt	3.6.0	All	All	All
Application	Bestpractical	Rt	3.6.1	All	All	All
Application	Bestpractical	Rt	3.6.2	All	All	All
Application	Bestpractical	Rt	3.6.3	All	All	All
Application	Bestpractical	Rt	3.6.4	All	All	All
Application	Bestpractical	Rt	3.6.5	All	All	All
Application	Bestpractical	Rt	3.6.6	All	All	All
Application	Bestpractical	Rt	3.6.7	All	All	All

Application	Bestpractical	Rt	3.6.8	All	All	All
Application	Bestpractical	Rt	3.8.0	All	All	All
Application	Bestpractical	Rt	3.8.1	All	All	All
Application	Bestpractical	Rt	3.8.2	All	All	All
Application	Bestpractical	Rt	3.8.3	All	All	All
Application	Bestpractical	Rt	3.8.4	All	All	All
cpe:2.3:a:bestpractical:rt:3.4.6:*****:						
cpe:2.3:a:bestpractical:rt:3.6.0:*****:						
cpe:2.3:a:bestpractical:rt:3.6.1:*****:						
cpe:2.3:a:bestpractical:rt:3.6.2:*****:						
cpe:2.3:a:bestpractical:rt:3.6.3:*****:						
cpe:2.3:a:bestpractical:rt:3.6.4:*****:						
cpe:2.3:a:bestpractical:rt:3.6.5:*****:						
cpe:2.3:a:bestpractical:rt:3.6.6:*****:						
cpe:2.3:a:bestpractical:rt:3.6.7:*****:						
cpe:2.3:a:bestpractical:rt:3.6.8:*****:						
cpe:2.3:a:bestpractical:rt:3.8.0:*****:						
cpe:2.3:a:bestpractical:rt:3.8.1:*****:						
cpe:2.3:a:bestpractical:rt:3.8.2:*****:						
cpe:2.3:a:bestpractical:rt:3.8.3:*****:						
cpe:2.3:a:bestpractical:rt:3.8.4:*****:						
cpe:2.3:a:bestpractical:rt:3.4.6:*****:						
cpe:2.3:a:bestpractical:rt:3.6.0:*****:						
cpe:2.3:a:bestpractical:rt:3.6.1:*****:						
cpe:2.3:a:bestpractical:rt:3.6.2:*****:						
cpe:2.3:a:bestpractical:rt:3.6.3:*****:						
cpe:2.3:a:bestpractical:rt:3.6.4:*****:						
cpe:2.3:a:bestpractical:rt:3.6.5:*****:						
cpe:2.3:a:bestpractical:rt:3.6.6:*****:						

cpe:2.3:a:bestpractical:rt:3.6.7:*****:
cpe:2.3:a:bestpractical:rt:3.6.8:*****:
cpe:2.3:a:bestpractical:rt:3.8.0:*****:
cpe:2.3:a:bestpractical:rt:3.8.1:*****:
cpe:2.3:a:bestpractical:rt:3.8.2:*****:
cpe:2.3:a:bestpractical:rt:3.8.3:*****:
cpe:2.3:a:bestpractical:rt:3.8.4:*****:

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID→](#)