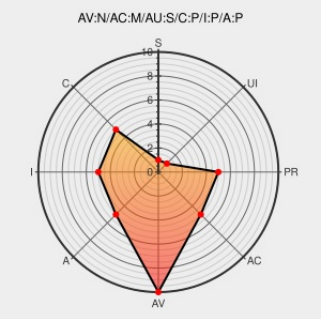
CVE-2012-4733

Published on: 08/23/2013 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:28:15 PM UTC

CVE-2012-4733

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Rt from Bestpractical contain the following vulnerability:

Request Tracker (RT) 4.x before 4.0.13 does not properly enforce the DeleteTicket and "custom lifecycle transition" permission, which allows remote authenticated users with the ModifyTicket permission to delete tickets via unspecified vectors.

CVE-2012-4733 has been assigned by cve@mitre.org to track the vulnerability

CVSS2 Score: 6 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	SINGLE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
[rt-announce] Security vulnerabilities in RT	Vendor Advisory, lists.bestpractical.com, text/html	MLIST [rt-announce] 20130522 Security vulnerabilities in RT
Security Advisory SA53522 - RT Multiple Vulnerabilities - Secunia	Vendor Advisory, web.archive.org, text/html	SECUNIA 53522
No Description Provided	www.osvdb.org, Inactive Link, Not Archived	OSVDB 93611
[rt-announce] RT 4.0.13 released	Patch, lists.bestpractical.com, text/html	MLIST [rt-announce] 20130522 RT 4.0.13 released

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	4.0.0	All	All	All
Application	Bestpractical	Rt	4.0.0	rc1	All	All
Application	Bestpractical	Rt	4.0.0	rc2	All	All
Application	Bestpractical	Rt	4.0.0	rc3	All	All
Application	Bestpractical	Rt	4.0.0	rc4	All	All
Application	Bestpractical	Rt	4.0.0	rc5	All	All
Application	Bestpractical	Rt	4.0.0	rc6	All	All
Application	Bestpractical	Rt	4.0.0	rc7	All	All
Application	Bestpractical	Rt	4.0.0	rc8	All	All
Application	Bestpractical	Rt	4.0.1	All	All	All
Application	Bestpractical	Rt	4.0.1	rc1	All	All
Application	Bestpractical	Rt	4.0.1	rc2	All	All
Application	Bestpractical	Rt	4.0.10	All	All	All
Application	Bestpractical	Rt	4.0.11	All	All	All
Application	Bestpractical	Rt	4.0.12	All	All	All
Application	Bestpractical	Rt	4.0.2	All	All	All
Application	Bestpractical	Rt	4.0.2	rc1	All	All
Application	Bestpractical	Rt	4.0.2	rc2	All	All
Application	Bestpractical	Rt	4.0.3	All	All	All
Application	Bestpractical	Rt	4.0.0	All	All	All
Application	Bestpractical	Rt	4.0.0	rc1	All	All
Application	Bestpractical	Rt	4.0.0	rc2	All	All
Application	Bestpractical	Rt	4.0.0	rc3	All	All
Application	Bestpractical	Rt	4.0.0	rc4	All	All
Application	Bestpractical	Rt	4.0.0	rc5	All	All
Application	Bestpractical	Rt	4.0.0	rc6	All	All
Application	Bestpractical	Rt	4.0.0	rc7	All	All
Application	Bestpractical	Rt	4.0.0	rc8	All	All

Application	Bestpractical	Rt	4.0.1	All	All	All
Application	Bestpractical	Rt	4.0.1	rc1	All	All
Application	Bestpractical	Rt	4.0.1	rc2	All	All
Application	Bestpractical	Rt	4.0.10	All	All	All
Application	Bestpractical	Rt	4.0.11	All	All	All
Application	Bestpractical	Rt	4.0.12	All	All	All
Application	Bestpractical	Rt	4.0.2	All	All	All
Application	Bestpractical	Rt	4.0.2	rc1	All	All
Application	Bestpractical	Rt	4.0.2	rc2	All	All
Application	Bestpractical	Rt	4.0.3	All	All	All

cpe:2.3:a:bestpractical:rt:4.0.0:*:*:*:*:*:*:*:

cpe:2.3:a:bestpractical:rt:4.0.0:rc1:*:*:*:*:*:*:

cpe:2.3:a:bestpractical:rt:4.0.0:rc2:*:*:*:*:*:*:

cpe:2.3:a:bestpractical:rt:4.0.0:rc3:*:*:*:*:*:*:

cpe:2.3:a:bestpractical:rt:4.0.0:rc4:*:*:*:*:*:*:

cpe:2.3:a:bestpractical:rt:4.0.0:rc5:*:*:*:*:*:*:

cpe:2.3:a:bestpractical:rt:4.0.0:rc6:*:*:*:*:*:*:

cpe:2.3:a:bestpractical:rt:4.0.0:rc7:*:*:*:*:*:*:

cpe:2.3:a:bestpractical:rt:4.0.0:rc8:*:*:*:*:*:*:

cpe:2.3:a:bestpractical:rt:4.0.1:*:*:*:*:*:*:*:

cpe:2.3:a:bestpractical:rt:4.0.1:rc1:*:*:*:*:*:*:

cpe:2.3:a:bestpractical:rt:4.0.1:rc2:*:*:*:*:*:*:

cpe:2.3:a:bestpractical:rt:4.0.10:*:*:*:*:*:*:*:

cpe:2.3:a:bestpractical:rt:4.0.11:*:*:*:*:*:*:*:

cpe:2.3:a:bestpractical:rt:4.0.12:*:*:*:*:*:*:*:

cpe:2.3:a:bestpractical:rt:4.0.2:*:*:*:*:*:*:*:

cpe:2.3:a:bestpractical:rt:4.0.2:rc1:*:*:*:*:*:*:

cpe:2.3:a:bestpractical:rt:4.0.2:rc2:*:*:*:*:*:*:

cpe:2.3:a:bestpractical:rt:4.0.3:*:*:*:*:*:*:*:

cpe:2.3:a:bestpractical:rt:4.0.0:*:*:*:*:*:*:*:

cpe:2.3:a:bestpractical:rt:4.0.0:rc1:*:*:*:*:*:*:

cpe:2.3:a:bestpractical:rt:4.0.0:rc1:*:*:*:*:*:*:

cpe:2.3:a:bestpractical:rt:4.0.0:rc2:*:*:*:*:*:*:

cpe:2.3:a:bestpractical:rt:4.0.0:rc3:*:*:*:*:*:*:

cpe:2.3:a:bestpractical:rt:4.0.0:rc4:*:*:*:*:*:*:

cpe:2.3:a:bestpractical:rt:4.0.0:rc5:*:*:*:*:*:*:

cpe:2.3:a:bestpractical:rt:4.0.0:rc6:*:*:*:*:*:*:

cpe:2.3:a:bestpractical:rt:4.0.0:rc7:*:*:*:*:*:*:

cpe:2.3:a:bestpractical:rt:4.0.0:rc8:*:*:*:*:*:*:

cpe:2.3:a:bestpractical:rt:4.0.1:*:*:*:*:*:*:*:

cpe:2.3:a:bestpractical:rt:4.0.1:rc1:*:*:*:*:*:*:

cpe:2.3:a:bestpractical:rt:4.0.1:rc2:*:*:*:*:*:*:

cpe:2.3:a:bestpractical:rt:4.0.10:*:*:*:*:*:*:*:

cpe:2.3:a:bestpractical:rt:4.0.11:*:*:*:*:*:*:*:

cpe:2.3:a:bestpractical:rt:4.0.12:*:*:*:*:*:*:*:

cpe:2.3:a:bestpractical:rt:4.0.2:*:*:*:*:*:*:*:

cpe:2.3:a:bestpractical:rt:4.0.2:rc1:*:*:*:*:*:*:

cpe:2.3:a:bestpractical:rt:4.0.2:rc2:*:*:*:*:*:*:

cpe:2.3:a:bestpractical:rt:4.0.3:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→