



CVE-2011-5093

Published on: 06/04/2012 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:23:17 PM UTC

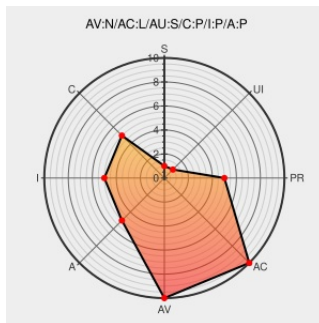
CVE-2011-5093

[Source: Mitre](#)

[Source: NIST](#)

[CVE.ORG](#)

[Print: PDF](#)



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

Best Practical Solutions RT 4.x before 4.0.6 does not properly implement the DisallowExecuteCode option, which allows remote authenticated users to bypass intended access restrictions and execute arbitrary code by leveraging access to a privileged account, a different vulnerability than CVE-2011-4458 and CVE-2011-5092.

CVE-2011-5093 has been assigned by [M](#) cve@mitre.org to track the vulnerability

CVSS2 Score: **6.5 - MEDIUM**

Access Vector

NETWORK

Access Complexity

LOW

Authentication

SINGLE

Confidentiality Impact

PARTIAL

Integrity Impact

PARTIAL

Availability Impact

PARTIAL

CVE References

Description

Tags

Link

[rt-announce] RT 4.0.6 Released - Security Release

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

[MLIST \[rt-announce\] 20120522 RT 4.0.6 Released - Security Release](#)

[rt-announce] Security vulnerabilities in RT

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

[MLIST \[rt-announce\] 20120522 Security vulnerabilities in RT](#)

[rt-announce] RT 3.8.12 Released - Security Release

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

[MLIST \[rt-announce\] 20120522 RT 3.8.12 Released - Security Release](#)

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,

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	3.8.12	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	4.0.2	All	All	All
Application	Bestpractical	Rt	4.0.3	All	All	All
Application	Bestpractical	Rt	4.0.4	All	All	All
Application	Bestpractical	Rt	4.0.5	All	All	All
Application	Bestpractical	Rt	3.8.12	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	4.0.2	All	All	All
Application	Bestpractical	Rt	4.0.3	All	All	All
Application	Bestpractical	Rt	4.0.4	All	All	All
Application	Bestpractical	Rt	4.0.5	All	All	All

Application	bestpractical	rt	4.0.0	All	All	All
cpe:2.3:a:bestpractical:rt:3.8.12:*:*:*:*:*:						
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:4.0.2:*:*:*:*:*:						
cpe:2.3:a:bestpractical:rt:4.0.3:*:*:*:*:*:						
cpe:2.3:a:bestpractical:rt:4.0.4:*:*:*:*:*:						
cpe:2.3:a:bestpractical:rt:4.0.5:*:*:*:*:*:						
cpe:2.3:a:bestpractical:rt:3.8.12:*:*:*:*:*:						
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:4.0.2:*:*:*:*:*:						
cpe:2.3:a:bestpractical:rt:4.0.3:*:*:*:*:*:						

cpe:2.3:a:bestpractical:rt:4.0.4:*:*:*:*:*:

cpe:2.3:a:bestpractical:rt:4.0.5:*:*:*:*:*:

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID→](#)

© [CVE.report](#) 2023   |

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](#)