



CVE-2013-3737

Published on: 11/15/2014 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:28:30 PM UTC

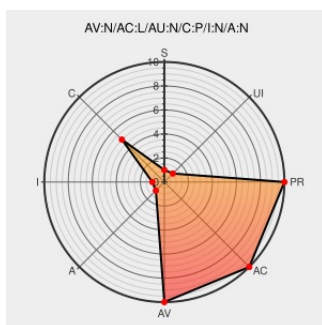
CVE-2013-3737

Source: [Mitre](#)

Source: [NIST](#)

[CVE.ORG](#)

Print: [PDF](#)



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

The MobileUI (aka RT-Extension-MobileUI) extension before 1.04 in Request Tracker (RT) 4.0.0 before 4.0.13, when using the file-based session store (Apache::Session::File) and certain authentication extensions, allows remote attackers to reuse unauthorized sessions and obtain user preferences and caches via unspecified vectors.

CVE-2013-3737 has been assigned by [M](#) cve@mitre.org to track the vulnerability

CVSS2 Score: **5 - MEDIUM**

Access
Vector

NETWORK

Access
Complexity

LOW

Authentication

NONE

Confidentiality
Impact

PARTIAL

Integrity
Impact

NONE

Availability
Impact

NONE

CVE References

Description

Tags

Link

No Description Provided

www.osvdb.org

[OSVDB 94280](#)

Inactive Link **Not Archived**

Security Advisory SA53799 - RT::Extension::MobileUI Session Re-use and Attachment Filename Script Insertion Vulnerabilities - Secunia

web.archive.org
[text/html](#)

[SECUNIA 53799](#)

[rt-announce] Security vulnerability in RT::Extension::MobileUI

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

[MLIST \[rt-announce\]](#)
20130612 Security vulnerability
in RT::Extension::MobileUI

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

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Bestpractical	Request Tracker	4.0.0	All	All	All
Application	Bestpractical	Request Tracker	4.0.1	All	All	All
Application	Bestpractical	Request Tracker	4.0.10	All	All	All
Application	Bestpractical	Request Tracker	4.0.11	All	All	All
Application	Bestpractical	Request Tracker	4.0.12	All	All	All
Application	Bestpractical	Request Tracker	4.0.2	All	All	All
Application	Bestpractical	Request Tracker	4.0.3	All	All	All
Application	Bestpractical	Request Tracker	4.0.4	All	All	All
Application	Bestpractical	Request Tracker	4.0.5	All	All	All
Application	Bestpractical	Request Tracker	4.0.6	All	All	All
Application	Bestpractical	Request Tracker	4.0.7	All	All	All
Application	Bestpractical	Request Tracker	4.0.8	All	All	All
Application	Bestpractical	Request Tracker	4.0.9	All	All	All
Application	Bestpractical	Request Tracker	4.0.0	All	All	All
Application	Bestpractical	Request Tracker	4.0.1	All	All	All
Application	Bestpractical	Request Tracker	4.0.10	All	All	All
Application	Bestpractical	Request Tracker	4.0.11	All	All	All
Application	Bestpractical	Request Tracker	4.0.12	All	All	All
Application	Bestpractical	Request Tracker	4.0.2	All	All	All
Application	Bestpractical	Request Tracker	4.0.3	All	All	All
Application	Bestpractical	Request Tracker	4.0.4	All	All	All
Application	Bestpractical	Request Tracker	4.0.5	All	All	All
Application	Bestpractical	Request Tracker	4.0.6	All	All	All
Application	Bestpractical	Request Tracker	4.0.7	All	All	All
Application	Bestpractical	Request Tracker	4.0.8	All	All	All
Application	Bestpractical	Request Tracker	4.0.9	All	All	All

```
cpe:2.3:a:bestpractical:request_tracker:4.0.0:*:*:*:*:*:*
```

```
cpe:2.3:a:bestpractical:request_tracker:4.0.1:*:*:*:*:*:*
```

```
cpe:2.3:a:bestpractical:request_tracker:4.0.10::*:~::~
```

cpe:2.3:a:bestpractical:request_tracker:4.0.11:*****:
cpe:2.3:a:bestpractical:request_tracker:4.0.12:*****:
cpe:2.3:a:bestpractical:request_tracker:4.0.2:*****:
cpe:2.3:a:bestpractical:request_tracker:4.0.3:*****:
cpe:2.3:a:bestpractical:request_tracker:4.0.4:*****:
cpe:2.3:a:bestpractical:request_tracker:4.0.5:*****:
cpe:2.3:a:bestpractical:request_tracker:4.0.6:*****:
cpe:2.3:a:bestpractical:request_tracker:4.0.7:*****:
cpe:2.3:a:bestpractical:request_tracker:4.0.8:*****:
cpe:2.3:a:bestpractical:request_tracker:4.0.9:*****:
cpe:2.3:a:bestpractical:request_tracker:4.0.0:*****:
cpe:2.3:a:bestpractical:request_tracker:4.0.1:*****:
cpe:2.3:a:bestpractical:request_tracker:4.0.10:*****:
cpe:2.3:a:bestpractical:request_tracker:4.0.11:*****:
cpe:2.3:a:bestpractical:request_tracker:4.0.12:*****:
cpe:2.3:a:bestpractical:request_tracker:4.0.2:*****:
cpe:2.3:a:bestpractical:request_tracker:4.0.3:*****:
cpe:2.3:a:bestpractical:request_tracker:4.0.4:*****:
cpe:2.3:a:bestpractical:request_tracker:4.0.5:*****:
cpe:2.3:a:bestpractical:request_tracker:4.0.6:*****:
cpe:2.3:a:bestpractical:request_tracker:4.0.7:*****:
cpe:2.3:a:bestpractical:request_tracker:4.0.8:*****:
cpe:2.3:a:bestpractical:request_tracker:4.0.9:*****:

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID →](#)

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](#)