



CVE-2010-4179

Published on: 12/07/2010 12:00:00 AM UTC

Last Modified on: 02/13/2023 04:28:00 AM UTC

CVE-2010-4179

Source: Mitre

Source: NIST

CVE.ORG

Print: PDF



Certain versions of [Enterprise Mrg](#) from [Redhat](#) contain the following vulnerability:

The installation documentation for Red Hat Enterprise Messaging, Realtime and Grid (MRG) 1.3 recommends that Condor should be configured so that the MRG Management Console (cumin) can submit jobs for users, which creates a trusted channel with insufficient access control that allows local users with the ability to publish to a broker to run jobs as arbitrary users via Condor QMF plug-ins.

CVE-2010-4179 has been assigned by secalert@redhat.com to track the vulnerability

CVSS2 Score: **7.5 - HIGH**

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
access.redhat.com CVE-2010-4179	access.redhat.com text/html	MISC access.redhat.com/security/cve/CVE-2010-4179
Support	Vendor Advisory www.redhat.com text/html	REDHAT RHSA-2010:0922
Red Hat Enterprise MRG Messaging Lets Local Users Gain Elevated Privileges - SecurityTracker	www.securitytracker.com text/html	SECTRAK 1024806
Red Hat Enterprise MRG Condor QMF Plug-ins Vulnerability - Secunia.com	Vendor Advisory web.archive.org text/html	SECUNIA 42406

Red Hat Customer Portal	access.redhat.com text/html	 MISC access.redhat.com/errata/RHSA-2010:0921
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	Vendor Advisory www.vupen.com text/html	 VUPEN ADV-2010-3091
Red Hat Customer Portal - Access to 24x7 support and knowledge	access.redhat.com text/html Inactive Link Not Archived	 MISC access.redhat.com/errata/RHSA-2010:0922
654856 – (CVE-2010-4179) CVE-2010-4179 schedd plugin: enable QUEUE_ALL_USERS_TRUSTED for Submit/Hold/Release/Remove ops	bugzilla.redhat.com text/html	 CONFIRM bugzilla.redhat.com/show_bug.cgi?id=654856
Support	Vendor Advisory www.redhat.com text/html	 REDHAT RHSA-2010:0921

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	Redhat	Enterprise Mrg	1.3	All	All	All
Operating System	Redhat	Enterprise Mrg	1.3	All	All	All
Application	Redhat	Enterprise Mrg	1.3	All	All	All
cpe:2.3:a:redhat:enterprise_mrg:1.3:*****:*						
cpe:2.3:o:redhat:enterprise_mrg:1.3:*****:*						
cpe:2.3:a:redhat:enterprise_mrg:1.3:*****:*						

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](#).

