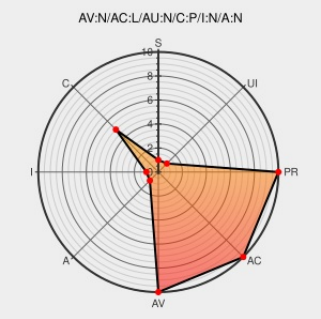
CVE-2013-6445

Published on: 04/30/2014 12:00:00 AM UTC

Last Modified on: 02/13/2023 12:08:14 AM UTC

CVE-2013-6445

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



Certain versions of Enterprise Mrg from Redhat contain the following vulnerability:

Cumin (aka MRG Management Console), as used in Red Hat Enterprise MRG 2.5, uses the DES-based crypt function to hash passwords, which makes it easier for attackers to obtain sensitive information via a brute-force attack.

CVE-2013-6445 has been assigned by secalert@redhat.com to track the vulnerability

CVSS2 Score: 5 - MEDIUM

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

CVE References

Description	Tags	Link
Red Hat Enterprise MRG Messaging Management Console Password Hashing Method Lets Local Users Recover Passwords - SecurityTracker	www.securitytracker.com, text/html	SECTRACK 1030158
Red Hat Customer Portal	Vendor Advisory, web.archive.org, text/html, Inactive Link, Not Archived	REDHAT RHSA-2014:0441
Red Hat Customer Portal	Vendor Advisory, web.archive.org, text/html, Inactive Link, Not Archived	REDHAT RHSA-2014:0440

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	2.5	All	All	All
Operating System	Redhat	Enterprise Mrg	2.5	All	All	All
Application	Redhat	Enterprise Mrg	2.5	All	All	All

cpe:2.3:a:redhat:enterprise_mrg:2.5:*:*:*:*:*:*:*:

cpe:2.3:o:redhat:enterprise_mrg:2.5:*:*:*:*:*:*:*:

cpe:2.3:a:redhat:enterprise_mrg:2.5:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→