



# CVE-2010-2492

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064\_img.jpg\)](#)

## Summary

|                        |   |
|------------------------|---|
| <b>CVE</b>             | CVE-2010-2492   |
| <b>State</b>           | PUBLIC  |
| <b>Assigner</b>        | secalert@redhat.com   |
| <b>Source Priority</b> | CVE Program / NVD first with legacy fallback  |
| <b>Published</b>       | 2010-09-08 20:00:00 UTC   |
| <b>Updated</b>         | 2023-02-13 03:15:00 UTC   |
| <b>Description</b>     | Buffer overflow in the ecryptfs_uid_hash macro in fs/ecryptfs/messaging.c in the eCryptfs subsystem in the Linux kernel bef |

## Risk And Classification

**Problem Types:** CWE-120

## NVD Known Affected Configurations (CPE 2.3)

| Type        | Vendor | Product                    | Version | Update | Edition | Language |
|-------------|--------|----------------------------|---------|--------|---------|----------|
| Application | Avaya  | Aura Communication Manager | 5.2     | All    | All     | All      |
| Application | Avaya  | Aura Communication Manager | 5.2     | All    | All     | All      |
| Application | Avaya  | Aura Presence Services     | 6.0     | All    | All     | All      |
| Application | Avaya  | Aura Presence Services     | 6.1     | All    | All     | All      |
| Application | Avaya  | Aura Presence Services     | 6.1.1   | All    | All     | All      |
| Application | Avaya  | Aura Presence Services     | 6.0     | All    | All     | All      |
| Application | Avaya  | Aura Presence Services     | 6.1     | All    | All     | All      |
| Application | Avaya  | Aura Presence Services     | 6.1.1   | All    | All     | All      |
| Application | Avaya  | Aura Session Manager       | 1.1     | All    | All     | All      |
| Application | Avaya  | Aura Session Manager       | 5.2     | All    | All     | All      |
| Application | Avaya  | Aura Session Manager       | 6.0     | All    | All     | All      |
| Application | Avaya  | Aura Session Manager       | 1.1     | All    | All     | All      |
| Application | Avaya  | Aura Session Manager       | 5.2     | All    | All     | All      |
| Application | Avaya  | Aura Session Manager       | 6.0     | All    | All     | All      |
| Application | Avaya  | Aura System Manager        | 5.2     | All    | All     | All      |
| Application | Avaya  | Aura System Manager        | 6.0     | All    | All     | All      |
| Application | Avaya  | Aura System Manager        | 6.1     | All    | All     | All      |

|                  |        |                      |       |     |     |     |
|------------------|--------|----------------------|-------|-----|-----|-----|
| Application      | Avaya  | Aura System Manager  | 6.1.1 | All | All | All |
| Application      | Avaya  | Aura System Manager  | 5.2   | All | All | All |
| Application      | Avaya  | Aura System Manager  | 6.0   | All | All | All |
| Application      | Avaya  | Aura System Manager  | 6.1   | All | All | All |
| Application      | Avaya  | Aura System Manager  | 6.1.1 | All | All | All |
| Application      | Avaya  | Aura System Platform | 1.1   | All | All | All |
| Application      | Avaya  | Aura System Platform | 6.0   | -   | All | All |
| Application      | Avaya  | Aura System Platform | 6.0   | sp1 | All | All |
| Application      | Avaya  | Aura System Platform | 1.1   | All | All | All |
| Application      | Avaya  | Aura System Platform | 6.0   | -   | All | All |
| Application      | Avaya  | Aura System Platform | 6.0   | sp1 | All | All |
| Application      | Avaya  | Aura Voice Portal    | 5.0   | All | All | All |
| Application      | Avaya  | Aura Voice Portal    | 5.1   | -   | All | All |
| Application      | Avaya  | Aura Voice Portal    | 5.1   | sp1 | All | All |
| Application      | Avaya  | Aura Voice Portal    | 5.0   | All | All | All |
| Application      | Avaya  | Aura Voice Portal    | 5.1   | -   | All | All |
| Application      | Avaya  | Aura Voice Portal    | 5.1   | sp1 | All | All |
| Application      | Avaya  | Iq                   | 5.0   | All | All | All |
| Application      | Avaya  | Iq                   | 5.1   | All | All | All |
| Application      | Avaya  | Iq                   | 5.0   | All | All | All |
| Application      | Avaya  | Iq                   | 5.1   | All | All | All |
| Operating System | Linux  | Linux Kernel         | All   | All | All | All |
| Operating System | Linux  | Linux Kernel         | All   | All | All | All |
| Operating System | Vmware | Esx                  | 4.0   | All | All | All |
| Operating System | Vmware | Esx                  | 4.1   | All | All | All |
| Operating System | Vmware | Esx                  | 4.0   | All | All | All |
| Operating System | Vmware | Esx                  | 4.1   | All | All | All |

## References

| Reference  | Source   | Link   | Tags                     |
|--|----------|--|--------------------------|
| 404: File not found  | CONFIRM  | <a href="http://www.kernel.org">www.kernel.org</a>       | Broken Link              |
| Support / Security / Advisories // MDVSA-2010:172   Mandriva | MANDRIVA | <a href="http://www.mandriva.com">www.mandriva.com</a>   | Broken Link              |
| Red Hat Customer Portal                                      | MISC     | <a href="http://access.redhat.com">access.redhat.com</a> |                          |
| Red Hat Customer Portal                                      | MISC     | <a href="http://access.redhat.com">access.redhat.com</a> |                          |
| kernel/git/torvalds/linux.git - Linux kernel source tree     | CONFIRM  | <a href="http://git.kernel.org">git.kernel.org</a>       | Mailing List, Patch, Ven |

|  |          |  |                                      |
|--|----------|--|--------------------------------------|
| SecurityFocus  | BUGTHAQ  | <a href="http://www.securityfocus.com">www.securityfocus.com</a> | Third Party Advisory, Vulnerability  |
| Bug 611385 – CVE-2010-2492 kernel: ecryptfs_uid_hash() buffer overflow                                       | CONFIRM  | <a href="http://bugzilla.redhat.com">bugzilla.redhat.com</a>     | Issue Tracking, Patch, Vulnerability |
| Support / Security / Advisories // MDVSA-2010:198   Mandriva   | MANDRIVA | <a href="http://www.mandriva.com">www.mandriva.com</a>           | Broken Link                          |
| <a href="http://access.redhat.com">access.redhat.com</a>   CVE-2010-2492                                     | MISC     | <a href="http://access.redhat.com">access.redhat.com</a>         |                                      |
| <a href="https://kernel/git/torvalds/linux.git">kernel/git/torvalds/linux.git</a> - Linux kernel source tree | MISC     | <a href="https://git.kernel.org">git.kernel.org</a>              |                                      |
| ASA-2010-291 (RHSAs-2010-0723)   | CONFIRM  | <a href="http://support.avaya.com">support.avaya.com</a>         | Third Party Advisory                 |
| VMSA-2011-0012.2   | CONFIRM  | <a href="http://www.vmware.com">www.vmware.com</a>               | Patch, Third Party Advisory          |
| Support  | REDHAT   | <a href="http://www.redhat.com">www.redhat.com</a>               | Broken Link                          |
| Red Hat update for kernel - Advisories - Community   | SECUNIA  | <a href="http://secunia.com">secunia.com</a>                     | Broken Link                          |
| About Secunia Research   Flexera   | SECUNIA  | <a href="http://secunia.com">secunia.com</a>                     | Broken Link                          |
| <a href="http://access.redhat.com">access.redhat.com</a>   | REDHAT   | <a href="http://www.redhat.com">www.redhat.com</a>               | Broken Link                          |
| CVE Program record   | CVE.ORG  | <a href="http://www.cve.org">www.cve.org</a>                     | canonical                            |
| NVD vulnerability detail   | NVD      | <a href="http://nvd.nist.gov">nvd.nist.gov</a>                   | canonical, analysis                  |

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

© [CVE.report](http://CVE.report) 2026 |

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](http://The MITRE Corporation) and the authoritative source of CVE content is [MITRE's CVE web site](http://MITRE's CVE web site). This site includes MITRE data granted under the following [license](http://license).

**CVE.report and Source URL Uptime Status** [status.cve.report](http://status.cve.report)