

## 1. Synopsis

A standard structure that gives the reader the package name, the errata type and, in the case of security errata, the severity. The example note is a condor update that includes moderate security fixes, bug fixes and enhancements (new features).

There are three Advisory types:

Red Hat Security Advisory	RHSA
Red Hat Bug Fix Advisory	RHBA
Red Hat Enhancement Advisory	RHEA

But there are eight Synopses types:

RHSA: <i>security update</i>
RHSA: <i>security &amp; bug fix update</i>
RHSA: <i>security, bug fix &amp; enhancement update</i>
RHBA: <i>bug fix update</i>
RHBA: <i>bug fix &amp; enhancement update</i>
RHEA: <i>enhancement update</i>
RHEA: <i>new package</i>

The Advisory type is always the most severe of any of the Synopses types. If the update includes bug fixes and enhancements, it's an RHBA, even if there's one bug fix and a dozen new features.

If there is a security fix in the update, it's an RHSA. RHSAs do **not** generally contain other changes. As the example shows, exceptions exist.

The structure of a Synopsis is pretty simple.

RHSA: [severity]: [package] security update
RHBA: [package] bug fix update
RHEA: [package] enhancement update
RHEA: new package: [package-name]

Replace [package] with the package name, not the application name (*httpd* not *Apache*). Version numbers are not included.

Replace [severity] with whichever of the following the Red Hat Security Response Team (RHST) directs: critical, important, moderate, low.

If an update includes more than one sort of change, the Synopsis should reflect this, presenting the change types in order of importance, as per the example.

An RHBA with enhancements is

[package] bug fix & enhancement update
--

An RHSA with bug fixes is

[severity]: [package] security & bug fix update
---

An RHSA with bug fixes and enhancements is as per the example.

RHEAs are always either just enhancements or new packages. And new package means just that. Re-basing on upstream or major updates aren't new packages. Unless it's never been available before, it's not a new package.

## 2. Topic

A slightly longer version of the synopsis consisting of one or two complete sentences. RHBA and RHEA errata require one sentence; RHSA errata require two. The following Topic boilerplates are organised by errata type, package number and, in the case of security notes, whether or not the released package is a synchronous or asynchronous update.

RHBA, single package:

An updated [package] package that fixes [a   various] [bug   bugs] is now available.
--

RHBA, multiple packages:

Updated [package] packages that fix [a   various] [bug   bugs] are now available.
---

RHEA, single package

[A   An] [new   enhanced] [package] package is now available.
---

RHEA, multiple packages

[New   Enhanced] [package] packages are now available.
--

Synchronous RHSA (released as part of a regular update), multiple packages

Updated [package] packages] are now available as part of ongoing support and maintenance of [product] [version/s] . This is the [ordinal] regular update.
---

This update has been rated as having [severity] security impact by the Red Hat Security Response Team.
--

Asynchronous RHSA (released in between regular updates), single package

An updated [package] package that fixes [type of security issue] is now available for [product] [version/s].
--

This update has been rated as having [severity] security impact by the Red Hat Security Response Team.
--

Choose the singular or plural according to the number of RPM packages included for any *single* architecture. NB: source, devel and debuginfo packages are not counted when deciding if an errata release contains multiple packages.

Note, the RHSA boilerplates above don't explicitly include single package Synchronous RHSAs or multiple package Asynchronous RHSAs. These do exist, of course, and the appropriate pronouns should be used for each circumstance.

As in the Synopsis, replace [severity] with one of the following: critical, important, moderate, low.

Replace [product] with, unsurprisingly, the product name. Replace [version/s] with the appropriate version number or version numbers if the update is for multiple versions of a product (eg Red Hat Enterprise Linux 3, 4, and 5).

## 3. Problem Description opening

This field has three parts: boilerplate opening and closing paragraphs and a middle section, which is where the real writing happens.

The opening paragraph is the "what is it" text. We deal with package names all day; don't assume this is routine for others. Just because you know *initscripts* includes the basic scripts used to boot a system, change runlevels, and shut the system down cleanly, doesn't mean everyone else does.

The primary source for this text is the %description field in a package's .spec file. If a package is installed on your system, retrieve the text using the following command:

```
$ rpm -qi <package name>
```

Alternatively, download the src rpm from Brew, extract [package].spec from said rpm and copy-and-paste into the errata tool.

If you encounter a poorly-written %description (and you will), re-write it for the current errata and file your improved text as a bug against the package.

## 4. Problem Description closing

The closing paragraph is the "what to do" paragraph. This section directs the user to take action or possibly directs them to think about whether they should take action. Watch out for the singular/plural pitfall with both the number of packages and the number of issues addressed.

# Moderate: condor security, bug fix and enhancement update

<b>Advisory:</b>	RHSA-2008:0911-12
<b>Type:</b>	Security Advisory
<b>Severity:</b>	Moderate
<b>Issued on:</b>	2008-10-07
<b>Last updated on:</b>	2008-10-07
<b>Affected Products:</b>	<a href="#">Red Hat Enterprise MRG v1 for Red Hat Enterprise Linux (version 5)</a>
<b>OVAL:</b>	N/A
<b>CVEs (cve.mitre.org):</b>	<a href="#">CVE-2008-3826</a> <a href="#">CVE-2008-3828</a> <a href="#">CVE-2008-3829</a> <a href="#">CVE-2008-3830</a>

## Details

Updated condor packages that address multiple security issues, fix several bugs, and introduce feature enhancements are now available for Red Hat Enterprise MRG 1.0 for Red Hat Enterprise Linux 5.

This update has been rated as having moderate security impact by the Red Hat Security Response Team.

Condor is a specialized workload management system for compute-intensive jobs. It provides a job queuing mechanism, scheduling policy, priority scheme, and resource monitoring and management.

A flaw was found in the way Condor processed user submitted jobs. It was possible for a user to submit a job in a way that could cause that job to run as a different user with access to the pool. (CVE-2008-3826)

A stack based buffer overflow flaw was found in Condor's condor\_schedd daemon. A user who had permissions to submit a job could do so in a manner that could cause condor\_schedd to crash or, potentially, execute arbitrary code with the permissions of condor\_schedd. (CVE-2008-3828)

A denial-of-service flaw was found in Condor's condor\_schedd daemon. A user who had permissions to submit a job could do so in a manner that would cause condor\_schedd to crash. (CVE-2008-3829)

A flaw was found in the way Condor processes allowed and denied netmasks for access control. If a configuration file contained an overlapping netmask in the allow or deny rules, it could cause that rule to be ignored, allowing unintended access. (CVE-2008-3830)

This update also fixes the following bugs:

\* the "amazon\_gahp -m" command sets the AMAZON\_GAHP\_WORKER\_MAX\_NUM configuration option, fixing the maximum number of processes contacting EC2 at any given time. Previously, Condor did not honor this option, leaving the maximum number of created threads unbounded. This has been corrected: values set with the "-m" argument are now properly understood. (BZ#451069)

\* the gridmanager constructed KeyPairs for all outstanding EC2 jobs before any jobs are started. When there were many (>10,000) EC2 jobs in the queue, significant delays occurred. With this update, KeyPairs are no longer constructed up-front. (BZ#451799)

\* an error in condor\_negotiator caused initialization code to re-run whenever condor\_reconfig was run. The flag which noted if the initialization code should run was always set to "true". This error has been corrected: the initialization code now executes only at startup. (BZ#459891)

As well, this update adds the following enhancements:

\* this release introduces Concurrency Limits. These allow Condor to account for resources not directly under its control, such as software licenses. (BZ#459897)

\* base support for low-latency scheduling and transparent translation of EC2 jobs has also been added in this update. Note: implementation of these two features depends on separate packages which are yet to be released. (BZ#462662)

Note: this update includes the latest stable upstream release of Condor: version 7.0.5. Information on the features and fixes included with this release are in the Condor Release Notes, available via the link in the References section below.

All Red Hat Enterprise MRG 1.0 users are advised to upgrade to these updated packages which address these vulnerabilities, fix these bugs and add these enhancements.

## Solution

Before applying this update, make sure that all previously-released errata relevant to your system have been applied.

This update is available via Red Hat Network. Details on how to use the Red Hat Network to apply this update are available at [http://kbase.redhat.com/faq/FAQ\\_58\\_10188](http://kbase.redhat.com/faq/FAQ_58_10188)

## Updated packages

### Red Hat Enterprise MRG v1 for Red Hat Enterprise Linux (version 5)

<b>SRPMS:</b>		
condor-7.0.5-2.el5.src.rpm		c6b9e714f8c447f9e61c7b7f9ede684c0

<b>IA-32:</b>		
condor-7.0.5-2.el5.i386.rpm		fa60e67437f32a61df67a534dc163c0b

condor-static-7.0.5-2.el5.i386.rpm		5176f0a95d70f1c1058e03a03e156af9
------------------------------------	--	----------------------------------

<b>x86_64:</b>		
condor-7.0.5-2.el5.x86_64.rpm		5bd359ef59a54ae758aa32d6a0493ae7

condor-static-7.0.5-2.el5.x86_64.rpm		7f42d8d06e70a700e44790cd5c57b9e2
--------------------------------------	--	----------------------------------

(The unlinked packages above are only available from the [Red Hat Network](#))

## Bugs fixed (see [bugzilla](#) for more information)

[451069](#) - gSOAP amazon-gahp needs max to worker pool

[451799](#) - upfront construction of ec2 KeyPairs is time consuming

[462662](#) - SetAttribute does not check validity of attribute's name

[463987](#) - CVE-2008-3826 condor: users can run jobs with arbitrary owners

[463990](#) - CVE-2008-3828 condor: buffer overflow in lookup\_macro

[463995](#) - CVE-2008-3829 condor: denial of service attack on Schedd via corrupt logfile

[463997](#) - CVE-2008-3830 condor: allow or deny with overlapping netmasks may be ignored

## References

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-3826>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-3828>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-3829>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-3830>

<http://www.redhat.com/security/updates/classification/#moderate>

[http://cs.wisc.edu/condor/manual/v7.0/8\\_3Stable\\_Release.html](http://cs.wisc.edu/condor/manual/v7.0/8_3Stable_Release.html)

These packages are GPG signed by Red Hat for security. Our key and details on how to verify the signature are available from: <https://www.redhat.com/security/team/key/#package>

The Red Hat security contact is [secalert@redhat.com](mailto:secalert@redhat.com). More contact details at <http://www.redhat.com/security/team/contact/>

---

Copyright © 2008 Red Hat, Inc. All rights reserved. [Privacy statement](#) : [Legal statement](#) : [redhat.com](#)  
Red Hat Network release 5.0.8

field and we've hit that limit more than once when attempting to document every fix and every change in a package.

This is not a carte blanche for adding 'more info here' to errata. Character limits aside, this is a judgement call, and you should err on the side of putting information into the note when possible.

The core boilerplate for this paragraph is as follows:

Users are advised to upgrade to [this   these] updated [package   packages], which [resolves   resolve] [this   these] [issue   issues].
--

Standard variations on this boilerplate include:

All users are advised to upgrade to these updated gcc packages, which contain a backported fix and are not vulnerable to this issue.
--

Users should upgrade to this updated package, which resolves these issues.
--

All users requiring ksh should install this new package, which adds this enhancement.
---

Although Red Hat Enterprise Linux shipped with a version of mod_python that contains this bug, our testing was unable to trigger the denial of service vulnerability. However, mod_python users are advised to upgrade to these errata packages, which contain a backported patch that corrects this bug.
---

Users of Red Hat Enterprise Linux 2.1 are advised to upgrade to these erratum packages, which contain a backported security patch and are not vulnerable to these issues. Please note that Red Hat Enterprise Linux 3 does not contain Metamail and is therefore not vulnerable to these issues.
--

The third variation above gives the accepted boilerplate for the special case of new packages. The fourth and fifth examples show how to direct customers to determine if their environment is one that requires action or not.

Only include directions concerning restarting daemons, modifying config files and the like if they are absolutely required for an erratum install to succeed.

If installing an erratum requires a system re-boot before the effects of the erratum are functional on said system, this constitutes an absolute requirement for the erratum install to succeed. Consequently, it must be documented.

Boilerplate for instances where a system re-start is required are offered below. With tweaking they can be used for other instances of required further action (eg when a service needs to be restarted).

After installing this erratum, a system re-boot is required to effect the changes noted above.
--

Installing this erratum does not, of itself, close this vulnerability. The issue addressed in this erratum remains open until the system is re-booted. To ensure this vulnerability is closed, the system should be re-booted immediately the erratum is installed.
---

Installing this erratum does not, of itself, close the [brief summary of a particular security problem] vulnerability. That issue remains open until the system is re-booted. To close this, the system should be re-booted immediately the erratum is installed.
---

One of the fixes included with this update requires a system re-boot before the change documented above goes in to effect.
--

A system re-boot is recommended after installing this update. The [summary of the particular bug fix] requires a system re-boot before coming in to effect.
---

## 5. Problem Description middle

The heart of an errata note: the middle section of a Problem Description. This section consists of a series of paragraphs, each one describing fully but succinctly the changes introduced by the updated package and the reasons for the change.

These paragraphs are structured using the **four words to live by**.

<i>cause:</i>	what actions or circumstances cause the bug to present
---------------	--

<i>consequence:</i>	what happens when the bug presents
---------------------	------------------------------------

<i>fix:</i>	what was done to fix the bug
-------------	------------------------------

<i>result:</i>	what now happens when the actions or circumstances occur
----------------	--

NB: this last is not the same as 'the bug doesn't present anymore'.

Examples are more helpful than abstract descriptions, so use the example note here; the example note provided in the Errata Writing Test; and the thousands of real-world examples in the errata tool as your guide.

## 5a. CVE & BZ numbers

In brackets after each documented change (and after the final full-stop) is the CVE or BZ number of the change. The RHST are responsible for CVE numbers but we are (currently) responsible for the BZ numbers.

## 6. References

RHSAs include links to the appropriate CVE documentation and a link to our severity classification documentation by default.

In general, other "for more information" directions (directing customers to read files or browse URLs) should not be included here. If it's worth directing them to an external information source, it's worth including that information in the erratum.

That said, there are occasions where a reference or link to an external information source is acceptable. For example, when an updated package includes dozens of changes. We have a 4,000 character limit in the Problem Description

field and we've hit that limit more than once when attempting to document every fix and every change in a package.

This is not a carte blanche for adding 'more info here' to errata. Character limits aside, this is a judgement call, and you should err on the side of putting information into the note when possible.