FOLLOW US:
TWITTER.COM/REDDHATSUMMIT

TWEET ABOUT US:
ADD #SUMMIT AND/OR #JBOSSWORLD TO THE END OF YOUR EVENT-RELATED TWEET
Today's Topics

What is a security flaw?
What is an RHSA
What gets fixed
How can I find more information about security flaws
The world today

Security cannot be ignored

Threats

Crackers
Worms
Botnets
Phishers
Spammers
Security Bugs

All software has bugs

Some of these bugs have security implications

What's the difference?

Not all software is written equally

Code quality differs between projects
Examples

Image file that crashes the image viewer
  Bug (just don't open it again)
Image file that zips up your home directory and mails it to the bad guys
  Security flaw
Crash the computer with a network packet
  Security flaw
Crash the computer by smashing it with a hammer
  Not a security flaw (probably not a bug either)
Organizing our bugs

Every security issue gets a CVE id
Not all CVE ids are security issues
  Vendor disputes
    MITRE is often quite liberal with CVE assignment
Not every CVE id affects us
Deciding what to fix

We have a set of issues
  Some new, some old
Fix it now?
Fix it later?

We have finite resources, flaws must be prioritized and dealt with in a sensible order
Bug Severities

“unlikely circumstances .. or where a successful exploit would lead to minimal consequences”
Bug Severities

“harder or more unlikely to be exploitable”
Bug Severities

“easily compromise the Confidentiality, Integrity or Availability of resources”
Bug Severities

- Critical
- Important
- Moderate
- Low

“A vulnerability whose exploitation could allow the propagation of an Internet worm without user action.”
How do we fix it?

Backport the patch

Upgrade

This is not common

The update is bundled in a security advisory
How Does Backporting Work?

Apache httpd 2.0.54

NEW!

Enterprise Linux 4
httpd-2.0.52-12.ent

httpd-2.0.52-12.1.ent
RHSA-2005:582

httpd-2.0.52-12.2.ent
RHSA-2005:608

Apache httpd 2.0.55
What is an RHSA?

**Red Hat Security Advisory**

Special Errata that fix security flaws
- Sometimes bugs too

Released when an update is ready
- No pre-defined update schedule
What's in an RHSA?

Header
Details
Solution
Updated Packages
Bugs Fixed
References
Important: bind security update

Advisory: RHSA-2009:1179-2

Type: Security Advisory

Severity: Important

Issued on: 2009-07-29

Last updated on: 2009-07-29

Affected Products:
- RHEL Desktop Workstation (v. 5 client)
- Red Hat Enterprise Linux (v. 5 server)
- Red Hat Enterprise Linux Desktop (v. 5 client)
- Red Hat Enterprise Linux EUS (v. 5.3.2 server)

OVAL: com.redhat.rhsa-20091179.xml

CVEs (cve.mitre.org): CVE-2009-0696

Details

Updated bind packages that fix a security issue are now available for Red Hat Enterprise Linux 5.

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

Updated bind packages that fix a security issue are now available for Red Hat Enterprise Linux 5.

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

[Updated 29th July 2009]
The packages in this erratum have been updated to also correct this issue in the bind-sdb package.

The Berkeley Internet Name Domain (BIND) is an implementation of the Domain Name System (DNS) protocols. BIND includes a DNS server (named), a resolver library (routines for applications to use when interfacing with DNS); and tools for verifying that the DNS server is operating correctly.

A flaw was found in the way BIND handles dynamic update message packets containing the "ANY" record type. A remote attacker could use this flaw to send a specially-crafted dynamic update packet that could cause named to exit with an assertion failure. (CVE-2009-0696)

Note: even if named is not configured for dynamic updates, receiving such a specially-crafted dynamic update packet could still cause named to exit unexpectedly.

All BIND users are advised to upgrade to these updated packages, which contain a backported patch to resolve this issue. After installing the update, the BIND daemon (named) will be restarted automatically.

Solution

Before applying this update, make sure that all previously released...
Solution

Note: even if named is not configured for dynamic updates, receiving such a specially-crafted dynamic update packet could still cause named to exit unexpectedly.

All BIND users are advised to upgrade to these updated packages, which contain a backported patch to resolve this issue. After installing the update, the BIND daemon (named) will be restarted automatically.

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/docs/DOC-11259

Updated packages

RHEL Desktop Workstation (v. 5 client)

SRPMS:

bind-9.3.4-10.P1.el5_3.3.src.rpm 217 cb2f 652a6f b555 ebb5 5b052460f43

IA-32:

bind-chroot-9.3.4-10.P1.el5_3.3.i386.rpm 8aa7c2a7eece72ce6af1826dbf693cba
bind-devel-9.3.4-10.P1.el5_3.3.i386.rpm 0cdec1e23d7ed5e19e65a6bf9c58c
bind-devel-9.3.4-10.P1.el5_3.3.i386
bind-devel-9.3.4-10.P1.el5_3.3.i386
bind-devel-9.3.4-10.P1.el5_3.3.i386
## Updated Packages

**RHEL Desktop Workstation (v. 5 client)**

<table>
<thead>
<tr>
<th>SRPMS:</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>bind-9.3.4-10.P1.el5_3.3.src.rpm</td>
<td>217cb2f652a6fb555eb59b992460f13</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>IA-32:</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>bind-chroot-9.3.4-10.P1.el5_3.3.i386.rpm</td>
<td>8aa7c2a7e2c726e6af1826dbf653cbb</td>
</tr>
<tr>
<td>bind-devel-9.3.4-10.P1.el5_3.3.i386.rpm</td>
<td>0cdec1e623b7ed59d19e03a6bf9c58c</td>
</tr>
<tr>
<td>bind-libbind-devel-9.3.4-10.P1.el5_3.3.i386.rpm</td>
<td>4c9faa3681c8163d18bfba8bf0e587f</td>
</tr>
<tr>
<td>caching-nameserver-9.3.4-10.P1.el5_3.3.i386.rpm</td>
<td>89b5bf65d8815851ab469793b156a2</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>x86_64:</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>bind-chroot-9.3.4-10.P1.el5_3.3.x86_64.rpm</td>
<td>94c2fcd37bd404e04e0e9c40cole4eb71</td>
</tr>
<tr>
<td>bind-devel-9.3.4-10.P1.el5_3.3.i386.rpm</td>
<td>0cdec1e623b7ed59d19e03a6bf9c58c</td>
</tr>
<tr>
<td>bind-devel-9.3.4-10.P1.el5_3.3.x86_64.rpm</td>
<td>610e77b48a6cc05c173a6ad65b718</td>
</tr>
<tr>
<td>bind-libbind-devel-9.3.4-10.P1.el5_3.3.i386.rpm</td>
<td>4c9faa3681c8163d18bfba8bf0e587f</td>
</tr>
<tr>
<td>bind-libbind-devel-9.3.4-10.P1.el5_3.3.x86_64.rpm</td>
<td>a691ff311c9bad968b2812888fedef</td>
</tr>
<tr>
<td>caching-nameserver-9.3.4-10.P1.el5_3.3.x86_64.rpm</td>
<td>776560f3a7844abc741785ec5da874bfe</td>
</tr>
</tbody>
</table>
Bugs Fixed

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

Bugs fixed (see bugzilla for more information)

514292 - CVE-2009-0696 bind: DoS (assertion failure) via nsupdate packets

References

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-0696
http://www.redhat.com/security/updates/classification/#important
https://www.isc.org/node/474

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. More contact details at http://www.redhat.com/security/team/contact/
References

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

Bugs fixed (see bugzilla for more information)

514292 - CVE-2009-0696 bind: DoS (assertion failure) via nsupdate packets

References

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-0696
http://www.redhat.com/security/updates/classification/#important
https://www.isc.org/node/474

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. More contact details at http://www.redhat.com/security/team/contact/
Mining for CVE data

What happens if I want information on a specific CVE id?
Old Way

Our previous instructions were quite manual
Multiple locations had to be checked
Does an issue affect Red Hat?

Get the CVE name and use RHN
see if we've issued an update already

CVE-2008-0072

Updated packages to correct this issue are available along with our advisory at the URLs below. Users of the Red Hat Network can update their systems using the 'up2date' tool.

Red Hat Enterprise Linux:

Perhaps it doesn't affect us, try NVD

https://nvd.nist.gov/nvd.cfm?cvname=CVE-2008-2420

Vendor Statements (disclaimer)

Official Statement from Red Hat (5/26/2008)
Not vulnerable. OCSP protocol support was only implemented in upstream stunnel version 4.16. Therefore OCSP protocol is not available in the versions of stunnel as shipped with Red Hat Enterprise Linux 2.1, 3, 4, or 5.
Bugzilla Bug 448290: CVE-2008-2420 stunnel: incorrect CRL verification using OCSP

Common Vulnerabilities and Exposures assigned an identifier CVE-2008-2420 to the following vulnerability:

The OCSP functionality in stunnel before 4.24 does not properly search certificate revocation lists (CRL), which allows remote attackers to bypass intended access restrictions by using revoked certificates.

References:
http://stunnel.mirt.net/pipermail/stunnel-announce/2008-May/000035.html
http://www.securityfocus.com/bid/29309
http://secunia.com/advisories/30335
http://xforce.iss.net/xforce/xfdb/42528

This issue does not affect versions of stunnel as shipped in Red Hat Enterprise Linux 2.1, 3, 4 and 5. Support for OCSP protocol was only implemented in
New Way

http://www.redhat.com/security/data/cve
CVE-2009-2408

**Impact:** Important (classification)

**Public:** July 29 2009

**Bugzilla:** 510751: CVE-2009-2408 firefox/nss: doesn't handle NULL in Common Name properly

**Details**

The MITRE CVE dictionary describes this issue as:

Mozilla Firefox before 3.5 and NSS before 3.12.3 do not properly handle a `\0` character in a domain name in the subject's Common Name (CN) field of an X.509 certificate, which allows man-in-the-middle attackers to spoof arbitrary SSL servers via a crafted certificate issued by a legitimate Certification Authority.

Find out more about CVE-2009-2408 from the [MITRE CVE dictionary](http://cve.mitre.org) and [NIST NVD](http://cvedetails.com).

**CVSS v2 metrics**

<table>
<thead>
<tr>
<th>Base Score</th>
<th>4.3</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access Vector</td>
<td>Network</td>
</tr>
<tr>
<td>Access Complexity</td>
<td>Medium</td>
</tr>
<tr>
<td>Authentication</td>
<td>None</td>
</tr>
<tr>
<td>Base Metrics:</td>
<td>AV:N/AC:M/Au:N/C:N/I:P/A:N</td>
</tr>
<tr>
<td>Confidentiality Impact</td>
<td>None</td>
</tr>
<tr>
<td>Integrity Impact</td>
<td>Partial</td>
</tr>
<tr>
<td>Availability Impact</td>
<td>None</td>
</tr>
</tbody>
</table>

Find out more about [Red Hat support for the Common Vulnerability Scoring System (CVSS)](http://access.redhat.com/security/adv/CVSS)

**Red Hat security errata**

<table>
<thead>
<tr>
<th>Platform</th>
<th>Errata</th>
<th>Release Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Red Hat Enterprise Linux version 4</td>
<td>RHSA-2009:1184</td>
<td>July 30 2009</td>
</tr>
<tr>
<td>Red Hat Enterprise Linux version 5</td>
<td>RHSA-2009:1186</td>
<td>July 30 2009</td>
</tr>
<tr>
<td>Red Hat Enterprise Linux version 4.7.z</td>
<td>RHSA-2009:1190</td>
<td>July 31 2009</td>
</tr>
</tbody>
</table>
CVE-2009-2689

Details

The MITRE CVE dictionary describes this issue as:

** RESERVED ** This candidate has been reserved by an organization or individual that will use it when announcing a new security problem. When the candidate has been publicized, the details for this candidate will be provided.

Find out more about CVE-2009-2689 from the MITRE CVE dictionary and NIST NVD.

Red Hat security errata

<table>
<thead>
<tr>
<th>Platform</th>
<th>Errata</th>
<th>Release Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Red Hat Enterprise Linux version 4 Extras (java-1.5.0-sun)</td>
<td>RHSA-2009-1199</td>
<td>August 06 2009</td>
</tr>
<tr>
<td>RHEL Supplementary version 5 (java-1.5.0-sun)</td>
<td>RHSA-2009-1199</td>
<td>August 06 2009</td>
</tr>
<tr>
<td>Red Hat Enterprise Linux version 5 (java-1.6.0-openjdk)</td>
<td>RHSA-2009-1201</td>
<td>August 06 2009</td>
</tr>
</tbody>
</table>
CVE-2009-1630

**Impact:** Moderate

**Public:** May 09 2009

**Bugzilla:** 500297: CVE-2009-1630 kernel: nfs: fix NFS v4 client handling of MAY EXEC in nfs_permission

**Details**

The MITRE CVE dictionary describes this issue as:

The nfs_permission function in fs/nfs/dir.c in the NFS client implementation in the Linux kernel 2.6.29.3 and earlier, when atomic_open is available, does not check execute (aka EXEC or MAY_EXEC) permission bits, which allows local users to bypass permissions and execute files, as demonstrated by files on an NFSv4 fileserver.

Find out more about CVE-2009-1630 from the [MITRE CVE dictionary](https://www.cve.mitre.org) and [NIST NVD](https://nvd.nist.gov).

**Statement**

Red Hat has provided the following NVD statement on the NIST website:

Red Hat is aware of this issue and is tracking it via the following bug: [https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=CVE-2009-1630](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=CVE-2009-1630)

This issue did not affect the versions of Linux kernel as shipped with Red Hat Enterprise Linux 2.1, and 3.

It was addressed in Red Hat Enterprise MRG via: [https://rhn.redhat.com/errata/RHSA-2009-1157.html](https://rhn.redhat.com/errata/RHSA-2009-1157.html)

Future kernel updates in Red Hat Enterprise Linux 4 and 5 will address this flaw.
Passive Notification

Red Hat Network will notify you of updates needed to packages installed on your systems

By email if you enable it
By up2date/pup
By logging in

Cuts down the number of alerts to those that affect your installation

Subscribing to enterprise-watch-list@redhat.com
or rhsa-announce@redhat.com

From the web https://rhn.redhat.com/errata/

RSS feed
QUESTIONS?
TELL US WHAT YOU THINK:
REDHAT.COM/SUMMIT-SURVEY