



Security Response and Vendor Accountability

LinuxWorld 2003

Mark J Cox

Security Response Team

revision 3

www.awe.com/mark/lw2003



Response and Accountability

- Peeking inside Apache
 - *Security is more than the software*
 - It's accountability
 - It's how you deal with incidents
 - It's the processes
- Show the role vendors play
 - *Adding trust to Open Source Solutions*
 - *In selecting software*
 - *In providing a single source of trusted information*
 - *In QA and auditing*
 - *In keeping systems up to date*
 - *In reducing risk and exposure*



Open Source makes this easy

- Flexible
 - *No forced upgrades*
 - *Alter the fix*
- Accountable
 - *You can't hide vulnerabilities*
 - *You can't deny vulnerabilities exist*
 - *Competition escalates time scales*
 - *Anyone can assess the risk and impact*
 - *Vendors provide many eyes and QA*
- Education
 - *Everyone can learn from security mistakes*





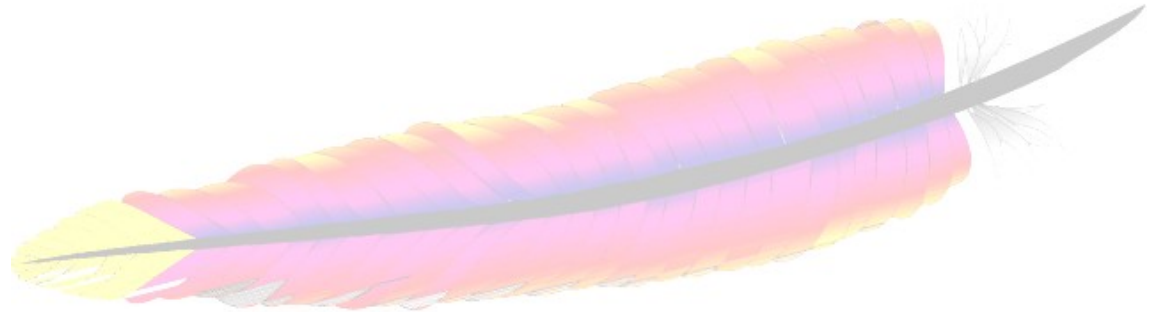
Open Source makes this hard

- Unique challenges
 - *No control over open source groups*
 - *Lack of common process*
 - *Many vendors who all ship the same thing*
 - Or nearly the same thing
- Just because it's open
 - *Doesn't mean anyone is looking*
 - *Doesn't help the press get it right*

Apache



- Apache web server
 - Powers over half of the Internet web server infrastructure
 - Mature project, over 7 years old
- Apache Software Foundation
 - 1999, umbrella organisation





“a loose confederation of programmers ... working in their spare time over gin and tonics at home” -- The Wall Street Journal



Apache Software Foundation

- Engineers for security
 - *designed for security*
- Uses revision control
 - *open process*
- Has established release management process
 - *including code signing*
- Uses bug tracking system
 - *open process*



Apache Quality Assurance

- Has automated testing and regression tools
- Quality Assurance and fixes
 - *From Red Hat*
 - *From SuSE*
 - *From Covalent*
 - *From IBM*
 - *From HP*
 - *From Mandrake*
 - *From OpenBSD*
 - *From*



Apache Emergency Response

- Has a dedicated security response team
 - *Defines process and follows procedures*
 - Responsible Vulnerability Disclosure Process draft
 - *Works with organisations like CERT and Mitre*
 - *Works with vendors that distribute Apache*
 - *Can be trusted with early disclosure*
- Quickly responds to security incidents





Apache Security Record

1.3.0 to 1.3.28 (5 years 1 month)

Type of issue	Severity	Number of vulnerabilities
Denial of Service	High	6
Show a directory listing	Low	4
Read files on the system	High	3
Remote arbitrary code execution	High	2
Cross Site Scripting	Medium	2
Local privilege escalation	Medium	1
Remote Root Exploit	High	0

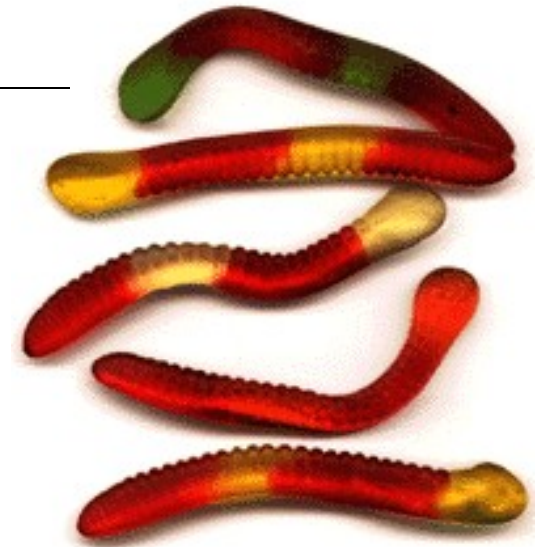


**Open Source Software projects
can be trusted**

Linux Worms



<i>Name</i>	<i>Date Found</i>	<i>Date Fixed</i>
Slapper	Sep 2002	July 2002
Adore	Apr 2001	Jan 2001
Lion	Mar 2001	Jan 2001
Ramen Noodle	Jan 2001	Sep 2000





Who was vulnerable?

- People who didn't update their systems
 - *Why didn't they upgrade?*
 - Abandoned
 - Install and Forget
 - Cry Wolf (too much information)
 - Incorrect or misleading information.
 - They thought they already had
 - Inertia, too hard to upgrade
 - *How can we help?*
 - Reduce the impact of worms
 - Better quality information
 - consistent naming
 - Easier to upgrade

Everybody thought Somebody would do it. Anybody could have done it. But Nobody did. And in the end Everybody got mad at Somebody Because... Nobody did what Anybody could have done.



**It's critical to keep systems up
to date**



'Chinese Whispers'

Severity: Medium (Session hijacking/possible compromise)

A vulnerability exists in the SSI error pages of Apache 2.0 that involves incorrect filtering of server signature data. The vulnerability could enable an attacker to hijack web sessions, allowing a range of potential compromises on the targeted host.

- Matthew Murphy, Bugtraq





Apache is susceptible to a cross site scripting vulnerability in the default 404 page of any web server hosted on a domain that allows wildcard DNS lookups. We thank Matthew Murphy for notification of this issue.

-- Official Apache Announcement





Apache HTTPD servers versions 2.0.42 and prior, and 1.3.26 and prior, with wildcard DNS enabled and UseCanonicalName disabled, are vulnerable to a cross-site scripting attack via the error page. Only versions 2.0 to 2.0.33 have UseCanonicalName disabled by default. All other versions had UseCanonicalName enabled by default and are not vulnerable unless this option is disabled.

-- CERT CC





EXPLOIT : local

A vulnerability exists in the SSI error pages of Apache 2.0 that involves incorrect filtering of server signature data. The vulnerability could enable an attacker to hijack web sessions, allowing a range of potential compromises on the targeted host.

- Gentoo Security Advisory





Two cross-site scripting vulnerabilities are present in the error pages for the default "404 Not Found" error, and for the error response when a plain HTTP request is received on an SSL port. Both of these issues are only exploitable if the "UseCanonicalName" setting has been changed to "Off", and wildcard DNS is in use, and would allow remote attackers to execute scripts as other Web page visitors, for instance, to steal cookies.

- Red Hat Security Advisory





CAN-2002-0840 This is a cross-site scripting vulnerability involving the default error 404 pages. It can occur on all Oracle database platforms.

- Oracle Security Advisory





Apache is updated to version 1.3.27 to address a number of issues.

- Apple Security Advisor





Cross-site scripting (XSS) vulnerability in the default error page of Apache 2.0 before 2.0.43, and 1.3.x up to 1.3.26, when UseCanonicalName is "Off" and support for wildcard DNS is present, allows remote attackers to execute script as other web page visitors via the Host: header.

-- Apache Week





Vulnerabilities that are being exploited because of a failure to upgrade Apache itself include the 404 page cross-site scripting bug, which manages wildcard DNS lookups; ...

Risk level - serious

-- ZDNet UK



Apache fixes scripting flaw

By [John Leyden](#)

Posted: 04/10/2002 at 11:26 GMT

Apache is vulnerable to a number of cross-site scripting attacks.

According to a [posting](#) to BugTraq this week, the popular Web server platform is vulnerable due to "SSI error pages of the Web server not being properly sanitised of malicious HTML code".

Because of this, attacker-constructed HTML pages or script code may be executed on a web client visiting the malicious link placed on sites run using Apache. Cookie-based authentication credentials might be stolen using the attack or, worse, a number of arbitrary actions might be taken on a victim's machine.


A proof-of-concept exploit has been posted to BugTraq.

Previous versions of Apache on a wide variety of platform are potentially vulnerable, as explained in greater detail [here](#).

Admins are advised to update their Web server software to either Apache versions 1.3.27 or 2.0.43, which are both resilient to the attack. These versions incorporate a fix, as [explained](#) in more depth on Apache's Web site, by security researcher Matthew Murphy, who reported the flaw. ®





Address  <http://www.sans.org/top20/#U2>

[Back to Top ^](#)


U2 Apache Web Server

U2.1 Description


Web administrators too often conclude that since Microsoft's Internet Information Server (IIS) is exceptionally prone to compromise (see W1. Internet Information Server), the open-source [Apache web server](#) is completely secure. While the comparison with IIS may be true, and although Apache has a well-deserved reputation for security, it has not proved invulnerable under scrutiny.

There have been weaknesses found in Apache. Even [the apache.org website was defaced in early 2000](#). Exploits of core Apache or its modules in the recent past have been few, but they have been well-documented and quickly utilized in attacks. Among the most recent:

- [Apache/mod_ssl Worm \(CERT Advisory CA-2002-27\)](#)
- [Apache Chunk Handling Exploit \(CERT Advisory CA-2002-17\)](#)

Address  <http://www.sans.org/top20/#U2>

For more Apache security information, see <http://www.sans.org/Gold/apache.php> and http://www.infosecuritymaa.com/articles/april01/features1_web_server_sec.shtml.

Address  <http://www.sans.org/Gold/apache.php>

Bottom line: Can Apache be hacked? Absolutely. In fact, even apache.org itself was defaced in early 2000 (see <http://packetstormsecurity.nl/papers/general/cruciphux>). But Apache isn't as easily hacked as IIS, because it can't be taken down by the kiddie scripts that plague so many unpatched IIS servers. (A)

Solution: The Center for Internet Security's Apache Benchmark CIS Benchmarks enumerate security configuration settings and actions that "harden" your systems. They are unique, not because the settings and



With security advisories such as this that have the potential to boost business for the security companies making the warning, it's often best to seek out several sources of information about the seriousness of the threat.

-- MSNBC 16 Sep 2002

Security companies have their own agendas



Analysing Vulnerabilities

- What is this issue all about?
- How does it affect you?
 - *Impact on your organisation*
 - *Threat assessment*
- How was it fixed?
- Requires Detective work
- Requires trusted information sources
 - *Chinese Whispers*
 - *Press FUD*
- Vendor mailing lists
- MARC



3. Problem description:

KDE is a graphical desktop environment for the X Window System.

KDE versions 2.2.2 and earlier have a vulnerability in their SSL implementation that makes it possible for users of Konqueror and other SSL enabled KDE software to fall victim to a man-in-the-middle attack. Red Hat Linux 7.1 and 7.2 shipped with KDE packages that are vulnerable to this issue.

Users of KDE should upgrade to these erratum packages, which contain KDE 2.2.2 with a backported patch to correct this vulnerability.



1. Problem Description

The Apache mod_dav module contains a format string vulnerability in the "ap_log_error()" function.

- What is mod_dav?
- What is the implication?
- Work arounds?
- How was it fixed?



apache-1.3/src/CHANGES - view - 1.1892 - Mozilla

File Edit View Go Bookmarks Tools Window Help

http://cvs.apache.org/viewcvs.cgi/apache-1.3/src/CHANGES?re...

Home Bookmarks RHTA Google SecBugs RHAT Bugzilla bug 49... Apache Week. Release

*) SECURITY: CVE-2001-0731 (cve.mitre.org)
Close autoindex /?M=D directory listing hole reported
in bugtraq id 3009. In some releases autoindex is enabled for a directory listing result in a directory listing that is more than the negotiated index length. The work around (in some releases) is to disable IndexOptions in the directory listing. [Bill Stoddard]

*) Enabled Win32/OS2/Netware...

Address http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2001-0731

Home Get CVE About CVE News and Events Editorial Board Advisory Council Compatible Products



Common Vulnerabilities and Exposures
The Key to Information Sharing

CVE-2001-0731

redhat.com | Red Hat Support - Mozilla

File Edit View Go Bookmarks Tools Window Help

http://rhn.redhat.com/errata/RHSA-2001-126-29

Home Bookmarks RHTA Google SecBugs RHAT Bugzilla bug 49...

LOG IN / LOG OUT BECOME A MEMBER DOWNLOAD STORE

redhat

SEARCH RED HAT: [] Go

Products and Services Solutions Support and Docs Training About Red Hat Worldwide

Errata >

Updated apache packages available

Advisory: RHSA-2001:126-29

Last updated on: 2002-01-15

Affected Products: [Red Hat Linux 6.2](#)
[Red Hat Linux 7.0](#)
[Red Hat Linux 7.1](#)
[Red Hat Linux 7.2](#)

CVEs (cve.mitre.org): [CVE-2001-0730](#)
[CVE-2001-0731](#)

[back](#)

Security Advisory

Version: 20020625

This advisory is an entry on the [CVE list](#), which standardizes names for security vulnerabilities. It was reviewed and accepted by the [CVE Editorial Board](#). This advisory was added to CVE.

CVE-2001-0731
Apache 1.3.20 with Multiviews enabled allows remote attackers to view directory contents and bypass the index page via a URL containing the "M=D" query string.

References

- BUGTRAQ:20010709 How Google indexed a file with no external link
- CONFIRM: <http://www.apacheweek.com/issues/01-10-05#security>
- MANDRAKE:MDKSA-2001:077
- OID:3009
- XF:apache-multiviews-directory-listing(8275)
- SGI:20020301-01-P

References are provided for the convenience of the reader to distinguish between CVE entries. The list of references is not intended to be complete.

Created on 20020625.

redhat.

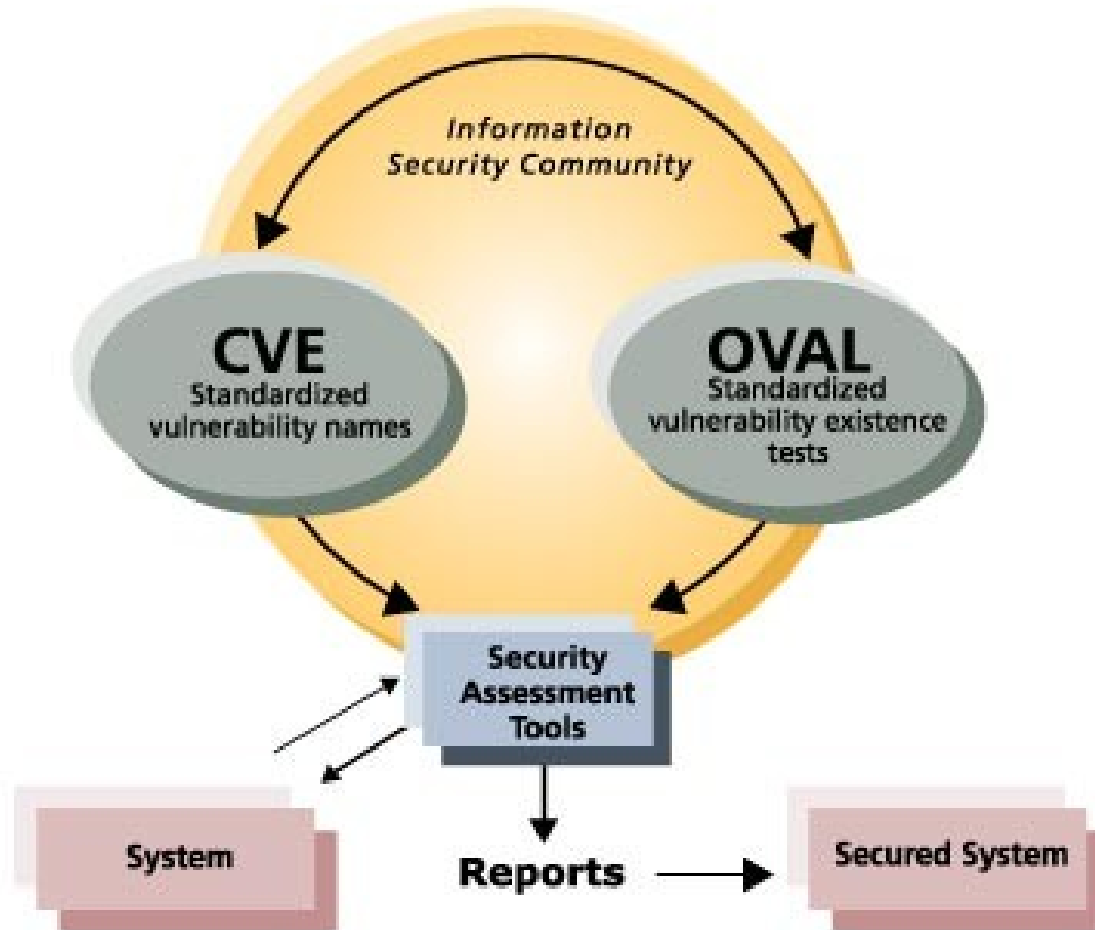


Mitre OVAL

- To determine the existence of vulnerabilities
 - *By evaluating a statement*
 - *Currently SQL (so human readable)*
- Is my system vulnerable to CVE-2001-0730?
 - *Depends on what your system is*
 - *Depends on the version of components, your updates, patches applied, local modifications, reboots*
 - *Might depend on the configuration*
- Another Nessus?
 - *Assumes you have access to the machine*
 - *Bases it on the state of your machine*
- It's tricky



More about OVAL





Role of the Vendor

- To package Open Source software
- QA
 - *to provide the “many eyes”*
- A single point of contact
- Provide support, backup
- Provide accountability
- Clear and established response process
- Security audits
- Certification





Vendor Versions

■ Positives

- *Works out of the box*
- *Customised for the OS*
- *Tested, QA'd*
- *The kitchen sink*
- *One source of security information*
- *Automatic updates*
- *Install and forget*
- *Accountability*

■ Trust

- *Trust the vendor's analysis*
- *Trust the vendor to produce timely critical fixes*

■ Risks

- *Mix and Match?*
- *Forced to Upgrade?*
- *What was fixed?*





Reducing the impact of exploits

- exec-shield
 - *Provides protection against stack, buffer or function pointer overflows*
 - *Provides protection against other types of data overwriting exploits*
 - *Works transparently, - no application recompilation is necessary*
- **Doesn't negate the need for security updates**
- PIE
- IPSec
 - *Secure IP layer communications*
- File system ACLs



Reducing the impact of exploits

- SELinux
 - *Mandatory Access Controls*
 - *Integrated into Linux Kernel*
 - *10 years of NSA research*
 - *Separates policy from enforcement*
 - *Role-based access control*
- SELinux and Apache
 - *Choose your policy*
 - High – only display pages in /var/www/html
 - Medium – can run CGI scripts in /var/www/cgi-bin
 - Low – can display pages in users home directories
 - *A cracker only gets the same access as the policy states*



Security Fix Backporting

- Making it easy to keep systems current
 - *Customer demand*
 - *Too many new features*
 - *Certification*
 - *Quicker and painless upgrades*
 - *Minimize impact of automated updates*
- Issues
 - *Version number doesn't change*
 - Confuses tools
 - Confuses Nessus
 - Confuses users
 - *Requires good quality communication*





Red Hat Security Response

- Continually assessing threats and vulnerabilities that affect our users
- Providing a single point of contact for security issues and patches : single source
- Working with organisations
 - *CERT, Mitre, OIS*
- Following Responsible Disclosure guidelines
- Working with our competitors
 - *Linux (and other Open Source OS vendors) ISAC*
- Helping projects set up emergency response teams and processes



What else is Red Hat doing?

- Improving the quality of information
 - *CVE*
 - *allow customers to make informed choices*
- Reducing the risk of exploits
 - *exec-shield, other kernel innovation*
 - *SELinux*
- Making it easy to apply security updates
 - *backporting of security patches*
- Make sure known flaws get corrected, quickly
 - *Even in the absence of known threats*
- Helping people keep their systems up to date
 - *Red Hat Network*



Mark J Cox
Security Response Team

mjc@redhat.com
www.awe.com/mark/lw2003