



Apache Security Secrets: Revealed! (Again!)

for ApacheCon 2003, Las Vegas
Mark J Cox



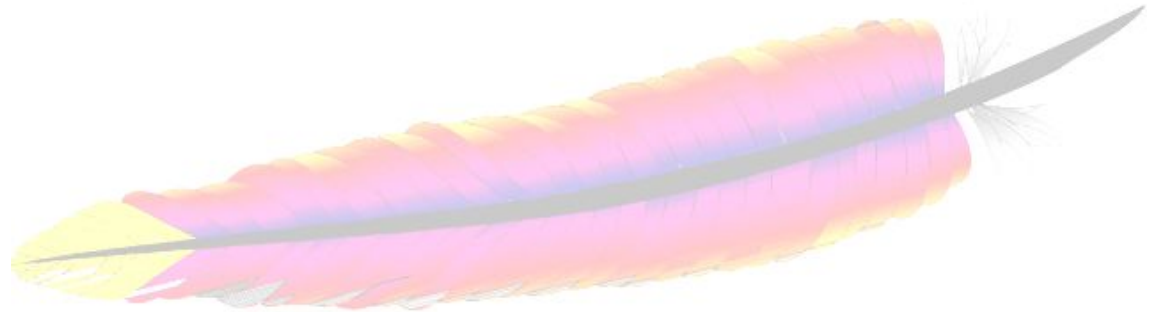
revision 3

www.awe.com/mark/apcon2003

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



Arbitrary code execution

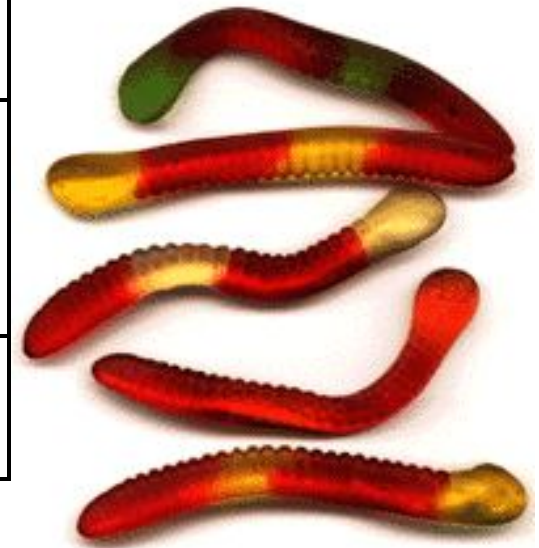
- Nightmare scenario
- It's only happened *ONCE* to Apache 1.3
 - *and then it was limited to some platforms*
 - *and you didn't get root*

C V E	T i t l e	D e s c r i p t i o n
C A N - 2 0 0 2 - 0 3 9 2	A p a c h e C h u n k e d e n c o d i n g v u l n e r a b i l i t y	R e q u e s t s t o a l l v e r s i o n s o f A p a c h e 1 . 3 c a n c a u s e v a r i o u s e f f e c t s r a n g i n g f r o m a r e l a t i v e l y h a r m l e s s i n c r e a s e i n s y s t e m r e s o u r c e s t h r o u g h t o d e n i a l o f s e r v i c e a t t a c k s a n d i n s o m e c a s e s t h e a b i l i t y t o b e r e m o t e l y e x p l o i t e d .
C A N - 2 0 0 2 - 0 0 6 1	W i n 3 2 A p a c h e R e m o t e c o m m a n d e x e c u t i o n	A p a c h e f o r W i n 3 2 b e f o r e 1 . 3 . 2 4 a n d 2 . 0 . 3 4 - b e t a a l l o w s r e m o t e a t t a c k e r s t o e x e c u t e a r b i t r a r y c o m m a n d s v i a p a r a m e t e r s p a s s e d t o b a t c h f i l e C G I s c r i p t s .



Apache Worms

Name	Date	Affects	Exploits
Slapper (Linux.Slapper-A, Linux.Slapper- Worm, Apache/mod_ssl Worm)	13 Sept 2002	Apache with mod_ssl and OpenSSL on various Linux platforms	C.A.S. 2002- 0656
Linux.Devnull	30 Sept 2002	Apache with mod_ssl and OpenSSL on various Linux platforms	C.A.S. 2002- 0656
Sculper (E.kokapa, PHP/Exploit- Apache)	20 June 2002	Apache on OpenBSD and FreeBSD	C.A.S. 2002- 0332





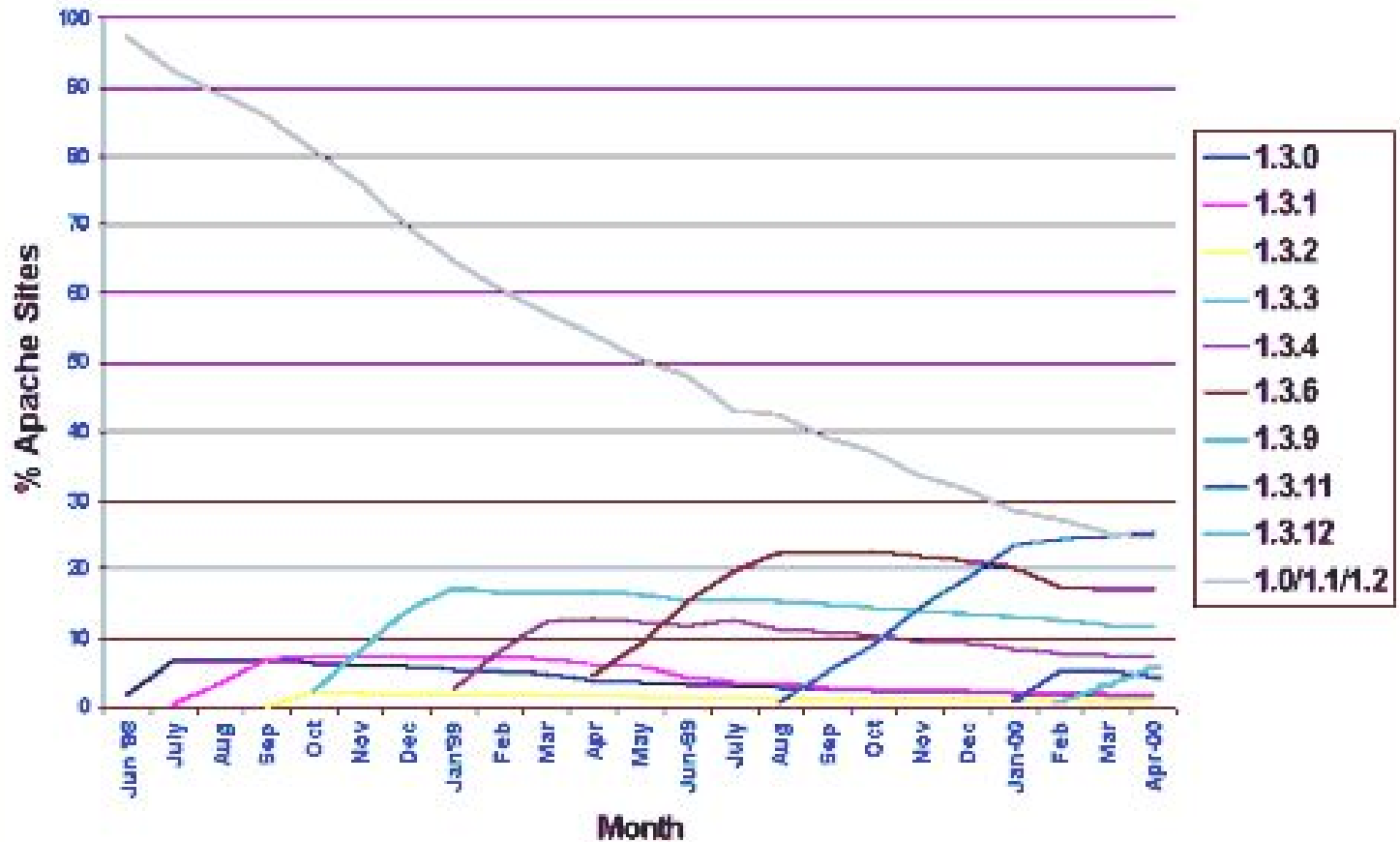
Who was vulnerable?

- 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.



Release take up





**Secret: Keep your System up
to date**





Security Policy

- Why bother?
- Security response policy for Apache
 - *Alert Phase*
 - *Analysis Phase*
 - *Response Phase*
 - *Maintenance Phase*
- Assumptions
 - *Just Apache*
 - *Not from a vendor*





Alert Phase

- Where to get your information
 - *How the quality varies*
- Keep notes
- Apache mailing lists
- CERT CC
- Bugtraq
- Full Disclosure
- Apache Week
- Apache web site
- Security Sites



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



'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 \(CERT Advisory CA-2002-27\)](#)
- [Apa](#)

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

For more Apache security information, see <http://www.sans.org/Gold/apache.php> and http://www.infosecuritymag.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

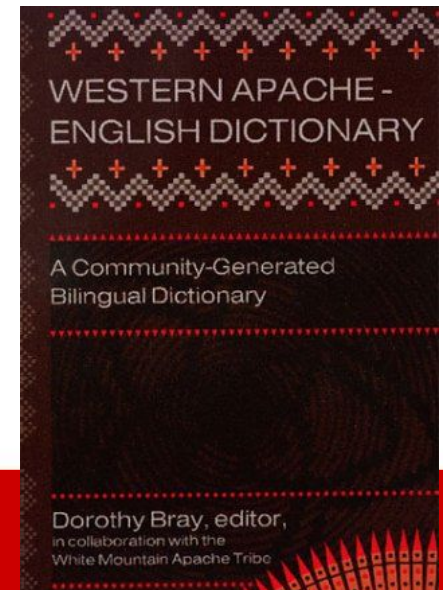
Secret: Security companies have their own agendas





Apache and CVE

- Lots of vendors ship Apache
- Lots of vendors report on Apache issues
 - *As do the press*
 - *As do weekly journals*
- Common Vulnerabilities and Exposures
 - *Dictionary of issues from Mitre*
 - *Cross-reference with vulnerability databases*
 - *Standardisation and Normalisation*
- www.apacheweek.com/security





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

File Edit View Go Bookmarks Tools Window Help

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

*) 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 result in a directory listing more than the negotiated index listing is expected. The work around (in some releases) is to disable IndexOptions in the configuration for the affected directories. [Bill Stoddard]

*) Enabled Win32/OS2/Netware...



Common Vulnerabilities and Exposures

The Key to Information Sharing

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

CVE-2001-0731

redhat.com | Red Hat Support - Mozilla

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

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

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
- OSVDB: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.



Analysing an Apache issue

- What you need to document
 - *Vulnerability name and identifiers*
 - Short name, CVE, CERT
 - *Versions affected*
 - *Configuration required*
 - Default? Special configuration?
 - *Impact and severity*
 - Severity is often hard to catagorise
 - *Work-arounds*
 - *Patches*



Getting to know you

- What are you running?
 - *manually*
 - *Nmap*
- Are you vulnerable?
 - *Exploits*
 - *Nessus*
- Dependencies

```
flooble% /usr/sbin/httpd -v
Server version: Apache/1.3.22 (Unix)
Server built:   Jun 19 2002 12:27:54
```

```
flooble% telnet localhost 80
Trying 127.0.0.1...
Connected to localhost.
Escape character is '^]'.
HEAD / HTTP/1.0

HTTP/1.1 200 OK
Date: Fri, 04 Oct 2002 12:54:06 GMT
Server: Apache/1.3.22 (Unix)
```



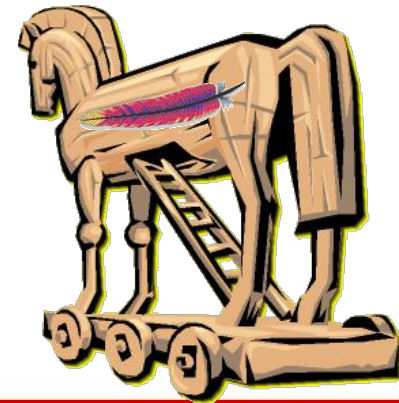
Secret: Go to the source





Response Phase

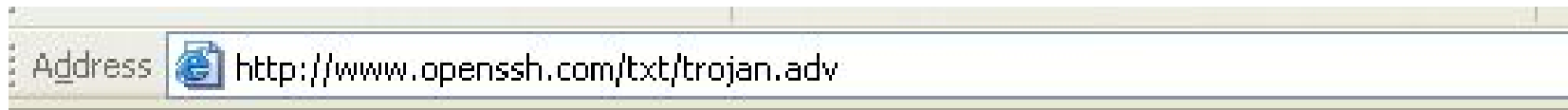
- What are you going to do about it
 - *What is the impact?*
 - *What policies affect it*
 - *Upgrade to the latest version?*
 - Apache Software Foundation recommended
 - *or Phased approach?*
 - *or Patch?*
 - *or do nothing?*
- But make sure your source isn't a trojan





Trojan source

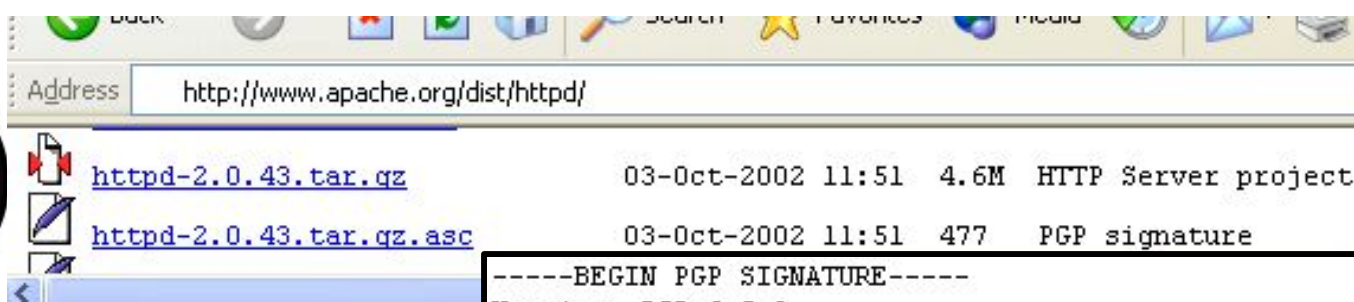
- It's happened to OpenSSH and Sendmail
 - *But not to Apache*
 - Yet



OpenSSH Security Advisory (adv.trojan)

1. Systems affected:

OpenSSH version 3.2.2p1, 3.4p1 and 3.4 have been trojaned on the OpenBSD ftp server and potentially propagated via the normal mirroring process to other ftp servers. The code was inserted some time between the 30th and 31th of July. We replaced the trojaned files with their originals at 7AM MDT, August 1st.



```
flurble% wget http://www.apache.org/dist/httpd/httpd-2.0.43.tar.gz
Connecting to www.apache.org:80
HTTP request sent, awaiting response...
Length: 88,641 [text/plain]
```

```
OK -> .....
50K -> .....
```

```
11:57:33 (317.08 KB/s) - 'KEYS' saved [88641/88641]
```

```
flurble% gpg --import KEYS
gpg: Warning: using insecure memory!
gpg: key 2719AF35: public key imported
gpg: key A99F75DD: public key imported
gpg: key 302DA568: public key imported
gpg: key 2C312D2F: public key imported
gpg: key A0BB71C1: public key imported
```

```
flurble% gpg httpd-2.0.43.tar.gz.asc
gpg: Signature made Thu 03 Oct 2002 07:01:01 AM BST using RSA key ID 10FDE075
gpg: Good signature from "wrowe@covalent.net"
gpg: aka "William A. Rowe, Jr. <wrowe@rowe-clan.net>"
gpg: aka "wrowe@lnd.com"
gpg: aka "wrowe@apache.org"
```

```
-----BEGIN PGP SIGNATURE-----
Version: PGP 6.5.8

iQEVAwUAPZvdHfcTqHkQ/eBlAQEasQf+PiY2EMrwMV+vxN6R9+Z2r6f8cfQZz00u
rIlleG073F4x7cyGw+P38ZwIK30v6cUrnAlvYHC2GUeuwZEjeNMSL82G+UebIrK2
p/17a0WJr09vcfPLW2RkplUk32y8ju+RxZ2LMPT298sA5UspGr74qxcFbQXtAuHQ
StnsMrkxBzT/TAA2EFksagSE05VSKAj5jVXLe42uafTFyZt6IggLgKmtxl6fBAB0
6QCvM5xKflv9XhXBxCJ90KPoqv0qumcZ7dnUWuhSjiZBPSilu6tflvZZweQY2XFA
fuiHHmdUuUls77NUNJxKp80SABFqLb0gkL5EFkcsRgsR+8FftVvkyQ==
-----END PGP SIGNATURE-----
```



Finishing the Policy

- Security response policy for Apache
 - *Alert Phase*
 - *Analysis Phase*
 - *Response Phase*
 - *Maintenance Phase*
- Steps for recovering from compromise
 - *Don't believe the press*
 - *LKM rootkits*
 - *CERT CC*
 - *Hope you kept a backup*



Secret: Create a Security Policy





**Secret: assume you are going
to get hacked**





Secret: Keep Backups





Vendor versions

- Benefits
 - *Works out of the box*
 - *Customised for the OS*
 - *Tested, QA'd*
 - *Modules galore (The kitchen sink)*
 - *One source of security information*
 - *Automatic updates*
 - *Install and forget*
 - *Accountability*
- Trust
 - *Trust the vendors analysis*
 - *Trust the vendor to produce timely critical fixes*
- Risks
 - *Mix and match*
 - *Forced to upgrade*
 - *What did they fix*





Secret: Trust your vendor
(if you don't then change vendor!)





Backporting

- Confuses everyone
- It's no longer Apache!
- So why do it?
 - *Customers demand it*
 - *Too many new features*
 - *Certification*
 - *Quicker and painless upgrades*
 - *Automatic upgrades*
- Problems
 - *Version number doesn't change*
 - Confuses tools
 - Confuses Nessus
 - Confuses users
 - *Vendors have their own package versioning*
 - inconsistent





Open source myths?

- “Many eyes”
 - *How many of you have audited Apache?*
 - *OpenSSL vulnerabilities “easily spotted”*
 - *There are other benefits*
 - No need for FUD
- Apache’s history
 - *Just Apache*
 - *Normalising to CVE*





Apache 1.3.0 to 1.3.29

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	2
Remote Root Exploit	High	0

Type of issue	Severity	Who and When
Run Arbitrary Commands	High	Oracle, SCO, 2002
Show the source to CGI scripts	Medium	SuSE Linux, 2000
Show files in /usr/doc	Low	Debian Linux, 1999 SuSE Linux, 2000
Read and write any file in docroot	High	SuSE Linux 2000
Read .htaccess files	Medium	Cobalt, 2000
Run arbitrary commands remotely	High	IBM, 2000
See files in /perl	Low	Manrake, 2000



Secret: Apache is already pretty secure





Denial of Service

- Only interesting if it is easy to do
- Directives to help stop regular DOS
 - *RLimit* LimitRequest**

C V E	Title	Description
C A N - 2001-1342	Denial of service attack on Win32 and OS2	A client submitting a carefully constructed URL could cause a General Protection Fault in a child process, bringing up a message box which would have to be cleared by the operator to resume.
C A N - 2003-0542	Denial of service on Win32 and OS2	The rotatologs support program on Win32 and OS/2 would quit logging and exit if it received special control characters such as 0x1A.
none	Denial of service attack on Win32	There have been a number of important security fixes to Apache on Windows. The most important is that there is much better protection against people trying to access special DOS device names (such as 'nul').
C A N - 1999-1199	Multiple header Denial of Service vulnerability	A problem exists when a client sends a large number of headers with the same header name. Apache uses up memory faster than the amount of memory required to simply store the received data itself.
none	Denial of service attacks	Apache 1.3.2 has better protection against denial of service attacks.



Get docroot directory listings

- Should be a minor impact
 - *As long as you don't do something silly*
- Disable mod_autoindex unless you need it

C V E	T i t l e	D e s c r i p t i o n
C A N - 2 0 0 1 - 0 7 2 9	R e q u e s t s c a n c a u s e d i r e c t o r y l i s t i n g t o b e d i s p l a y e d	A v u l n e r a b i l i t y w a s f o u n d i n t h e W i n 3 2 p o r t o f A p a c h e 1.3.20. A c l i e n t s u b m i t t i n g a v e r y l o n g U R L c o u l d c a u s e a d i r e c t o r y l i s t i n g t o b e r e t u r n e d
C A N - 2 0 0 1 - 0 7 3 1	M u l t i v i e w s c a n c a u s e a d i r e c t o r y l i s t i n g t o b e d i s p l a y e d	W h e n M u l t i v i e w s a r e u s e d t o n e g o t i a t e t h e d i r e c t o r y i n d e x . I n s o m e c o n f i g u r a t i o n s , r e q u e s t i n g a U R L w i t h a Q U E R Y S T R I N G o f M = D c o u l d r e t u r n a d i r e c t o r y l i s t i n g
C A N - 2 0 0 1 - 0 9 2 5	R e q u e s t s c a n c a u s e d i r e c t o r y l i s t i n g t o b e d i s p l a y e d	T h e d e f a u l t i n s t a l l a t i o n c a n l e a d m o d _ n e g o t i a t i o n a n d m o d _ d i r o r m o d _ a u t o i n d e x t o d i s p l a y a d i r e c t o r y l i s t i n g i f a v e r y l o n g p a t h w a s c r e a t e d a r t i f i c i a l l y b y u s i n g m a n y s l a s h e s .
C V E - 2 0 0 0 - 0 5 0 5	R e q u e s t s c a n c a u s e d i r e c t o r y l i s t i n g t o b e d i s p l a y e d o n N T	A u s e r t o v i e w t h e l i s t i n g o f a d i r e c t o r y i n s t e a d o f t h e d e f a u l t H T M L p a g e b y s e n d i n g a c a r e f u l l y c o n s t r u c t e d r e q u e s t .



Local privilege escalation

- One unique issue due to a bug
 - *Local Apache uid can do things as root*
 - Cause a DOS, Kill arbitrary processes
 - *You can get Apache uid from CGI, Perl etc*
- One issue allowing apache uid “escalation”

C V E	T itle	D escription
C A N - 2 0 0 2 - 0 8 3 9	S h a r e d m e m o r y p e r m i s s i o n s l e a d t o l o c a l p r i v i l e g e e s c a l a t i o n	T h e p e r m i s s i o n s o f t h e s h a r e d m e m o r y u s e d f o r t h e s c o r e b o a r d a l l o w s a n a t t a c k e r w h o c a n e x e c u t e u n d e r t h e A p a c h e U I D t o s e n d a s i g n a l t o a n y p r o c e s s a s r o o t o r c a u s e a l o c a l d e n i a l o f s e r v i c e a t t a c k .
C A N - 2 0 0 3 - 0 5 4 2	L o c a l c o n f i g u r a t i o n r e g u l a r e x p r e s s i o n o v e r f l o w	B y u s i n g a r e g u l a r e x p r e s s i o n w i t h m o r e t h a n 9 c a p t u r e s a b u f f e r o v e r f l o w c a n o c c u r i n m o d _ a l i a s o r m o d _ r e w r i t e . T o e x p l o i t t h i s a n a t t a c k e r w o u l d n e e d t o b e a b l e t o c r e a t e a c a r e f u l l y c r a f t e d c o n f i g u r a t i o n f i l e (.htaccess or httpd.conf)



Serve arbitrary files

- It's actually hard to do
 - *Much easier through a bad CGI or PHP script*
- CHROOT jail solution

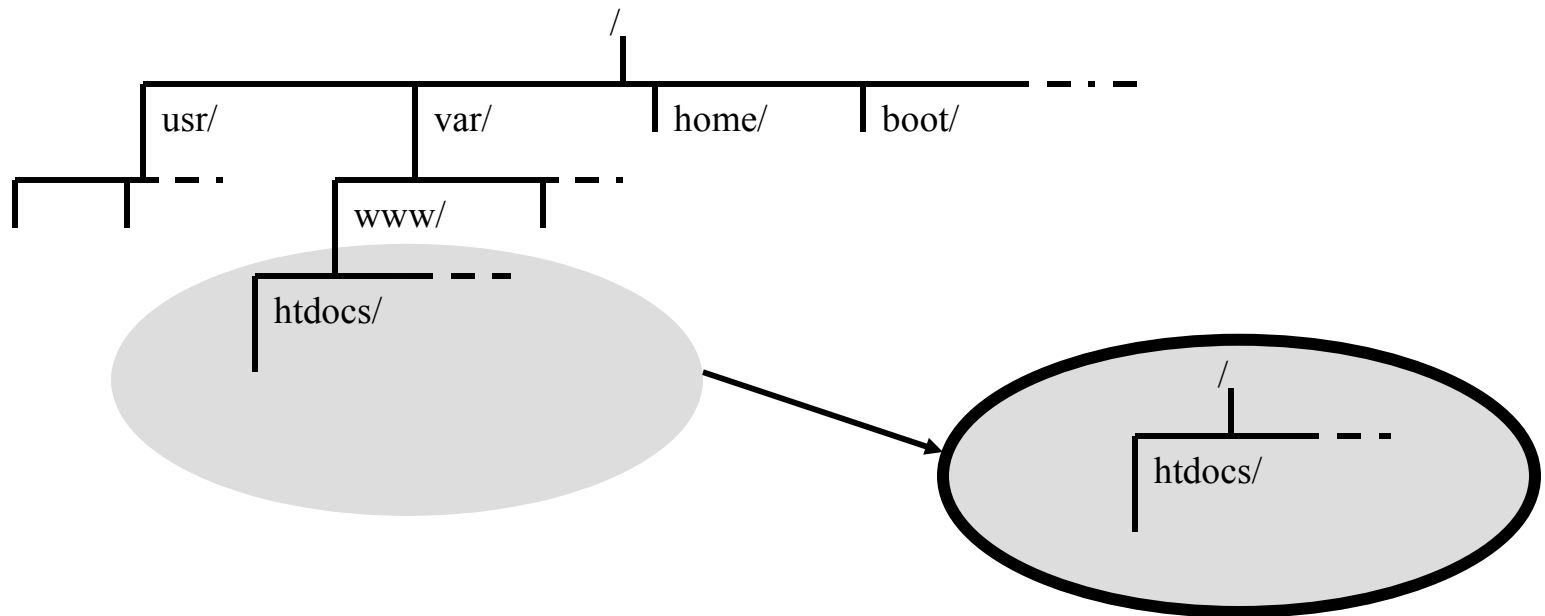
C V E	T i t l e	D e s c r i p t i o n
C A N - 2 0 0 0 - 0 9 1 3	R e w r i t e r u l e s t h a t i n c l u d e r e f e r e n c e s a l l o w a c c e s s t o a n y f i l e	T h e R e w r i t e m o d u l e , m o d _ r e w r i t e , c a n a l l o w a c c e s s t o a n y f i l e o n t h e w e b s e r v e r . T h e v u l n e r a b i l i t y o c c u r s o n l y w i t h c e r t a i n s p e c i f i c c a s e s o f u s i n g r e g u l a r e x p r e s s i o n r e f e r e n c e s i n R e w r i t e R u l e d i r e c t i v e s
C A N - 2 0 0 0 - 1 2 0 4	M a s s v i r t u a l h o s t i n g c a n d i s p l a y C G I s o u r c e	A s e c u r i t y p r o b l e m f o r u s e r s o f t h e m a s s v i r t u a l h o s t i n g m o d u l e , m o d _ v h o s t _ a l i a s , c a u s e s t h e s o u r c e t o a C G I t o b e s e n t i f t h e c g i - b i n d i r e c t o r y i s u n d e r t h e d o c u m e n t r o o t . H o w e v e r , i t i s n o t n o r m a l t o h a v e y o u r c g i - b i n d i r e c t o r y u n d e r a d o c u m e n t r o o t .
C A N - 2 0 0 0 - 1 2 0 6	M a s s v i r t u a l h o s t i n g s e c u r i t y i s s u e	A s e c u r i t y p r o b l e m c a n o c c u r f o r s i t e s u s i n g m a s s n a m e - b a s e d v i r t u a l h o s t i n g (u s i n g t h e n e w m o d _ v h o s t _ a l i a s m o d u l e) o r w i t h s p e c i a l m o d _ r e w r i t e r u l e s .



Mitigate remote exploits

- Use a CHROOT jail

“This is the best approach we can currently take against such a monolithic piece of software with such bad behaviours. It is just too big to audit, so for simple usage, we are constraining it to within that jail.” -- Theo de Raadt, OpenBSD





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**



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*



Cross Site Scripting (XSS)

- Completely misunderstood

C V E	T i t l e	D e s c r i p t i o n
C A N - 2 0 0 2 - 0 8 4 0	E r r o r p a g e X S S u s i n g w i l d c a r d D N S	C r o s s - s i t e s c r i p t i n g (X S S) v u l n e r a b i l i t y i n t h e d e f a u l t e r r o r p a g e o f A p a c h e 2 . 0 b e f o r e 2 . 0 . 4 3 , a n d 1 . 3 . x u p t o 1 . 3 . 2 6 , w h e n U s e C a n o n i c a l N a m e i s " O f f " a n d s u p p o r t f o r w i l d c a r d D N S i s p r e s e n t , a l l o w s r e m o t e a t t a c k e r s t o e x e c u t e s c r i p t a s o t h e r w e b p a g e v i s i t o r s v i a t h e H o s t : h e a d e r .
C A N - 2 0 0 0 - 1 2 0 5	C r o s s - s i t e s c r i p t i n g c a n r e v e a l p r i v a t e s e s s i o n i n f o r m a t i o n	A p a c h e w a s v u l n e r a b l e t o c r o s s - s i t e s c r i p t i n g i s s u e s . I t w a s s h o w n t h a t m a l i c i o u s H T M L t a g s c a n b e e m b e d d e d i n c l i e n t w e b r e q u e s t s i f t h e s e r v e r o r s c r i p t h a n d l i n g t h e r e q u e s t d o e s n o t c a r e f u l l y e n c o d e a l l i n f o r m a t i o n d i s p l a y e d t o t h e u s e r . U s i n g t h e s e v u l n e r a b i l i t i e s a t t a c k e r s c o u l d , f o r e x a m p l e , o b t a i n c o p i e s o f y o u r p r i v a t e c o o k i e s u s e d t o a u t h e n t i c a t e y o u t o o t h e r s i t e s .



mod_rewrite canonicalisation

- CVE-2001-1072, August 2001
- Pass // to most rewrite rules
 - Including ones in our own documentation

- **Wrong!**

```
RewriteRule ^/somepath(.*) /otherpath$1  
[R]
```

- **Right**

```
RewriteRule ^/+somepath(.*) /otherpath$1  
[R]
```

```
http://www.awe.com/somepath/fred
```

```
http://www.awe.com//somepath/fred
```

...This isn't fixed!!!



htpasswd races

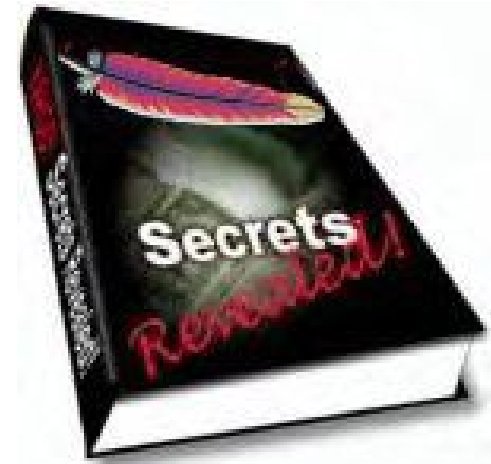
- CVE-2001-0131, 2001
- Temporary file creation vulnerability
 - *Any local user can read or modify contents of Apache password file if they exploit a race when an administrator runs htpasswd (or htdigest)*
- Fixed in some places
 - *Some Debian distributions (Jan 2001-Jun 2002, Oct 2002+)*
 - *Some Red Hat distributions (Red Hat Linux 7.0+)*

...This isn't fixed!!!



Secrets, finally revealed

- Don't Panic
- Make a security policy for dealing with Apache emergencies
- Give good evaluation feedback
- Mitigate the risks
- Review the secrets





"The only truly secure system is one that is powered off, cast in a block of concrete and sealed in a lead-lined room with armed guards -- and even then I have my doubts."
-- Gene Spafford

Secret: If this is too much effort, turn off your server

