Scan Report

May 11, 2017

Summary

This document reports on the results of an automatic security scan. All dates are displayed using the timezone "Coordinated Universal Time", which is abbreviated "UTC". The task was "Immediate scan of IP 192.168.8.102". The scan started at Thu May 11 01:17:07 2017 UTC and ended at Thu May 11 02:40:06 2017 UTC. The report first summarises the results found. Then, for each host, the report describes every issue found. Please consider the advice given in each description, in order to rectify the issue.

Contents

1 Result Overview

Host	High	Medium	Low	Log	False Positive
192.168.8.102	96	106	16	67	0
Total: 1	96	106	16	67	0

Vendor security updates are not trusted.
Overrides are on. When a result has an override, this report uses the threat of the override.
Information on overrides is included in the report.
Notes are included in the report.
This report might not show details of all issues that were found.

This report contains all 285 results selected by the filtering described above. Before filtering there were 285 results.

1.1 Host Authentications

Host	Protocol	Result	Port/User
192.168.8.102	SMB	Success	Protocol SMB, Port 445, User

2 Results per Host

2.1 192.168.8.102

Host scan start Thu May 11 01:17:39 2017 UTC
Host scan end Thu May 11 02:40:06 2017 UTC

Service (Port)	Threat Level
5432/tcp	High
22/tcp	High
8787/tcp	High
5900/tcp	High
6200/tcp	High
general/tcp	High
445/tcp	High
1524/tcp	High
21/tcp	High
53/tcp	High
3632/tcp	High
80/tcp	High
1099/tcp	High
6667/tcp	Medium
5432/tcp	Medium

. . . (continues) . . .

... (continued) ...

Service (Port)	Threat Level
22/tcp	Medium
general/tcp	Medium
445/tcp	Medium
21/tcp	Medium
53/tcp	Medium
80/tcp	Medium
5432/tcp	Low
22/tcp	Low
general/tcp	Low
445/tcp	Low
53/tcp	Low
80/tcp	Low
6667/tcp	Log
general/CPE-T	Log
5432/tcp	Log
2121/tcp	Log
22/tcp	Log
512/tcp	Log
8787/tcp	Log
8009/tcp	Log
3306/tcp	Log
5900/tcp	Log
6000/tcp	Log
23/tcp	Log
513/tcp	Log
general/tcp	Log
111/tcp	Log
445/tcp	Log
1524/tcp	Log
21/tcp	Log
53/tcp	Log
514/tcp	Log
80/tcp	Log
1099/tcp	Log
general/icmp	Log
139/tcp	Log
25/tcp	Log

2.1.1 High 5432/tcp

High (CVSS: 10.0)
NVT: PostgreSQL End Of Life Detection

Product detection result

... continues on next page ...

... continued from previous page ...

cpe:/a:postgresql:postgresql:8.3.1
Detected by PostgreSQL Detection (OID: 1.3.6.1.4.1.25623.1.0.100151)

Summary
The PostgreSQL version on the remote host has reached the end of life and should not be used anymore.

Vulnerability Detection Result
The PostgreSQL version has reached the end of life.
Installed version: 8.3.1
EOL version: 8.3
EOL date: 2013-02-01

Impact
An end of life version of PostgreSQL is not receiving any security updates from the vendor. Unfixed security vulnerabilities might be leveraged by an attacker to compromise the security of this host.

Solution
Solution type: VendorFix
Update the PostgreSQL version on the remote host to a still supported version.

Vulnerability Detection Method
Get the installed version with the help of the detect NVT and check if the version is unsupported.
Details:PostgreSQL End Of Life Detection
OID:1.3.6.1.4.1.25623.1.0.140158
Version used: $Revision: 5294 $

Product Detection Result
Product: cpe:/a:postgresql:postgresql:8.3.1
Method: PostgreSQL Detection
OID: 1.3.6.1.4.1.25623.1.0.100151)

References
Other:
URL:https://www.postgresql.org/support/versioning/

High (CVSS: 8.5)
NVT: PostgreSQL Multiple Security Vulnerabilities

Product detection result
cpe:/a:postgresql:postgresql:8.3.1
Detected by PostgreSQL Detection (OID: 1.3.6.1.4.1.25623.1.0.100151)

... continues on next page ...

... continued from previous page ...

Summary
PostgreSQL is prone to multiple security vulnerabilities.
Attackers can exploit these issues to bypass certain security restrictions and execute arbitrary Perl or Tcl code.
These issues affect versions prior to the following PostgreSQL versions:
8.4.4 8.3.11 8.2.17 8.1.21 8.0.25 7.4.29

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Solution
Updates are available. Please see the references for more information.

Vulnerability Detection Method
Details:`PostgreSQL Multiple Security Vulnerabilities`
OID:1.3.6.1.4.1.25623.1.0.100645
Version used: `$Revision: 5373 $`

Product Detection Result
Product: `cpe:/a:postgresql:postgresql:8.3.1`
Method: `PostgreSQL Detection`
OID: 1.3.6.1.4.1.25623.1.0.100151)

References
```
CVE: CVE-2010-1169, CVE-2010-1170, CVE-2010-1447
BID:40215
Other:
  URL:http://www.securityfocus.com/bid/40215
   URL:http://www.postgresql.org/about/news.1203
   URL:http://www.postgresql.org/
   URL:http://www.postgresql.org/support/security
```

High (CVSS: 9.0)
NVT: PostgreSQL Multiple Vulnerabilities - Mar15 (Linux)

Product detection result
```
cpe:/a:postgresql:postgresql:8.3.1
Detected by PostgreSQL Detection (OID: 1.3.6.1.4.1.25623.1.0.100151)
```

Summary
This host is running PostgreSQL and is prone to multiple vulnerabilities.

Vulnerability Detection Result
```
Installed version: 8.3.1
```

... continues on next page ...

... continued from previous page ...

Fixed version: 9.1.20

Impact
Successful exploitation will allow a remote attacker to escalate privileges and to cause denial of service conditions.
Impact Level: Application

Solution
Solution type: VendorFix
Upgrade to version 9.1.20 or 9.2.15 or 9.3.11 or 9.4.6 or 9.5.1 or higher, For updates refer to http://www.postgresql.org/download

Affected Software/OS
PostgreSQL version before 9.1.20, 9.2.x before 9.2.15, 9.3.x before 9.3.11, 9.4.x before 9.4.6, and 9.5.x before 9.5.1 on Linux.

Vulnerability Insight
Multiple flaws are due to the PostgreSQL incorrectly handle certain regular expressions and certain configuration settings (GUCS) for users of PL/Java.

Vulnerability Detection Method
Get the installed version with the help of detect NVT and check the version is vulnerable or not.
Details:PostgreSQL Multiple Vulnerabilities - Mar15 (Linux)
OID:1.3.6.1.4.1.25623.1.0.807518
Version used: $Revision: 5712 $

Product Detection Result
Product: cpe:/a:postgresql:postgresql:8.3.1
Method: PostgreSQL Detection
OID: 1.3.6.1.4.1.25623.1.0.100151)

References
CVE: CVE-2016-0773, CVE-2016-0766
BID:83184
Other:
URL:http://www.ubuntu.com/usn/USN-2894-1
URL:http://www.postgresql.org/about/news/1644

High (CVSS: 9.0)
NVT: PostgreSQL weak password

Summary
It was possible to login into the remote PostgreSQL as user postgres using weak credentials.

Vulnerability Detection Result

... continues on next page ...

... continued from previous page ...

It was possible to login as user postgres with password "postgres".

Solution
Change the password as soon as possible.

Vulnerability Detection Method
Details:PostgreSQL weak password
OID:1.3.6.1.4.1.25623.1.0.103552
Version used: $Revision: 5888 $

[return to 192.168.8.102]

2.1.2 High 22/tcp

High (CVSS: 7.5)
NVT: OpenSSH 'schnorr.c' Remote Memory Corruption Vulnerability

Summary
OpenSSH is prone to a remote memory-corruption vulnerability.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact
An attacker can exploit this issue to execute arbitrary code in context of the application. Failed exploits may result in denial-of- service conditions.

Solution
Updates are available.

Affected Software/OS
OpenSSH 6.4 and prior with J-PAKE implemented are vulnerable.

Vulnerability Insight
The hash_buffer function in schnorr.c in OpenSSH through 6.4, when Makefile.inc is modified to enable the J-PAKE protocol, does not initialize certain data structures, which might allow remote attackers to cause a denial of service (memory corruption) or have unspecified other impact via vectors that trigger an error condition.

Vulnerability Detection Method
Check the version.
Details:OpenSSH 'schnorr.c' Remote Memory Corruption Vulnerability
OID:1.3.6.1.4.1.25623.1.0.105001
Version used: $Revision: 4336 $

References

... continues on next page ...

... continued from previous page ...

CVE: CVE-2014-1692
BID:65230
Other:
URL:http://www.securityfocus.com/bid/65230
URL:http://www.openssh.com

High (CVSS: 7.8)
NVT: OpenSSH Denial of Service And User Enumeration Vulnerabilities (Linux)

Product detection result
cpe:/a:openbsd:openssh:4.7p1
Detected by SSH Server type and version (OID: 1.3.6.1.4.1.25623.1.0.10267)

Summary
This host is installed with openssh and is prone to denial of service and user enumeration vulnerabilities.

Vulnerability Detection Result
Installed version: 4.7p1
Fixed version: 7.3

Impact
Successfully exploiting this issue allows remote attackers to cause a denial of service (crypt CPU consumption) and to enumerate users by leveraging the timing difference between responses when a large password is provided.
Impact Level: Application

Solution
Solution type: VendorFix
Upgrade to OpenSSH version 7.3 or later. For updates refer to http://www.openssh.com

Affected Software/OS
OpenSSH versions before 7.3 on Linux

Vulnerability Insight
Multiple flaws exists due to, - The auth_password function in 'auth-passwd.c' script does not limit password lengths for password authentication. - The sshd in OpenSSH, when SHA256 or SHA512 are used for user password hashing uses BLOWFISH hashing on a static password when the username does not exist and it takes much longer to calculate SHA256/SHA512 hash than BLOWFISH hash.

Vulnerability Detection Method
Get the installed version with the help of detect NVT and check the version is vulnerable or not.
Details:OpenSSH Denial of Service And User Enumeration Vulnerabilities (Linux)
OID:1.3.6.1.4.1.25623.1.0.809154

... continues on next page ...

... continued from previous page ...

Version used: $Revision: 5352 $

Product Detection Result
Product: cpe:/a:openbsd:openssh:4.7p1
Method: SSH Server type and version
OID: 1.3.6.1.4.1.25623.1.0.10267)

References
CVE: CVE-2016-6515, CVE-2016-6210
BID:92212
Other:
URL:http://www.openssh.com/txt/release-7.3
URL:http://seclists.org/fulldisclosure/2016/Jul/51
URL:https://security-tracker.debian.org/tracker/CVE-2016-6210
URL:http://openwall.com/lists/oss-security/2016/08/01/2

High (CVSS: 8.5)
NVT: OpenSSH Multiple Vulnerabilities

Product detection result
cpe:/a:openbsd:openssh:4.7p1
Detected by SSH Server type and version (OID: 1.3.6.1.4.1.25623.1.0.10267)

Summary
This host is running OpenSSH and is prone to multiple vulnerabilities.

Vulnerability Detection Result
Installed version: 4.7p1
Fixed version: 7.0

Impact
Successful exploitation will allow an attacker to gain privileges, to conduct impersonation attacks, to conduct brute-force attacks or cause a denial of service.
Impact Level: Application

Solution
Solution type: VendorFix
Upgrade to OpenSSH 7.0 or later. For updates refer to http://www.openssh.com

Affected Software/OS
OpenSSH versions before 7.0

Vulnerability Insight

... continues on next page ...

... continued from previous page ...

Multiple flaws are due to: - Use-after-free vulnerability in the 'mm_answer_pam_free_ctx' function in monitor.c in sshd. - Vulnerability in 'kbdint_next_device' function in auth2-chall.c in sshd. - vulnerability in the handler for the MONITOR_REQ_PAM_FREE_CTX request.

Vulnerability Detection Method
Get the installed version with the help of detect NVT and check the version is vulnerable or not.
Details:`OpenSSH Multiple Vulnerabilities`
OID:1.3.6.1.4.1.25623.1.0.806052
Version used: `$Revision: 4336 $`

Product Detection Result
Product: `cpe:/a:openbsd:openssh:4.7p1`
Method: `SSH Server type and version`
OID: 1.3.6.1.4.1.25623.1.0.10267)

References
```
CVE: CVE-2015-6564, CVE-2015-6563, CVE-2015-5600
Other:
  URL:http://seclists.org/fulldisclosure/2015/Aug/54
   URL:http://openwall.com/lists/oss-security/2015/07/23/4
```

High (CVSS: 7.5)
NVT: OpenSSH Multiple Vulnerabilities Jan17 (Linux)

Product detection result
```
cpe:/a:openbsd:openssh:4.7p1
Detected by SSH Server type and version (OID: 1.3.6.1.4.1.25623.1.0.10267)
```

Summary
This host is installed with openssh and is prone to multiple vulnerabilities.

Vulnerability Detection Result
```
Installed version: 4.7p1
Fixed version:     7.4
```

Impact
Successfully exploiting this issue allows local users to obtain sensitive private-key information, to gain privileges, and allows remote attackers to execute arbitrary local PKCS#11 modules.
Impact Level: Application

Solution
Solution type: VendorFix
Upgrade to OpenSSH version 7.4 or later. For updates refer to http://www.openssh.com

... continues on next page ...

... continued from previous page ...

Affected Software/OS
OpenSSH versions before 7.4 on Linux

Vulnerability Insight
Multiple flaws exists due to, - An 'authfile.c' script does not properly consider the effects of realloc on buffer contents. - The shared memory manager (associated with pre-authentication compression) does not ensure that a bounds check is enforced by all compilers. - The sshd in OpenSSH creates forwarded Unix-domain sockets as root, when privilege separation is not used. - An untrusted search path vulnerability in ssh-agent.c in ssh-agent.

Vulnerability Detection Method
Get the installed version with the help of detect NVT and check the version is vulnerable or not.
Details:`OpenSSH Multiple Vulnerabilities Jan17 (Linux)`
OID:1.3.6.1.4.1.25623.1.0.8103256
Version used: `$Revision: 5084 $`

Product Detection Result
Product: `cpe:/a:openbsd:openssh:4.7p1`
Method: `SSH Server type and version`
OID: 1.3.6.1.4.1.25623.1.0.10267)

References
```
CVE: CVE-2016-10009, CVE-2016-10010, CVE-2016-10011, CVE-2016-10012
BID:94968, 94972, 94977, 94975
Other:
  URL:https://www.openssh.com/txt/release-7.4
   URL:http://www.openwall.com/lists/oss-security/2016/12/19/2
```

High (CVSS: 7.2)
NVT: OpenSSH Privilege Escalation Vulnerability - May16

Product detection result
```
cpe:/a:openbsd:openssh:4.7p1
Detected by SSH Server type and version (OID: 1.3.6.1.4.1.25623.1.0.10267)
```

Summary
This host is installed with openssh and is prone to privilege escalation vulnerability.

Vulnerability Detection Result
```
Installed version: 4.7p1
Fixed version:     7.2p2-3
```

Impact
Successfully exploiting this issue will allow local users to gain privileges.

... continues on next page ...

... continued from previous page ...

Impact Level: Application

Solution
Solution type: VendorFix
Upgrade to OpenSSH version 7.2p2-3 or later. For updates refer to http://www.openssh.com

Affected Software/OS
OpenSSH versions through 7.2p2

Vulnerability Insight
The flaw exists due to an error in 'do_setup_env function' in 'session.c' script in sshd which trigger a crafted environment for the /bin/login program when the UseLogin feature is enabled and PAM is configured to read .pam_environment files in user home directories.

Vulnerability Detection Method
Get the installed version with the help of detect NVT and check the version is vulnerable or not.
Details:`OpenSSH Privilege Escalation Vulnerability - May16`
OID:1.3.6.1.4.1.25623.1.0.807574
Version used: `$Revision: 5527 $`

Product Detection Result
Product: `cpe:/a:openbsd:openssh:4.7p1`
Method: `SSH Server type and version`
OID: 1.3.6.1.4.1.25623.1.0.10267)

References
`CVE: CVE-2015-8325`
`Other:`
`URL:https://people.canonical.com/~ubuntu-security/cve/2015/CVE-2015-8325.html`
`URL:https://anongit.mindrot.org/openssh.git/commit/?id=85bdcd7c92fe7ff133bbc4`
`↪e10a65c91810f88755`

High (CVSS: 7.5)
NVT: OpenSSH X11 Forwarding Security Bypass Vulnerability (Linux)

Product detection result
`cpe:/a:openbsd:openssh:4.7p1`
`Detected by SSH Server type and version (OID: 1.3.6.1.4.1.25623.1.0.10267)`

Summary
This host is installed with openssh and is prone to security bypass vulnerability.

Vulnerability Detection Result
`Installed version: 4.7p1`

... continues on next page ...

... continued from previous page ...

Fixed version: 7.2

Impact
Successfully exploiting this issue allows local users to bypass certain security restrictions and perform unauthorized actions. This may lead to further attacks.
Impact Level: Application

Solution
Solution type: VendorFix
Upgrade to OpenSSH version 7.2 or later. For updates refer to http://www.openssh.com

Affected Software/OS
OpenSSH versions before 7.2 on Linux.

Vulnerability Insight
An access flaw was discovered in OpenSSH, It did not correctly handle failures to generate authentication cookies for untrusted X11 forwarding. A malicious or compromised remote X application could possibly use this flaw to establish a trusted connection to the local X server, even if only untrusted X11 forwarding was requested.

Vulnerability Detection Method
Get the installed version with the help of detect NVT and check the version is vulnerable or not.
Details:OpenSSH X11 Forwarding Security Bypass Vulnerability (Linux)
OID:1.3.6.1.4.1.25623.1.0.810769
Version used: $Revision: 6002 $

Product Detection Result
Product: cpe:/a:openbsd:openssh:4.7p1
Method: SSH Server type and version
OID: 1.3.6.1.4.1.25623.1.0.10267)

References
CVE: CVE-2016-1908
BID:84427
Other:
URL:http://openwall.com/lists/oss-security/2016/01/15/13
URL:https://bugzilla.redhat.com/show_bug.cgi?id=1298741#c4
URL:http://www.openssh.com/txt/release-7.2
URL:https://anongit.mindrot.org/openssh.git/commit/?id=ed4ce82dbfa8a3a3c8ea6f
↪a0db113c71e234416c
URL:https://bugzilla.redhat.com/show_bug.cgi?id=1298741

[return to 192.168.8.102]

2.1.3 High 8787/tcp

High (CVSS: 10.0)
NVT: Distributed Ruby (dRuby/DRb) Multiple Remote Code Execution Vulnerabilities

Summary
Systems using Distributed Ruby (dRuby/DRb), which is available in Ruby versions 1.6 and later, may permit unauthorized systems to execute distributed commands.

Vulnerability Detection Result
```
The service is running in $SAFE >= 1 mode. However it is still possible to run a
↪rbitrary syscall commands on the remote host. Sending an invalid syscall the s
↪ervice returned the following response:
Flo:Errno::ENOSYS:bt["3/usr/lib/ruby/1.8/drb/drb.rb:1555:in `syscall'"0/usr/lib/
↪ruby/1.8/drb/drb.rb:1555:in `send'"4/usr/lib/ruby/1.8/drb/drb.rb:1555:in `__se
↪nd__'"A/usr/lib/ruby/1.8/drb/drb.rb:1555:in `perform_without_block'"3/usr/lib/
↪ruby/1.8/drb/drb.rb:1515:in `perform'"5/usr/lib/ruby/1.8/drb/drb.rb:1589:in `m
↪ain_loop'"0/usr/lib/ruby/1.8/drb/drb.rb:1585:in `loop'"5/usr/lib/ruby/1.8/drb/
↪drb.rb:1585:in `main_loop'"1/usr/lib/ruby/1.8/drb/drb.rb:1581:in `start'"5/usr
↪/lib/ruby/1.8/drb/drb.rb:1581:in `main_loop'"//usr/lib/ruby/1.8/drb/drb.rb:143
↪0:in `run'"1/usr/lib/ruby/1.8/drb/drb.rb:1427:in `start'"//usr/lib/ruby/1.8/dr
↪b/drb.rb:1427:in `run'"6/usr/lib/ruby/1.8/drb/drb.rb:1347:in `initialize'"//us
↪r/lib/ruby/1.8/drb/drb.rb:1627:in `new'"9/usr/lib/ruby/1.8/drb/drb.rb:1627:in
↪`start_service'"%/usr/sbin/druby_timeserver.rb:12:errnoi+:mesg"Function not im
↪plemented
```

Impact
By default, Distributed Ruby does not impose restrictions on allowed hosts or set the $SAFE environment variable to prevent privileged activities. If other controls are not in place, especially if the Distributed Ruby process runs with elevated privileges, an attacker could execute arbitrary system commands or Ruby scripts on the Distributed Ruby server. An attacker may need to know only the URI of the listening Distributed Ruby server to submit Ruby commands.

Solution
Solution type: Mitigation
Administrators of environments that rely on Distributed Ruby should ensure that appropriate controls are in place. Code-level controls may include:
- Implementing taint on untrusted input
- Setting $SAFE levels appropriately (>=2 is recommended if untrusted hosts are allowed to submit Ruby commands, and >=3 may be appropriate)
- Including drb/acl.rb to set ACLEntry to restrict access to trusted hosts

Vulnerability Detection Method
Send a crafted command to the service and check for a remote command execution via the instance_eval or syscall requests.
Details:`Distributed Ruby (dRuby/DRb) Multiple Remote Code Execution Vulnerabilities`
OID:1.3.6.1.4.1.25623.1.0.108010
Version used: `$Revision: 4387 $`

References

. . . continues on next page . . .

... continued from previous page ...

```
BID:47071
Other:
  URL:https://tools.cisco.com/security/center/viewAlert.x?alertId=22750
   URL:http://www.securityfocus.com/bid/47071
   URL:http://blog.recurity-labs.com/archives/2011/05/12/druby_for_penetration_t
↪esters/
   URL:http://www.ruby-doc.org/stdlib-1.9.3/libdoc/drb/rdoc/DRb.html
```

[return to 192.168.8.102]

2.1.4 High 5900/tcp

High (CVSS: 9.0)
NVT: VNC Brute Force Login

Summary
Try to log in with given passwords via VNC protocol.

Vulnerability Detection Result
`It was possible to connect to the VNC server with the password: password`

Solution
Solution type: Mitigation
Change the password to something hard to guess.

Vulnerability Insight
This script tries to authenticate to a VNC server with the passwords set in the password preference.
Note: Some VNC servers have a blacklisting scheme that blocks IP addresses after five unsuccessful connection attempts for a period of time. The script will abort the brute force attack if it encounters that it gets blocked. Note as well that passwords can be max. 8 characters long.

Vulnerability Detection Method
Details:`VNC Brute Force Login`
OID:1.3.6.1.4.1.25623.1.0.106056
Version used: `$Revision: 4472 $`

[return to 192.168.8.102]

2.1.5 High 6200/tcp

High (CVSS: 7.5)
NVT: vsftpd Compromised Source Packages Backdoor Vulnerability

... continues on next page ...

... continued from previous page ...

Summary
vsftpd is prone to a backdoor vulnerability.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact
Attackers can exploit this issue to execute arbitrary commands in the context of the application. Successful attacks will compromise the affected application.

Solution
Solution type: VendorFix
The repaired package can be downloaded from https://security.appspot.com/vsftpd.html. Please validate the package with its signature.

Affected Software/OS
The vsftpd 2.3.4 source package is affected.

Vulnerability Detection Method
Details:`vsftpd Compromised Source Packages Backdoor Vulnerability`
OID:1.3.6.1.4.1.25623.1.0.103185
Version used: `$Revision: 5026 $`

References
```
BID:48539
Other:
  URL:http://www.securityfocus.com/bid/48539
   URL:http://scarybeastsecurity.blogspot.com/2011/07/alert-vsftpd-download-back
↪doored.html
   URL:https://security.appspot.com/vsftpd.html
```

[return to 192.168.8.102]

2.1.6 High general/tcp

High (CVSS: 10.0)
NVT: OS End Of Life Detection

Summary
OS End Of Life Detection
The Operating System on the remote host has reached the end of life and should not be used anymore

Vulnerability Detection Result
`The Operating System (cpe:/o:canonical:ubuntu_linux:8.04) on the remote host has ↪ reached the end of life at 09 May 2013`

... continues on next page ...

... continued from previous page ...

and should not be used anymore.
See https://wiki.ubuntu.com/Releases for more information.

Vulnerability Detection Method
Details:OS End Of Life Detection
OID:1.3.6.1.4.1.25623.1.0.103674
Version used: $Revision: 5464 $

High (CVSS: 10.0)
NVT: Samba End Of Life Detection

Product detection result
cpe:/a:samba:samba:3.0.20
Detected by SMB NativeLanMan (OID: 1.3.6.1.4.1.25623.1.0.102011)

Summary
The PostgreSQL version on the remote host has reached the end of life and should not be used anymore.

Vulnerability Detection Result
The Samba version has reached the end of life.
Installed version: 3.0.20
EOL version: 3.0
EOL date: 2009-08-05

Impact
An end of life version of PostgreSQL is not receiving any security updates from the vendor. Unfixed security vulnerabilities might be leveraged by an attacker to compromise the security of this host.

Solution
Solution type: VendorFix
Update the PostgreSQL version on the remote host to a still supported version.

Vulnerability Detection Method
Get the installed version with the help of the detect NVT and check if the version is unsupported.
Details:Samba End Of Life Detection
OID:1.3.6.1.4.1.25623.1.0.140159
Version used: $Revision: 5300 $

Product Detection Result
Product: cpe:/a:samba:samba:3.0.20
Method: SMB NativeLanMan
OID: 1.3.6.1.4.1.25623.1.0.102011)

... continues on next page ...

... continued from previous page ...

References
Other:
URL:https://wiki.samba.org/index.php/Samba_Release_Planning

[return to 192.168.8.102]

2.1.7 High 445/tcp

High (CVSS: 7.5)
NVT: Samba 'mount.cifs' Utility Symlink Attack Local Privilege Escalation Vulnerability

Product detection result
cpe:/a:samba:samba:3.0.20
Detected by SMB NativeLanMan (OID: 1.3.6.1.4.1.25623.1.0.102011)

Summary
Samba is prone to a local privilege-escalation vulnerability in the 'mount.cifs' utility.

Vulnerability Detection Result
Installed version: 3.0.20
Fixed version: 3.0.38/3.3.13/3.4.8

Impact
Local attackers can exploit this issue to gain elevated privileges on affected computers.

Solution
Solution type: VendorFix
Updates are available. Please see the references for more information.

Vulnerability Detection Method
Details:Samba 'mount.cifs' Utility Symlink Attack Local Privilege Escalation Vulnerabil.
↪..
OID:1.3.6.1.4.1.25623.1.0.100623
Version used: $Revision: 4396 $

Product Detection Result
Product: cpe:/a:samba:samba:3.0.20
Method: SMB NativeLanMan
OID: 1.3.6.1.4.1.25623.1.0.102011)

References
CVE: CVE-2010-0747
BID:39898

... continues on next page ...

... continued from previous page ...

Other:
URL:http://www.securityfocus.com/bid/39898
URL:http://www.samba.org

High (CVSS: 7.5)
NVT: Samba 'mtab' Lock File Handling Local Denial of Service Vulnerability

Product detection result
cpe:/a:samba:samba:3.0.20
Detected by SMB NativeLanMan (OID: 1.3.6.1.4.1.25623.1.0.102011)

Summary
Samba is prone to a local denial-of-service vulnerability that affects the mounting utilities 'mount.cifs' and 'umount.cifs'.

Vulnerability Detection Result
Installed version: 3.0.20
Fixed version: 3.6.1

Impact
A local attacker can exploit this issue to cause the mounting utilities to abort, resulting in a denial-of-service condition.

Solution
Solution type: VendorFix
Updates are available. Please see the references for more information.

Vulnerability Detection Method
Details:Samba 'mtab' Lock File Handling Local Denial of Service Vulnerability
OID:1.3.6.1.4.1.25623.1.0.103283
Version used: $Revision: 4398 $

Product Detection Result
Product: cpe:/a:samba:samba:3.0.20
Method: SMB NativeLanMan
OID: 1.3.6.1.4.1.25623.1.0.102011)

References
CVE: CVE-2011-3585
BID:49940
Other:
URL:http://www.securityfocus.com/bid/49940
URL:https://bugzilla.samba.org/show_bug.cgi?id=7179
URL:http://git.samba.org/?p=cifs-utils.git;a=commitdiff;h=810f7e4e0f2dbcbee02
↪94d9b371071cb08268200

... continues on next page ...

... continued from previous page ...

URL:http://us1.samba.org/samba/

High (CVSS: 7.5)
NVT: Samba 'SMB1 Packet Chaining' Unspecified Remote Memory Corruption Vulnerability

Product detection result
cpe:/a:samba:samba:3.0.20
Detected by SMB NativeLanMan (OID: 1.3.6.1.4.1.25623.1.0.102011)

Summary
Samba is prone to an unspecified memory-corruption vulnerability.

Vulnerability Detection Result
Installed version: 3.0.20
Fixed version: 3.3.13

Impact
Attackers can exploit this issue to execute arbitrary code in the context of the application. Failed attacks may cause a denial-of-service condition.

Solution
Solution type: VendorFix
Updates are available. Please see the references for more information.

Affected Software/OS
Samba versions prior to 3.3.13 are vulnerable.

Vulnerability Detection Method
Details:Samba 'SMB1 Packet Chaining' Unspecified Remote Memory Corruption Vulnerability
OID:1.3.6.1.4.1.25623.1.0.100680
Version used: $Revision: 4396 $

Product Detection Result
Product: cpe:/a:samba:samba:3.0.20
Method: SMB NativeLanMan
OID: 1.3.6.1.4.1.25623.1.0.102011)

References
CVE: CVE-2010-2063
BID:40884
Other:
URL:https://www.securityfocus.com/bid/40884
URL:http://www.samba.org
URL:http://labs.idefense.com/intelligence/vulnerabilities/display.php?id=873
URL:http://www.samba.org/samba/security/CVE-2010-2063.html

High (CVSS: 10.0)
NVT: Samba 'TALLOC_FREE()' Function Remote Code Execution Vulnerability

Product detection result
cpe:/a:samba:samba:3.0.20
Detected by SMB NativeLanMan (OID: 1.3.6.1.4.1.25623.1.0.102011)

Summary
Samba 'TALLOC_FREE()' Function Remote Code Execution Vulnerability

Vulnerability Detection Result
Installed version: 3.0.20
Fixed version: 3.6.25 or 4.0.25 or 4.1.17, 4.2.0rc5, or later

Impact
An attacker can exploit this issue to execute arbitrary code with root privileges. Failed exploit attempts will cause a denial-of-service condition

Solution
Solution type: VendorFix
Updates are available. Please see the references or vendor advisory for more information.

Affected Software/OS
Samba 3.5.x and 3.6.x before 3.6.25, 4.0.x before 4.0.25, 4.1.x before 4.1.17, and 4.2.x before 4.2.0rc5

Vulnerability Insight
The Netlogon server implementation in smbd performs a free operation on an uninitialized stack pointer, which allows remote attackers to execute arbitrary code via crafted Netlogon packets that use the ServerPasswordSet RPC API, as demonstrated by packets reaching the _netr_ServerPasswordSet function in rpc_server/netlogon/srv_netlog_nt.c.

Vulnerability Detection Method
Check the version
Details:Samba 'TALLOC_FREE()' Function Remote Code Execution Vulnerability
OID:1.3.6.1.4.1.25623.1.0.105231
Version used: $Revision: 4398 $

Product Detection Result
Product: cpe:/a:samba:samba:3.0.20
Method: SMB NativeLanMan
OID: 1.3.6.1.4.1.25623.1.0.102011)

References
CVE: CVE-2015-0240
BID:72711

... continues on next page ...

... continued from previous page ...

Other:
URL:http://www.securityfocus.com/bid/72711
URL:http://www.samba.org

High (CVSS: 7.5)
NVT: Samba SID Parsing Remote Buffer Overflow Vulnerability

Product detection result
cpe:/a:samba:samba:3.0.20
Detected by SMB NativeLanMan (OID: 1.3.6.1.4.1.25623.1.0.102011)

Summary
Samba is prone to a remote stack-based buffer-overflow vulnerability because it fails to properly bounds-check user-supplied data before copying it to an insufficiently sized memory buffer.

Vulnerability Detection Result
Installed version: 3.0.20
Fixed version: 3.5.5

Impact
An attacker can exploit this issue to execute arbitrary code in the context of the affected application. Failed exploit attempts will likely result in a denial of service.

Solution
Solution type: VendorFix
Updates are available. Please see the references for more information.

Affected Software/OS
Samba versions prior to 3.5.5 are vulnerable.

Vulnerability Detection Method
Details:Samba SID Parsing Remote Buffer Overflow Vulnerability
OID:1.3.6.1.4.1.25623.1.0.100803
Version used: $Revision: 4396 $

Product Detection Result
Product: cpe:/a:samba:samba:3.0.20
Method: SMB NativeLanMan
OID: 1.3.6.1.4.1.25623.1.0.102011)

References
CVE: CVE-2010-3069
BID:43212
Other:

... continues on next page ...

... continued from previous page ...

URL:https://www.securityfocus.com/bid/43212
URL:http://us1.samba.org/samba/history/samba-3.5.5.html
URL:http://www.samba.org
URL:http://us1.samba.org/samba/security/CVE-2010-2069.html

[return to 192.168.8.102]

2.1.8 High 1524/tcp

High (CVSS: 10.0)
NVT: Possible Backdoor: Ingreslock

Summary
A backdoor is installed on the remote host

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact
Attackers can exploit this issue to execute arbitrary commands in the context of the application. Successful attacks will compromise the affected isystem.

Solution
Solution type: Workaround

Vulnerability Detection Method
Details:`Possible Backdoor: Ingreslock`
OID:1.3.6.1.4.1.25623.1.0.103549
Version used: `$Revision: 4718 $`

[return to 192.168.8.102]

2.1.9 High 21/tcp

High (CVSS: 7.5)
NVT: vsftpd Compromised Source Packages Backdoor Vulnerability

Summary
vsftpd is prone to a backdoor vulnerability.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact

... continues on next page ...

... continued from previous page ...

Attackers can exploit this issue to execute arbitrary commands in the context of the application. Successful attacks will compromise the affected application.

Solution
Solution type: VendorFix
The repaired package can be downloaded from https://security.appspot.com/vsftpd.html. Please validate the package with its signature.

Affected Software/OS
The vsftpd 2.3.4 source package is affected.

Vulnerability Detection Method
Details:`vsftpd Compromised Source Packages Backdoor Vulnerability`
OID:1.3.6.1.4.1.25623.1.0.103185
Version used: `$Revision: 5026 $`

References
```
BID:48539
Other:
  URL:http://www.securityfocus.com/bid/48539
   URL:http://scarybeastsecurity.blogspot.com/2011/07/alert-vsftpd-download-back
↪doored.html
   URL:https://security.appspot.com/vsftpd.html
```

[return to 192.168.8.102]

2.1.10 High 53/tcp

High (CVSS: 7.8)
NVT: ISC BIND 'buffer.c' Assertion Failure Denial of Service Vulnerability (Linux)

Product detection result
```
cpe:/a:isc:bind:9.4.2
Detected by Determine which version of BIND name daemon is running (OID: 1.3.6.1
↪.4.1.25623.1.0.10028)
```

Summary
The host is installed with ISC BIND and is prone to denial of service vulnerability.

Vulnerability Detection Result
```
Installed version: 9.4.2
Fixed version:     9.9.9-P3
```

Impact

... continues on next page ...

... continued from previous page ...

Successful exploitation will allow remote attackers to cause a denial of service (assertion failure and daemon exit) via a crafted query.
Impact Level: Application

Solution
Solution type: VendorFix
Upgrade to ISC BIND version 9.9.9-P3 or 9.10.4-P3 or 9.11.0rc3 or later on Linux. For updates refer to https://www.isc.org

Affected Software/OS
ISC BIND 9 before 9.9.9-P3, 9.10.x before 9.10.4-P3, and 9.11.x before 9.11.0rc3 on Linux.

Vulnerability Insight
The flaw exist due to the 'buffer.c' script in named in ISC BIND does not properly construct responses.

Vulnerability Detection Method
Get the installed version with the help of detect NVT and check the version is vulnerable or not.
Details:`ISC BIND 'buffer.c' Assertion Failure Denial of Service Vulnerability (Linux)`
OID:1.3.6.1.4.1.25623.1.0.810263
Version used: `$Revision: 5110 $`

Product Detection Result
Product: `cpe:/a:isc:bind:9.4.2`
Method: `Determine which version of BIND name daemon is running`
OID: 1.3.6.1.4.1.25623.1.0.10028)

References
`CVE: CVE-2016-2776`
`BID:93188`
`Other:`
`URL:https://kb.isc.org/article/AA-01419/0`

High (CVSS: 7.8)
NVT: ISC BIND 'buffer.c' Script Remote Denial of Service Vulnerability - Jan16

Product detection result
`cpe:/a:isc:bind:9.4.2`
`Detected by Determine which version of BIND name daemon is running (OID: 1.3.6.1`
`↪.4.1.25623.1.0.10028)`

Summary
The host is installed with ISC BIND and is prone to remote denial of service vulnerability.

... continues on next page ...

... continued from previous page ...

Vulnerability Detection Result
Installed version: 9.4.2
Fixed version: 9.9.7-P3

Impact
Successful exploitation will allow remote attackers to cause denial of service.
Impact Level: Application

Solution
Solution type: VendorFix
Upgrade to ISC BIND version 9.9.7-P3 or 9.10.2-P4 or later. For updates refer to https://www.isc.org

Affected Software/OS
ISC BIND versions 9.0.0 through 9.8.8 and 9.9.0 through 9.9.7-P2 and 9.10.x through 9.10.2-P3.

Vulnerability Insight
The flaw is due to an error in 'buffer.c' script in ISC BIND.

Vulnerability Detection Method
Get the installed version with the help of detect NVT and check the version is vulnerable or not.
Details:ISC BIND 'buffer.c' Script Remote Denial of Service Vulnerability - Jan16
OID:1.3.6.1.4.1.25623.1.0.807202
Version used: $Revision: 4429 $

Product Detection Result
Product: cpe:/a:isc:bind:9.4.2
Method: Determine which version of BIND name daemon is running
OID: 1.3.6.1.4.1.25623.1.0.10028)

References
CVE: CVE-2015-5722
BID:76605
Other:
URL:https://kb.isc.org/article/AA-01287

High (CVSS: 7.6)
NVT: ISC BIND 9 DNSSEC Bogus NXDOMAIN Response Remote Cache Poisoning Vulnerability

Product detection result
cpe:/a:isc:bind:9.4.2
Detected by Determine which version of BIND name daemon is running (OID: 1.3.6.1
↪.4.1.25623.1.0.10028)

... continues on next page ...

... continued from previous page ...

Summary
ISC BIND 9 is prone to a remote cache-poisoning vulnerability.

Vulnerability Detection Result
Installed version: 9.4.2
Fixed version: 9.4.3-P5

Impact
An attacker may leverage this issue to manipulate cache data, potentially facilitating man-in-the-middle, site-impersonation, or denial-of- service attacks.

Solution
Solution type: VendorFix
Updates are available. Please see the references for details.

Affected Software/OS
Versions prior to the following are vulnerable:
BIND 9.4.3-P5 BIND 9.5.2-P2 BIND 9.6.1-P3

Vulnerability Detection Method
Details:ISC BIND 9 DNSSEC Bogus NXDOMAIN Response Remote Cache Poisoning Vulnerability
OID:1.3.6.1.4.1.25623.1.0.100458
Version used: $Revision: 4433 $

Product Detection Result
Product: cpe:/a:isc:bind:9.4.2
Method: Determine which version of BIND name daemon is running
OID: 1.3.6.1.4.1.25623.1.0.10028)

References
CVE: CVE-2010-0097, CVE-2010-0290, CVE-2010-0382
BID:37865
Other:
URL:http://www.securityfocus.com/bid/37865
URL:http://www.isc.org/products/BIND/
URL:http://www.kb.cert.org/vuls/id/360341
URL:https://www.isc.org/advisories/CVE-2010-0097

High (CVSS: 7.8)
NVT: ISC BIND Delegation Handling Denial of Service Vulnerability

Product detection result
cpe:/a:isc:bind:9.4.2
Detected by Determine which version of BIND name daemon is running (OID: 1.3.6.1
↪.4.1.25623.1.0.10028)

... continues on next page ...

... continued from previous page ...

Summary
The host is installed with ISC BIND and is prone to denial of service vulnerability.

Vulnerability Detection Result
`Installed version: 9.4.2`
`Fixed version: Upgrade to 9.9.6-P1`

Impact
Successful exploitation will allow attackers to cause denial of service to clients.
Impact Level: Application

Solution
Solution type: VendorFix
Upgrade to ISC BIND version 9.9.6-p1 or 9.10.1-p1 or later for branches of BIND (9.9 and 9.10).
For updates refer to https://www.isc.org

Affected Software/OS
ISC BIND versions 9.0.x through 9.8.x, 9.9.0 through 9.9.6, and 9.10.0 through 9.10.1

Vulnerability Insight
The flaw is due to ISC BIND does not handle delegation chaining properly.

Vulnerability Detection Method
Get the installed version with the help of detect NVT and check the version is vulnerable or not.
Details:`ISC BIND Delegation Handling Denial of Service Vulnerability`
OID:1.3.6.1.4.1.25623.1.0.806080
Version used: `$Revision: 4445 $`

Product Detection Result
Product: `cpe:/a:isc:bind:9.4.2`
Method: `Determine which version of BIND name daemon is running`
OID: 1.3.6.1.4.1.25623.1.0.10028)

References
`CVE: CVE-2014-8500`
`Other:`
`URL:https://kb.isc.org/article/AA-01216/0/`

High (CVSS: 7.8)
NVT: ISC BIND Denial of Service Vulnerability

Product detection result
`cpe:/a:isc:bind:9.4.2`

... continues on next page ...

... continued from previous page ...

Detected by Determine which version of BIND name daemon is running (OID: 1.3.6.1
↪.4.1.25623.1.0.10028)

Summary
ISC BIND is prone to a denial of service vulnerability.

Vulnerability Detection Result
Installed version: 9.4.2
Fixed version: 9.9.9-P3

Impact
An remote attacker may cause a denial of service condition.

Solution
Solution type: VendorFix
Upgrade to 9.9.9-P3, 9.9.9-S5, 9.10.4-P3, 9.11.0rc3 or later.

Affected Software/OS
BIND 9

Vulnerability Insight
A crafted query could crash the BIND name server daemon, leading to a denial of service. All server roles (authoritative, recursive and forwarding) in default configurations are affected.

Vulnerability Detection Method
Checks the version.
Details:ISC BIND Denial of Service Vulnerability
OID:1.3.6.1.4.1.25623.1.0.106291
Version used: $Revision: 4429 $

Product Detection Result
Product: cpe:/a:isc:bind:9.4.2
Method: Determine which version of BIND name daemon is running
OID: 1.3.6.1.4.1.25623.1.0.10028)

References
CVE: CVE-2016-2776
Other:
URL:https://kb.isc.org/article/AA-01419

High (CVSS: 7.8)
NVT: ISC BIND Denial of Service Vulnerability - 06 - Jan16

Product detection result

... continues on next page ...

... continued from previous page ...

cpe:/a:isc:bind:9.4.2
Detected by Determine which version of BIND name daemon is running (OID: 1.3.6.1
↪.4.1.25623.1.0.10028)

Summary
The host is installed with ISC BIND and is prone to remote denial of service vulnerability.

Vulnerability Detection Result
Installed version: 9.4.2
Fixed version: 9.9.7-P2

Impact
Successful exploitation will allow remote attackers to cause denial of service.
Impact Level: Application

Solution
Solution type: VendorFix
Upgrade to ISC BIND version 9.9.7-P2 or 9.10.2-P3 or later. For updates refer to https://www.isc.org

Affected Software/OS
ISC BIND versions 9.1.0 through 9.9.7-P1, 9.10.0 through 9.10.2-P2.

Vulnerability Insight
The flaw is due to an error in handling TKEY queries can cause named to exit with a REQUIRE assertion failure.

Vulnerability Detection Method
Get the installed version with the help of detect NVT and check the version is vulnerable or not.
Details:ISC BIND Denial of Service Vulnerability - 06 - Jan16
OID:1.3.6.1.4.1.25623.1.0.807200
Version used: $Revision: 4426 $

Product Detection Result
Product: cpe:/a:isc:bind:9.4.2
Method: Determine which version of BIND name daemon is running
OID: 1.3.6.1.4.1.25623.1.0.10028)

References
CVE: CVE-2015-5477
BID:76092
Other:
URL:https://kb.isc.org/article/AA-01272

High (CVSS: 7.8)
NVT: ISC BIND DNS RDATA Handling Remote Denial of Service Vulnerability - Jan16

Product detection result
cpe:/a:isc:bind:9.4.2
Detected by Determine which version of BIND name daemon is running (OID: 1.3.6.1
↪.4.1.25623.1.0.10028)

Summary
The host is installed with ISC BIND and is prone to remote denial of service vulnerability.

Vulnerability Detection Result
Installed version: 9.4.2
Fixed version: 9.7.7

Impact
Successful exploitation will allow attackers to cause denial of service.
Impact Level: Application

Solution
Solution type: VendorFix
Upgrade to ISC BIND version 9.7.7 or 9.7.6-P4 or 9.6-ESV-R8 or 9.6-ESV-R7-P4 or 9.8.4 or 9.8.3-P4 or 9.9.2 or 9.9.1-P4 later. For updates refer to https://www.isc.org

Affected Software/OS
ISC BIND versions 9.2.x through 9.6.x, 9.4-ESV through 9.4-ESV-R5-P1, 9.6-ESV through 9.6-ESV-R7-P3, 9.7.0 through 9.7.6-P3, 9.8.0 through 9.8.3-P3, 9.9.0 through 9.9.1-P3.

Vulnerability Insight
The flaw exist due to an error in DNS RDATA Handling in ISC BIND.

Vulnerability Detection Method
Get the installed version with the help of detect NVT and check the version is vulnerable or not.
Details:ISC BIND DNS RDATA Handling Remote Denial of Service Vulnerability - Jan16
OID:1.3.6.1.4.1.25623.1.0.807203
Version used: $Revision: 4429 $

Product Detection Result
Product: cpe:/a:isc:bind:9.4.2
Method: Determine which version of BIND name daemon is running
OID: 1.3.6.1.4.1.25623.1.0.10028)

References
CVE: CVE-2012-5166
BID:55852
Other:

. . . continues on next page . . .

... continued from previous page ...

URL:https://kb.isc.org/article/AA-00801

[return to 192.168.8.102]

2.1.11 High 3632/tcp

High (CVSS: 8.5)
NVT: DistCC Detection

Summary
DistCC is a program to distribute builds of C, C++, Objective C or Objective C++ code across several machines on a network. DistCC should always generate the same results as a local build, is simple to install and use, and is often two or more times faster than a local compile.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact
DistCC by default trusts its clients completely that in turn could allow a malicious client to execute arbitrary commands on the server.

Solution
Solution type: Mitigation
For more information about DistCC's security see: http://distcc.samba.org/security.html

Vulnerability Detection Method
Details:DistCC Detection
OID:1.3.6.1.4.1.25623.1.0.12638
Version used: $Revision: 5420 $

High (CVSS: 9.3)
NVT: DistCC Remote Code Execution Vulnerability

Summary
DistCC 2.x, as used in XCode 1.5 and others, when not configured to restrict access to the server port, allows remote attackers to execute arbitrary commands via compilation jobs, which are executed by the server without authorization checks.

Vulnerability Detection Result
It was possible to execute the "id" command.
Result: uid=1(daemon) gid=1(daemon)

Solution
Solution type: VendorFix
Vendor updates are available. Please see the references for more information.

... continues on next page ...

... continued from previous page ...

Vulnerability Detection Method
Details:DistCC Remote Code Execution Vulnerability
OID:1.3.6.1.4.1.25623.1.0.103553
Version used: $Revision: 5120 $

References
CVE: CVE-2004-2687
Other:
URL:http://distcc.samba.org/security.html
URL:http://archives.neohapsis.com/archives/bugtraq/2005-03/0183.html

[return to 192.168.8.102]

2.1.12 High 80/tcp

High (CVSS: 7.1)
NVT: Apache 'mod_deflate' Denial Of Service Vulnerability - July09

Summary
This host is running Apache HTTP Server and is prone to Denial of Service vulnerability.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact
Successful exploitation will allow remote attackers to cause Denial of Service to the legitimate user by CPU consumption. Impact Level: Application

Solution
Fixed in the SVN repository. http://svn.apache.org/viewvc?view=rev&revision=791454
**** NOTE: Ignore this warning if above mentioned patch is already applied. ******

Affected Software/OS
Apache HTTP Server version 2.2.11 and prior

Vulnerability Insight
The flaw is due to error in 'mod_deflate' module which can cause a high CPU load by requesting large files which are compressed and then disconnecting.

Vulnerability Detection Method
Details:Apache 'mod_deflate' Denial Of Service Vulnerability - July09
OID:1.3.6.1.4.1.25623.1.0.800837
Version used: $Revision: 4865 $

References

... continues on next page ...

... continued from previous page ...

CVE: CVE-2009-1891
BID:35623
Other:
URL:http://secunia.com/advisories/35781
URL:http://www.vupen.com/english/advisories/2009/1841
URL:https://rhn.redhat.com/errata/RHSA-2009-1148.html
URL:https://bugzilla.redhat.com/show_bug.cgi?id=509125

High (CVSS: 7.5)
NVT: Apache 'mod_proxy_ftp' Module Command Injection Vulnerability (Linux)

Summary
The host is running Apache and is prone to Command Injection vulnerability.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact
Successful exploitation could allow remote attackers to bypass intended access restrictions in the context of the affected application, and can cause the arbitrary command injection. Impact Level: Application

Solution
Upgrade to Apache HTTP Server version 2.2.15 or later For updates refer to http://www.apache.org/

Affected Software/OS
Apache HTTP Server on Linux.

Vulnerability Insight
The flaw is due to error in the mod_proxy_ftp module which can be exploited via vectors related to the embedding of these commands in the Authorization HTTP header.

Vulnerability Detection Method
Details:Apache 'mod_proxy_ftp' Module Command Injection Vulnerability (Linux)
OID:1.3.6.1.4.1.25623.1.0.900842
Version used: $Revision: 5390 $

References
CVE: CVE-2009-3095
BID:36254
Other:
URL:http://intevydis.com/vd-list.shtml
URL:http://httpd.apache.org/docs/2.0/mod/mod_proxy_ftp.html

High (CVSS: 7.1)
NVT: Apache 'mod_proxy_http.c' Denial Of Service Vulnerability

Summary
This host is running Apache HTTP Server and is prone to Denial of Service vulnerability.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact
Successful exploitation will allow remote attackers to cause Denial of Service to the legitimate user by CPU consumption. Impact Level: Application

Solution
Fixed in the SVN repository. http://svn.apache.org/viewvc?view=rev&revision=790587

Affected Software/OS
Apache HTTP Server version prior to 2.3.3

Vulnerability Insight
The flaw is due to error in 'stream_reqbody_cl' function in 'mod_proxy_http.c' in the mod_proxy module. When a reverse proxy is configured, it does not properly handle an amount of streamed data that exceeds the Content-Length value via crafted requests.

Vulnerability Detection Method
Details:`Apache 'mod_proxy_http.c' Denial Of Service Vulnerability`
OID:1.3.6.1.4.1.25623.1.0.800827
Version used: `$Revision: 4865 $`

References
`CVE: CVE-2009-1890`
`BID:35565`
`Other:`
`URL:http://secunia.com/advisories/35691`
`URL:http://www.vupen.com/english/advisories/2009/1773`
`URL:http://svn.apache.org/viewvc/httpd/httpd/trunk/CHANGES?r1=790587&r2=79058`
`↪6&pathrev=790587`

High (CVSS: 10.0)
NVT: Apache Multiple Security Vulnerabilities

Summary
Apache is prone to multiple vulnerabilities.
These issues may lead to information disclosure or other attacks.
Apache versions prior to 2.2.15 are affected.

Vulnerability Detection Result

... continues on next page ...

... continued from previous page ...

Vulnerability was detected according to the Vulnerability Detection Method.

Solution
Upgrade to Apache 2.2.15 or Later.

Vulnerability Detection Method
Details:Apache Multiple Security Vulnerabilities
OID:1.3.6.1.4.1.25623.1.0.100514
Version used: $Revision: 5263 $

References
CVE: CVE-2010-0425, CVE-2010-0434, CVE-2010-0408, CVE-2007-6750
BID:38494, 38491
Other:
URL:http://www.securityfocus.com/bid/38494
URL:http://httpd.apache.org/security/vulnerabilities_22.html
URL:http://httpd.apache.org/
URL:https://issues.apache.org/bugzilla/show_bug.cgi?id=48359
URL:http://svn.apache.org/viewvc?view=revision&revision=917870

High (CVSS: 9.3)
NVT: PHP '_gdGetColors()' Buffer Overflow Vulnerability

Product detection result
cpe:/a:php:php:5.2.4
Detected by PHP Version Detection (Remote) (OID: 1.3.6.1.4.1.25623.1.0.800109)

Summary
The host is running PHP and is prone to Buffer Overflow vulnerability.

Vulnerability Detection Result
Installed version: 5.2.4
Fixed version: 5.2.11/5.3.1

Impact
Successful exploitation could allow attackers to potentially compromise a vulnerable system.
Impact Level: System

Solution
Solution type: VendorFix
Apply patches from SVN repository, http://svn.php.net/viewvc?view=revision&revision=289557
**** NOTE: Ignore this warning if patch is already applied. *****

Affected Software/OS
PHP version 5.2.x to 5.2.11 and 5.3.0 on Linux.

... continues on next page ...

... continued from previous page ...

Vulnerability Insight
The flaw is due to error in '_gdGetColors' function in gd_gd.c which fails to check certain colorsTotal structure member, whicn can be exploited to cause buffer overflow or buffer over-read attacks via a crafted GD file.

Vulnerability Detection Method
Details:PHP '_gdGetColors()' Buffer Overflow Vulnerability
OID:1.3.6.1.4.1.25623.1.0.801123
Version used: $Revision: 4504 $

Product Detection Result
Product: cpe:/a:php:php:5.2.4
Method: PHP Version Detection (Remote)
OID: 1.3.6.1.4.1.25623.1.0.800109)

References
CVE: CVE-2009-3546
BID:36712
Other:
URL:http://secunia.com/advisories/37080/
URL:http://www.vupen.com/english/advisories/2009/2930
URL:http://marc.info/?l=oss-security&m=125562113503923&w=2

High (CVSS: 7.5)
NVT: PHP 'libgd' Denial of Service Vulnerability (Linux)

Product detection result
cpe:/a:php:php:5.2.4
Detected by PHP Version Detection (Remote) (OID: 1.3.6.1.4.1.25623.1.0.800109)

Summary
This host is installed with PHP and is prone to denial of service vulnerability.

Vulnerability Detection Result
Installed version: 5.2.4
Fixed version: 5.6.27/7.0.12

Impact
Successfully exploiting this issue allow remote attackers to cause a denial of service, or possibly have unspecified other impact.
Impact Level: Application

Solution
Solution type: VendorFix

... continues on next page ...

... continued from previous page ...

Update to PHP version 5.6.27 or 7.0.12. For updates refer to http://www.php.net

Affected Software/OS
PHP versions 5.x through 5.6.26 and 7.0.x through 7.0.11 on Linux

Vulnerability Insight
The flaw exist due to an integer overflow in the gdImageWebpCtx function in gd_webp.c in the GD Graphics Library.

Vulnerability Detection Method
Get the installed version with the help of detect NVT and check the version is vulnerable or not.
Details:`PHP 'libgd' Denial of Service Vulnerability (Linux)`
OID:1.3.6.1.4.1.25623.1.0.809338
Version used: `$Revision: 5083 $`

Product Detection Result
Product: `cpe:/a:php:php:5.2.4`
Method: `PHP Version Detection (Remote)`
OID: 1.3.6.1.4.1.25623.1.0.800109)

References
`CVE: CVE-2016-7568`
`BID:93184`
`Other:`
`URL:http://www.php.net/ChangeLog-5.php`
`URL:http://www.php.net/ChangeLog-7.php`
`URL:http://seclists.org/oss-sec/2016/q3/639`
`URL:https://bugs.php.net/bug.php?id=73003`

High (CVSS: 10.0)
NVT: PHP 'phar_fix_filepath' Function Stack Buffer Overflow Vulnerability - Mar16 (Linux)

Product detection result
`cpe:/a:php:php:5.2.4`
`Detected by PHP Version Detection (Remote) (OID: 1.3.6.1.4.1.25623.1.0.800109)`

Summary
This host is installed with PHP and is prone to stack buffer overflow vulnerability.

Vulnerability Detection Result
`Installed version: 5.2.4`
`Fixed version: 5.4.43`

Impact

... continues on next page ...

... continued from previous page ...

Successfully exploiting this issue allow remote attackers to execute arbitrary code in the context of the PHP process. Failed exploit attempts will likely crash the webserver.
Impact Level: Application

Solution
Solution type: VendorFix
Upgrade to PHP version 5.4.43, or 5.5.27, or 5.6.11 or later. For updates refer to http://www.php.net

Affected Software/OS
PHP versions before 5.4.43, 5.5.x before 5.5.27, and 5.6.x before 5.6.11 on Linux

Vulnerability Insight
Multiple flaws are due to - Inadequate boundary checks on user-supplied input by 'phar_fix_filepath' function in 'ext/phar/phar.c' script. - Improper validation of file pointer in the 'phar_convert_to_other' function in 'ext/phar/phar_object.c' script.

Vulnerability Detection Method
Get the installed version with the help of detect NVT and check the version is vulnerable or not.
Details:`PHP 'phar_fix_filepath' Function Stack Buffer Overflow Vulnerability - Mar16 (L.`
`↪..`
OID:1.3.6.1.4.1.25623.1.0.807507
Version used: `$Revision: 5083 $`

Product Detection Result
Product: `cpe:/a:php:php:5.2.4`
Method: `PHP Version Detection (Remote)`
OID: 1.3.6.1.4.1.25623.1.0.800109)

References
`CVE: CVE-2015-5590, CVE-2015-8838, CVE-2015-5589`
`BID:75970, 88763, 75974`
`Other:`
`URL:http://www.php.net/ChangeLog-5.php`
`URL:https://bugs.php.net/bug.php?id=69923`

High (CVSS: 7.5)
NVT: PHP 'serialize_function_call' Function Type Confusion Vulnerability - Mar16 (Linux)

Product detection result
`cpe:/a:php:php:5.2.4`
`Detected by PHP Version Detection (Remote) (OID: 1.3.6.1.4.1.25623.1.0.800109)`

Summary

... continues on next page ...

... continued from previous page ...

This host is installed with PHP and is prone to remote code execution vulnerability.

Vulnerability Detection Result
Installed version: 5.2.4
Fixed version: 5.4.45

Impact
Successfully exploiting this issue allow remote attackers to execute arbitrary code in the context of the user running the affected application. Failed exploit attempts will likely cause a denial-of-service condition.
Impact Level: Application

Solution
Solution type: VendorFix
Upgrade to PHP version 5.4.45, or 5.5.29, or 5.6.13 or later. For updates refer to http://www.php.net

Affected Software/OS
PHP versions before 5.4.45, 5.5.x before 5.5.29, and 5.6.x before 5.6.13 on Linux

Vulnerability Insight
The flaw is due to 'SoapClient __call' method in 'ext/soap/soap.c' scripr does not properly manage headers.

Vulnerability Detection Method
Get the installed version with the help of detect NVT and check the version is vulnerable or not.
Details:PHP 'serialize_function_call' Function Type Confusion Vulnerability - Mar16 (Li.
↪..
OID:1.3.6.1.4.1.25623.1.0.807505
Version used: $Revision: 5083 $

Product Detection Result
Product: cpe:/a:php:php:5.2.4
Method: PHP Version Detection (Remote)
OID: 1.3.6.1.4.1.25623.1.0.800109)

References
CVE: CVE-2015-6836
BID:76644
Other:
URL:http://www.php.net/ChangeLog-5.php
URL:https://bugs.php.net/bug.php?id=70388

High (CVSS: 7.5)
NVT: PHP 'shmop_read()' Remote Integer Overflow Vulnerability

... continues on next page ...

... continued from previous page ...

Product detection result
cpe:/a:php:php:5.2.4
Detected by PHP Version Detection (Remote) (OID: 1.3.6.1.4.1.25623.1.0.800109)

Summary
PHP is prone to an integer-overflow vulnerability because it fails to ensure that integer values are not overrun.

Vulnerability Detection Result
Installed version: 5.2.4
Fixed version: 5.3.6

Impact
Successful exploits of this vulnerability allow remote attackers to execute arbitrary code in the context of a webserver affected by the issue. Failed attempts will likely result in denial-of-service conditions.

Solution
Solution type: VendorFix
Updates are available. Please see the references for more information.

Affected Software/OS
Versions prior to PHP 5.3.6 are vulnerable.

Vulnerability Detection Method
Details:PHP 'shmop_read()' Remote Integer Overflow Vulnerability
OID:1.3.6.1.4.1.25623.1.0.103113
Version used: $Revision: 4502 $

Product Detection Result
Product: cpe:/a:php:php:5.2.4
Method: PHP Version Detection (Remote)
OID: 1.3.6.1.4.1.25623.1.0.800109)

References
CVE: CVE-2011-1092
BID:46786
Other:
URL:https://www.securityfocus.com/bid/46786
URL:http://comments.gmane.org/gmane.comp.security.oss.general/4436
URL:http://www.php.net/
URL:http://svn.php.net/viewvc/?view=revision&revision=309018

High (CVSS: 7.5)
NVT: PHP 'SplObjectStorage' Unserializer Arbitrary Code Execution Vulnerability

Product detection result
cpe:/a:php:php:5.2.4
Detected by PHP Version Detection (Remote) (OID: 1.3.6.1.4.1.25623.1.0.800109)

Summary
PHP is prone to a vulnerability that an attacker could exploit to execute arbitrary code with the privileges of the user running the affected application.

Vulnerability Detection Result
Installed version: 5.2.4
Fixed version: 5.3.3

Impact
Successful exploits will compromise the application and possibly the computer.

Solution
Solution type: VendorFix
Updates are available please see the references for details.

Affected Software/OS
PHP 5 through 5.3.2 are vulnerable.

Vulnerability Detection Method
Details:PHP 'SplObjectStorage' Unserializer Arbitrary Code Execution Vulnerability
OID:1.3.6.1.4.1.25623.1.0.100684
Version used: $Revision: 4503 $

Product Detection Result
Product: cpe:/a:php:php:5.2.4
Method: PHP Version Detection (Remote)
OID: 1.3.6.1.4.1.25623.1.0.800109)

References
CVE: CVE-2010-2225
BID:40948
Other:
URL:https://www.securityfocus.com/bid/40948
URL:https://bugzilla.redhat.com/show_bug.cgi?id=605641
URL:http://www.php.net

High (CVSS: 7.5)
NVT: PHP 'sqlite_single_query()' and 'sqlite_array_query()' Arbitrary Code Execution Vulnerabilities

Product detection result
cpe:/a:php:php:5.2.4
Detected by PHP Version Detection (Remote) (OID: 1.3.6.1.4.1.25623.1.0.800109)

Summary
PHP is prone to multiple vulnerabilities that may allow attackers to execute arbitrary code.

Vulnerability Detection Result
Installed version: 5.2.4
Fixed version: 5.3.3/5.2.14

Impact
Attackers can exploit these issues to run arbitrary code within the context of the PHP process. This may allow them to bypass intended security restrictions or gain elevated privileges.

Solution
Solution type: VendorFix
Updates are available. Please see the references for more information.

Affected Software/OS
PHP 5.3.0 through 5.3.2, PHP 5.2.0 through 5.2.13 are vulnerable

Vulnerability Detection Method
Details:PHP 'sqlite_single_query()' and 'sqlite_array_query()' Arbitrary Code Execution.
↪..
OID:1.3.6.1.4.1.25623.1.0.100631
Version used: $Revision: 4503 $

Product Detection Result
Product: cpe:/a:php:php:5.2.4
Method: PHP Version Detection (Remote)
OID: 1.3.6.1.4.1.25623.1.0.800109)

References
CVE: CVE-2010-1868
BID:40013
Other:
URL:http://www.securityfocus.com/bid/40013
URL:http://php-security.org/2010/05/07/mops-2010-012-php-sqlite_single_query-
↪uninitialized-memory-usage-vulnerability/index.html
URL:http://php-security.org/2010/05/07/mops-2010-013-php-sqlite_array_query-u
↪ninitialized-memory-usage-vulnerability/index.html

... continues on next page ...

... continued from previous page ...

URL:http://www.php.net
URL:http://php-security.org/2010/05/07/mops-submission-03-sqlite_single_query
↪-sqlite_array_query-uninitialized-memory-usage/index.html

High (CVSS: 7.5)
NVT: PHP 'substr_replace()' Use After Free Vulnerability

Product detection result
cpe:/a:php:php:5.2.4
Detected by PHP Version Detection (Remote) (OID: 1.3.6.1.4.1.25623.1.0.800109)

Summary
This host is running PHP and is prone to Use After Free vulnerability.

Vulnerability Detection Result
Installed version: 5.2.4
Fixed version: 5.3.7

Impact
Successful exploitation could allow remote attackers to execute arbitrary code in the context of a web server. Failed attempts will likely result in denial-of-service conditions.
Impact Level: Network

Solution
Solution type: VendorFix
Upgrade to PHP version 5.3.7 or later. For updates refer to http://www.php.net/downloads.php

Affected Software/OS
PHP version 5.3.6 and prior.

Vulnerability Insight
The flaw is due to passing the same variable multiple times to the 'substr_replace()' function, which makes the PHP to use the same pointer in three variables inside the function.

Vulnerability Detection Method
Details:PHP 'substr_replace()' Use After Free Vulnerability
OID:1.3.6.1.4.1.25623.1.0.902356
Version used: $Revision: 4505 $

Product Detection Result
Product: cpe:/a:php:php:5.2.4
Method: PHP Version Detection (Remote)
OID: 1.3.6.1.4.1.25623.1.0.800109)

... continues on next page ...

... continued from previous page ...

References
CVE: CVE-2011-1148
BID:46843
Other:
URL:http://bugs.php.net/bug.php?id=54238
URL:http://openwall.com/lists/oss-security/2011/03/13/3

High (CVSS: 10.0)
NVT: PHP 'type confusion' Denial of Service Vulnerability (Linux)

Product detection result
cpe:/a:php:php:5.2.4
Detected by PHP Version Detection (Remote) (OID: 1.3.6.1.4.1.25623.1.0.800109)

Summary
This host is installed with PHP and is prone to denial of service vulnerability.

Vulnerability Detection Result
Installed version: 5.2.4
Fixed version: 5.6.7

Impact
Successfully exploiting this issue allow remote attackers to cause a denial of service.
Impact Level: Application

Solution
Solution type: VendorFix
Upgrade to PHP version 5.6.7 or later. For updates refer to http://www.php.net

Affected Software/OS
PHP versions prior to 5.6.7 on Linux

Vulnerability Insight
The flaw is due to 'type confusion' issues in 'ext/soap/php_encoding.c', 'ext/soap/php_http.c', and 'ext/soap/soap.c' scripts.

Vulnerability Detection Method
Get the installed version with the help of detect NVT and check the version is vulnerable or not.
Details:PHP 'type confusion' Denial of Service Vulnerability (Linux)
OID:1.3.6.1.4.1.25623.1.0.808673
Version used: $Revision: 5083 $

Product Detection Result
Product: cpe:/a:php:php:5.2.4
Method: PHP Version Detection (Remote)

... continues on next page ...

... continued from previous page ...

OID: 1.3.6.1.4.1.25623.1.0.800109)

References
CVE: CVE-2015-4601
BID:75246
Other:
URL:http://www.php.net/ChangeLog-5.php

High (CVSS: 7.5)
NVT: PHP 'var_unserializer' Denial of Service Vulnerability (Linux)

Product detection result
cpe:/a:php:php:5.2.4
Detected by PHP Version Detection (Remote) (OID: 1.3.6.1.4.1.25623.1.0.800109)

Summary
This host is installed with PHP and is prone to denial of service vulnerability.

Vulnerability Detection Result
Installed version: 5.2.4
Fixed version: 5.6.26

Impact
Successfully exploiting this issue allow remote attackers to cause a denial of service.
Impact Level: Application

Solution
Solution type: VendorFix
Upgrade to PHP version 5.6.26, or later. For updates refer to http://www.php.net

Affected Software/OS
PHP versions prior to 5.6.26 on Linux

Vulnerability Insight
The flaw is due to improper handling of object-deserialization failures in 'ext/standard/var_unserializer.re' script.

Vulnerability Detection Method
Get the installed version with the help of detect NVT and check the version is vulnerable or not.
Details:PHP 'var_unserializer' Denial of Service Vulnerability (Linux)
OID:1.3.6.1.4.1.25623.1.0.809321
Version used: $Revision: 5083 $

Product Detection Result

... continues on next page ...

... continued from previous page ...

Product: cpe:/a:php:php:5.2.4
Method: PHP Version Detection (Remote)
OID: 1.3.6.1.4.1.25623.1.0.800109)

References
CVE: CVE-2016-7411
BID:93009
Other:
URL:http://www.php.net/ChangeLog-5.php

High (CVSS: 10.0)
NVT: PHP < 5.2.12 Multiple Vulnerabilities

Product detection result
cpe:/a:php:php:5.2.4
Detected by PHP Version Detection (Remote) (OID: 1.3.6.1.4.1.25623.1.0.800109)

Summary
PHP is prone to a cross-site scripting vulnerability and to a code execution vulnerability.

Vulnerability Detection Result
Installed version: 5.2.4
Fixed version: 5.2.12

Impact
Attackers can exploit the code execution vulnerability to execute arbitrary code within the context of the PHP process. This may allow them to bypass intended security restrictions or gain elevated privileges.
An attacker may leverage the cross-site scripting vulnerability to execute arbitrary script code in the browser of an unsuspecting user in the context of the affected site. This may let the attacker steal cookie-based authentication credentials and launch other attacks.

Solution
Solution type: VendorFix
Updates are available please see the references for more information.

Affected Software/OS
Versions prior to PHP 5.2.12 are vulnerable.

Vulnerability Detection Method
Details:PHP < 5.2.12 Multiple Vulnerabilities
OID:1.3.6.1.4.1.25623.1.0.100409
Version used: $Revision: 4505 $

... continues on next page ...

... continued from previous page ...

Product Detection Result
Product: cpe:/a:php:php:5.2.4
Method: PHP Version Detection (Remote)
OID: 1.3.6.1.4.1.25623.1.0.800109)

References
CVE: CVE-2009-4143, CVE-2009-4142
BID:37390, 37389
Other:
URL:http://www.securityfocus.com/bid/37390
URL:http://www.securityfocus.com/bid/37389
URL:http://www.php.net/ChangeLog-5.php#5.2.12
URL:http://www.php.net/releases/5_2_12.php
URL:http://www.php.net
URL:http://www.suspekt.org/downloads/POC2009-ShockingNewsInPHPExploitation.pdf
URL:http://www.blackhat.com/presentations/bh-usa-09/ESSER/BHUSA09-Esser-PostExploitationPHP-PAPER.pdf
URL:http://d.hatena.ne.jp/t_komura/20091004/1254665511
URL:http://bugs.php.net/bug.php?id=49785

High (CVSS: 7.5)
NVT: PHP < 5.2.13 Multiple Vulnerabilities

Product detection result
cpe:/a:php:php:5.2.4
Detected by PHP Version Detection (Remote) (OID: 1.3.6.1.4.1.25623.1.0.800109)

Summary
The remote web server has installed a PHP Version which is prone to Multiple Vulnerabilities.

Vulnerability Detection Result
Installed version: 5.2.4
Fixed version: 5.2.13

Solution
Solution type: VendorFix
Updates are available. Please see the references for details.

Affected Software/OS
PHP versions prior to 5.2.13 are affected.

Vulnerability Insight
Multiple vulnerabilities exist due to:

... continues on next page ...

... continued from previous page ...

1. A 'safe_mode' restriction-bypass vulnerability. Successful exploits could allow an attacker to write session files in arbitrary directions.
2. A 'safe_mode' restriction-bypass vulnerability. Successful exploits could allow an attacker to access files in unauthorized locations or create files in any writable directory.
3. An unspecified security vulnerability that affects LCG entropy.

Vulnerability Detection Method
Details:PHP < 5.2.13 Multiple Vulnerabilities
OID:1.3.6.1.4.1.25623.1.0.100511
Version used: $Revision: 4505 $

Product Detection Result
Product: cpe:/a:php:php:5.2.4
Method: PHP Version Detection (Remote)
OID: 1.3.6.1.4.1.25623.1.0.800109)

References
CVE: CVE-2010-1128, CVE-2010-1129
BID:38182, 38431, 38430
Other:
URL:http://www.securityfocus.com/bid/38182
URL:http://www.securityfocus.com/bid/38431
URL:http://www.securityfocus.com/bid/38430
URL:http://securityreason.com/achievement_securityalert/82
URL:http://www.php.net/releases/5_2_13.php
URL:http://www.php.net
URL:http://svn.php.net/viewvc/php/php-src/branches/PHP_5_2/ext/session/sessio
↪n.c?r1=293036&r2=294272
URL:http://svn.php.net/viewvc/php/php-src/branches/PHP_5_3/ext/session/sessio
↪n.c?r1=293036&r2=294272

High (CVSS: 7.5)
NVT: PHP Arbitrary Code Execution Vulnerability - Aug16 (Linux)

Product detection result
cpe:/a:php:php:5.2.4
Detected by PHP Version Detection (Remote) (OID: 1.3.6.1.4.1.25623.1.0.800109)

Summary
This host is installed with PHP and is prone to arbitrary code execution vulnerability

Vulnerability Detection Result
Installed version: 5.2.4
Fixed version: 5.5.27

... continues on next page ...

... continued from previous page ...

Impact
Successfully exploiting this issue allow remote attackers to execute arbitrary code by triggering a failed SplMinHeap::compare operation.
Impact Level: Application

Solution
Solution type: VendorFix
Upgrade to PHP version 5.5.27, or 5.6.11, or later. For updates refer to http://www.php.net

Affected Software/OS
PHP versions prior to 5.5.27 and 5.6.x before 5.6.11 on Linux.

Vulnerability Insight
The flaw is due to Use-after-free vulnerability in the 'spl_ptr_heap_insert' function in 'ext/spl/spl_heap.c'.

Vulnerability Detection Method
Get the installed version with the help of detect NVT and check the version is vulnerable or not.
Details:`PHP Arbitrary Code Execution Vulnerability - Aug16 (Linux)`
OID:1.3.6.1.4.1.25623.1.0.808671
Version used: `$Revision: 5083 $`

Product Detection Result
Product: `cpe:/a:php:php:5.2.4`
Method: `PHP Version Detection (Remote)`
OID: 1.3.6.1.4.1.25623.1.0.800109)

References
`CVE: CVE-2015-4116`
`BID:75127`
`Other:`
`URL:http://www.php.net/ChangeLog-5.php`

High (CVSS: 10.0)
NVT: PHP Denial of Service And Unspecified Vulnerabilities - 01 - Jul16 (Linux)

Product detection result
`cpe:/a:php:php:5.2.4`
`Detected by PHP Version Detection (Remote) (OID: 1.3.6.1.4.1.25623.1.0.800109)`

Summary
This host is installed with PHP and is prone to denial of service and unspecified Vulnerabilities

... continues on next page ...

... continued from previous page ...

Vulnerability Detection Result
Installed version: 5.2.4
Fixed version: 5.5.32

Impact
Successfully exploiting this issue allow remote attackers to cause a denial of service (heap memory corruption) or possibly have unspecified other impact.
Impact Level: Application

Solution
Solution type: VendorFix
Upgrade to PHP version 5.5.32, or 5.6.18, or 7.0.3, or later. For updates refer to http://www.php.net

Affected Software/OS
PHP versions prior to 5.5.32, 5.6.x before 5.6.18, and 7.x before 7.0.3 on Linux

Vulnerability Insight
The flaw is due an improper handling of zero-length uncompressed data in 'ext/phar/phar_object.c' script.

Vulnerability Detection Method
Get the installed version with the help of detect NVT and check the version is vulnerable or not.
Details:PHP Denial of Service And Unspecified Vulnerabilities - 01 - Jul16 (Linux)
OID:1.3.6.1.4.1.25623.1.0.808607
Version used: $Revision: 5083 $

Product Detection Result
Product: cpe:/a:php:php:5.2.4
Method: PHP Version Detection (Remote)
OID: 1.3.6.1.4.1.25623.1.0.800109)

References
CVE: CVE-2016-4342, CVE-2016-2554
BID:89154, 83353
Other:
URL:http://www.php.net/ChangeLog-7.php
URL:http://www.openwall.com/lists/oss-security/2016/04/28/2

High (CVSS: 7.1)
NVT: PHP Denial of Service Vulnerability - 01 - Jul16 (Linux)

Product detection result
cpe:/a:php:php:5.2.4
Detected by PHP Version Detection (Remote) (OID: 1.3.6.1.4.1.25623.1.0.800109)

... continues on next page ...

... continued from previous page ...

Summary
This host is installed with PHP and is prone to denial of service vulnerability.

Vulnerability Detection Result
`Installed version: 5.2.4`
`Fixed version: 5.5.28`

Impact
Successfully exploiting this issue allow remote attackers to cause a denial of service (race condition and heap memory corruption) by leveraging an application that performs many temporary-file accesses.
Impact Level: Application

Solution
Solution type: VendorFix
Upgrade to PHP version 5.5.28, or 5.6.12, or later. For updates refer to http://www.php.net

Affected Software/OS
PHP versions prior to 5.5.28 and 5.6.x before 5.6.12 on Linux

Vulnerability Insight
The flaw is due to script 'main/php_open_temporary_file.c' does not ensure thread safety.

Vulnerability Detection Method
Get the installed version with the help of detect NVT and check the version is vulnerable or not.
Details:`PHP Denial of Service Vulnerability - 01 - Jul16 (Linux)`
OID:1.3.6.1.4.1.25623.1.0.808613
Version used: `$Revision: 5083 $`

Product Detection Result
Product: `cpe:/a:php:php:5.2.4`
Method: `PHP Version Detection (Remote)`
OID: 1.3.6.1.4.1.25623.1.0.800109)

References
`CVE: CVE-2015-8878`
`BID:90837`
`Other:`
`URL:http://www.php.net/ChangeLog-5.php`

High (CVSS: 7.5)
NVT: PHP Directory Traversal Vulnerability - Jul16 (Linux)

... continues on next page ...

... continued from previous page ...

Product detection result
cpe:/a:php:php:5.2.4
Detected by PHP Version Detection (Remote) (OID: 1.3.6.1.4.1.25623.1.0.800109)

Summary
This host is installed with PHP and is prone to Directory traversal vulnerability.

Vulnerability Detection Result
Installed version: 5.2.4
Fixed version: 5.4.45

Impact
Successfully exploiting this issue allow remote attackers to read arbitrary empty directories, also to cause a denial of service.
Impact Level: Application

Solution
Solution type: VendorFix
Upgrade to PHP version 5.4.45, or 5.5.29, or 5.6.13, or later. For updates refer to http://www.php.net

Affected Software/OS
PHP versions prior to 5.4.45, 5.5.x before 5.5.29, and 5.6.x before 5.6.13 on Linux

Vulnerability Insight
Multiple flaws are due to - An error in the 'ZipArchive::extractTo' function in 'ext/zip/php_zip.c' script. - The xsl_ext_function_php function in ext/xsl/xsltprocessor.c when libxml2 is used, does not consider the possibility of a NULL valuePop return value before proceeding with a free operation after the principal argument loop. - Improper handling of multiple php_var_unserialize calls. - Multiple use-after-free vulnerabilities.

Vulnerability Detection Method
Get the installed version with the help of detect NVT and check the version is vulnerable or not.
Details:PHP Directory Traversal Vulnerability - Jul16 (Linux)
OID:1.3.6.1.4.1.25623.1.0.808617
Version used: $Revision: 5083 $

Product Detection Result
Product: cpe:/a:php:php:5.2.4
Method: PHP Version Detection (Remote)
OID: 1.3.6.1.4.1.25623.1.0.800109)

References
CVE: CVE-2014-9767, CVE-2015-6834, CVE-2015-6835, CVE-2015-6837, CVE-2015-6838
BID:76652, 76649, 76733, 76734, 76738

... continues on next page ...

... continued from previous page ...

```
Other:
  URL:http://www.php.net/ChangeLog-5.php
   URL:http://www.openwall.com/lists/oss-security/2016/03/16/20
```

High (CVSS: 10.0)
NVT: PHP End Of Life Detection (Linux)

Product detection result
`cpe:/a:php:php:5.2.4`
`Detected by PHP Version Detection (Remote) (OID: 1.3.6.1.4.1.25623.1.0.800109)`

Summary
The PHP version on the remote host has reached the end of life and should not be used anymore.

Vulnerability Detection Result
`Installed version: 5.2.4`
`Fixed version: 5.6/7.0`

Impact
An end of life version of PHP is not receiving any security updates from the vendor. Unfixed security vulnerabilities might be leveraged by an attacker to compromise the security of this host.

Solution
Solution type: VendorFix
Update the PHP version on the remote host to a still supported version.

Affected Software/OS
PHP versions below PHP 5.6

Vulnerability Insight
Each release branch of PHP is fully supported for two years from its initial stable release. During this period, bugs and security issues that have been reported are fixed and are released in regular point releases.
After this two year period of active support, each branch is then supported for an additional year for critical security issues only. Releases during this period are made on an as-needed basis: there may be multiple point releases, or none, depending on the number of reports.
Once the three years of support are completed, the branch reaches its end of life and is no longer supported.

Vulnerability Detection Method
Get the installed version with the help of the detect NVT and check if the version is unsupported.
Details:`PHP End Of Life Detection (Linux)`
OID:1.3.6.1.4.1.25623.1.0.105889
Version used: `$Revision: 5580 $`

... continues on next page ...

... continued from previous page ...

Product Detection Result
Product: cpe:/a:php:php:5.2.4
Method: PHP Version Detection (Remote)
OID: 1.3.6.1.4.1.25623.1.0.800109)

References
Other:
URL:https://secure.php.net/supported-versions.php

High (CVSS: 10.0)
NVT: PHP Heap-based buffer overflow in 'mbstring' extension

Product detection result
cpe:/a:php:php:5.2.4
Detected by PHP Version Detection (Remote) (OID: 1.3.6.1.4.1.25623.1.0.800109)

Summary
The host is running PHP and is prone to Buffer Overflow vulnerability.

Vulnerability Detection Result
Installed version: 5.2.4
Fixed version: 5.2.7

Impact
Successful exploitation could allow attackers to execute arbitrary code via a crafted string containing an HTML entity.
Impact Level: Application

Solution
Solution type: VendorFix
Upgrade to version 5.2.7 or later, http://www.php.net/downloads.php

Affected Software/OS
PHP version 4.3.0 to 5.2.6 on all running platform.

Vulnerability Insight
The flaw is due to error in mbfilter_htmlent.c file in the mbstring extension. These can be exploited via mb_convert_encoding, mb_check_encoding, mb_convert_variables, and mb_parse_str functions.

Vulnerability Detection Method
Details:PHP Heap-based buffer overflow in 'mbstring' extension
OID:1.3.6.1.4.1.25623.1.0.900185
Version used: $Revision: 4505 $

... continues on next page ...

... continued from previous page ...

Product Detection Result
Product: cpe:/a:php:php:5.2.4
Method: PHP Version Detection (Remote)
OID: 1.3.6.1.4.1.25623.1.0.800109)

References
CVE: CVE-2008-5557
BID:32948
Other:
URL:http://bugs.php.net/bug.php?id=45722
URL:http://archives.neohapsis.com/archives/fulldisclosure/2008-12/0477.html

High (CVSS: 7.5)
NVT: PHP Interruptions and Calltime Arbitrary Code Execution Vulnerability

Product detection result
cpe:/a:php:php:5.2.4
Detected by PHP Version Detection (Remote) (OID: 1.3.6.1.4.1.25623.1.0.800109)

Summary
PHP is prone to a vulnerability that an attacker could exploit to execute arbitrary code with the privileges of the user running the affected application.

Vulnerability Detection Result
Installed version: 5.2.4
Fixed version: N/A

Impact
Successful exploits will compromise the application and possibly the computer.

Vulnerability Detection Method
Details:PHP Interruptions and Calltime Arbitrary Code Execution Vulnerability
OID:1.3.6.1.4.1.25623.1.0.100252
Version used: $Revision: 4505 $

Product Detection Result
Product: cpe:/a:php:php:5.2.4
Method: PHP Version Detection (Remote)
OID: 1.3.6.1.4.1.25623.1.0.800109)

References
BID:35867
Other:

... continues on next page ...

... continued from previous page ...

URL:http://www.securityfocus.com/bid/35867
URL:http://www.php.net
URL:http://www.blackhat.com/presentations/bh-usa-09/ESSER/BHUSA09-Esser-PostE
↪xploitationPHP-PAPER.pdf

High (CVSS: 7.5)
NVT: PHP Multiple Buffer Overflow Vulnerabilities

Product detection result
cpe:/a:php:php:5.2.4
Detected by PHP Version Detection (Remote) (OID: 1.3.6.1.4.1.25623.1.0.800109)

Summary
PHP is prone to multiple buffer-overflow vulnerabilities.

Vulnerability Detection Result
Installed version: 5.2.4
Fixed version: 5.2.8

Impact
Successful exploits may allow attackers to execute arbitrary code in the context of applications using the vulnerable PHP functions. This may result in a compromise of the underlying system. Failed attempts may lead to a denial-of-service condition.

Solution
Solution type: VendorFix
Updates are available. Please see the references for more information.

Affected Software/OS
Versions prior to PHP 4.4.9 and PHP 5.2.8 are vulnerable.

Vulnerability Detection Method
Details:PHP Multiple Buffer Overflow Vulnerabilities
OID:1.3.6.1.4.1.25623.1.0.100583
Version used: $Revision: 4503 $

Product Detection Result
Product: cpe:/a:php:php:5.2.4
Method: PHP Version Detection (Remote)
OID: 1.3.6.1.4.1.25623.1.0.800109)

References
CVE: CVE-2008-3659, CVE-2008-3658
BID:30649

... continues on next page ...

... continued from previous page ...

```
Other:
  URL:http://www.securityfocus.com/bid/30649
   URL:http://www.php.net/ChangeLog-5.php#5.2.8
   URL:http://www.php.net/archive/2008.php#id2008-08-07-1
   URL:http://www.php.net/
   URL:http://support.avaya.com/elmodocs2/security/ASA-2009-161.htm
```

High (CVSS: 7.5)
NVT: PHP Multiple Buffer Overflow Vulnerabilities - Jan15

Product detection result
`cpe:/a:php:php:5.2.4`
`Detected by PHP Version Detection (Remote) (OID: 1.3.6.1.4.1.25623.1.0.800109)`

Summary
This host is installed with PHP and is prone to denial of service and arbitrary code execution vulnerability.

Vulnerability Detection Result
`Installed version: 5.2.4`
`Fixed version: 5.2.7`

Impact
Successful exploitation will allow remote attackers to cause a denial of service or possibly execute arbitrary code.
Impact Level: Application

Solution
Solution type: VendorFix
Upgrade to PHP version 5.2.7 or later

Affected Software/OS
PHP versions 5.2.x before 5.2.7

Vulnerability Insight
The multiple flaws are due to - Improper validation of user supplied input passed to date_from_ISO8601() function in xmlrpc.c - including a timezone field in a date, leading to improper XML-RPC encoding.

Vulnerability Detection Method
Get the installed version with the help of detect NVT and check the version is vulnerable or not.
Details:`PHP Multiple Buffer Overflow Vulnerabilities - Jan15`
OID:1.3.6.1.4.1.25623.1.0.805410
Version used: `$Revision: 4498 $`

... continues on next page ...

... continued from previous page ...

Product Detection Result
Product: cpe:/a:php:php:5.2.4
Method: PHP Version Detection (Remote)
OID: 1.3.6.1.4.1.25623.1.0.800109)

References
CVE: CVE-2014-8626
BID:70928
Other:
URL:https://bugs.php.net/bug.php?id=45226
URL:http://openwall.com/lists/oss-security/2014/11/06/3

High (CVSS: 7.5)
NVT: PHP Multiple Denial of Service Vulnerabilities - 02 - Jan17 (Linux)

Product detection result
cpe:/a:php:php:5.2.4
Detected by PHP Version Detection (Remote) (OID: 1.3.6.1.4.1.25623.1.0.800109)

Summary
This host is installed with PHP and is prone to multiple denial of service vulnerabilities.

Vulnerability Detection Result
Installed version: 5.2.4
Fixed version: 5.6.30

Impact
Successfully exploiting this issue allow remote attackers to cause a denial of service (memory consumption or application crash).
Impact Level: Application

Solution
Solution type: VendorFix
Upgrade to PHP version 5.6.30, 7.0.15 or later. For updates refer to http://www.php.net

Affected Software/OS
PHP versions before 5.6.30 and 7.0.x before 7.0.15

Vulnerability Insight
Multiple flaws are due to - A integer overflow in the phar_parse_pharfile function in ext/phar/phar.c via a truncated manifest entry in a PHAR archive.
- A off-by-one error in the phar_parse_pharfile function in ext/phar/phar.c via a crafted PHAR archive with an alias mismatch.

... continues on next page ...

... continued from previous page ...

Vulnerability Detection Method
Get the installed version with the help of the detect NVT and check if the version is vulnerable or not.
Details:PHP Multiple Denial of Service Vulnerabilities - 02 - Jan17 (Linux)
OID:1.3.6.1.4.1.25623.1.0.108054
Version used: $Revision: 5132 $

Product Detection Result
Product: cpe:/a:php:php:5.2.4
Method: PHP Version Detection (Remote)
OID: 1.3.6.1.4.1.25623.1.0.800109)

References
CVE: CVE-2016-10159, CVE-2016-10160
Other:
URL:http://www.php.net/ChangeLog-5.php
URL:http://www.php.net/ChangeLog-7.php

High (CVSS: 7.5)
NVT: PHP Multiple Double Free Vulnerabilities - Jan15

Product detection result
cpe:/a:php:php:5.2.4
Detected by PHP Version Detection (Remote) (OID: 1.3.6.1.4.1.25623.1.0.800109)

Summary
This host is installed with PHP and is prone to denial of service vulnerability.

Vulnerability Detection Result
Installed version: 5.2.4
Fixed version: 5.5.21/5.6.5

Impact
Successful exploitation will allow remote attackers to cause a denial of service or possibly have unspecified other impact.
Impact Level: Application

Solution
Solution type: VendorFix
Upgrade to PHP version 5.5.21 or 5.6.5 or later

Affected Software/OS
PHP versions through 5.5.20 and 5.6.x through 5.6.4

... continues on next page ...

... continued from previous page ...

Vulnerability Insight
Multiple flaws are due to: - Double free error in the 'zend_ts_hash_graceful_destroy' function in 'zend_ts_hash.c script in the Zend Engine in PHP. - flaw in the 'GetCode_' function in 'gd_gif_in.c' script in GD Graphics Library (LibGD).

Vulnerability Detection Method
Get the installed version with the help of detect NVT and check the version is vulnerable or not.
Details:`PHP Multiple Double Free Vulnerabilities - Jan15`
OID:1.3.6.1.4.1.25623.1.0.805412
Version used: `$Revision: 4498 $`

Product Detection Result
Product: `cpe:/a:php:php:5.2.4`
Method: `PHP Version Detection (Remote)`
OID: 1.3.6.1.4.1.25623.1.0.800109)

References
`CVE: CVE-2014-9425, CVE-2014-9709`
`BID:71800, 73306`
`Other:`
`URL:http://securitytracker.com/id/1031479`
`URL:https://bugs.php.net/bug.php?id=68676`

High (CVSS: 7.5)
NVT: PHP Multiple Vulnerabilities - 01 - Apr16 (Linux)

Product detection result
`cpe:/a:php:php:5.2.4`
`Detected by PHP Version Detection (Remote) (OID: 1.3.6.1.4.1.25623.1.0.800109)`

Summary
This host is installed with PHP and is prone to multiple vulnerabilities.

Vulnerability Detection Result
`Installed version: 5.2.4`
`Fixed version: 5.5.33`

Impact
Successfully exploiting this issue allow remote attackers to gain access to potentially sensitive information and conduct a denial of service (memory corruption and application crash).
Impact Level: Application

Solution
Solution type: VendorFix

... continues on next page ...

... continued from previous page ...

Upgrade to PHP version 5.5.33 or 5.6.19 or later. For updates refer to http://www.php.net

Affected Software/OS
PHP versions before 5.5.33, and 5.6.x before 5.6.19 on Linux

Vulnerability Insight
Multiple flaws are due to, - A use-after-free error in wddx.c script in the WDDX extension in PHP - An error in the phar_parse_zipfile function in zip.c script in the PHAR extension in PHP.

Vulnerability Detection Method
Get the installed version with the help of detect NVT and check the version is vulnerable or not.
Details:`PHP Multiple Vulnerabilities - 01 - Apr16 (Linux)`
OID:1.3.6.1.4.1.25623.1.0.807807
Version used: `$Revision: 5083 $`

Product Detection Result
Product: `cpe:/a:php:php:5.2.4`
Method: `PHP Version Detection (Remote)`
OID: 1.3.6.1.4.1.25623.1.0.800109)

References
```
CVE: CVE-2016-3142, CVE-2016-3141
Other:
  URL:https://bugs.php.net/bug.php?id=71587
   URL:https://bugs.php.net/bug.php?id=71498
   URL:https://secure.php.net/ChangeLog-5.php
```

High (CVSS: 7.5)
NVT: PHP Multiple Vulnerabilities - 01 - Aug16 (Linux)

Product detection result
```
cpe:/a:php:php:5.2.4
Detected by PHP Version Detection (Remote) (OID: 1.3.6.1.4.1.25623.1.0.800109)
```

Summary
This host is installed with PHP and is prone to multiple vulnerabilities.

Vulnerability Detection Result
```
Installed version: 5.2.4
Fixed version:     5.5.37
```

Impact
Successfully exploiting this issue allow remote attackers to cause a denial of service (buffer overflow and application crash) or possibly execute arbitrary code.

... continues on next page ...

... continued from previous page ...

Impact Level: Application

Solution
Solution type: VendorFix
Upgrade to PHP version 5.5.37, or 5.6.23, or 7.0.8, or later. For updates refer to http://www.php.net

Affected Software/OS
PHP versions prior to 5.5.37, 5.6.x before 5.6.23, and 7.x before 7.0.8 on Linux

Vulnerability Insight
Multiple flaws are due to, - The 'php_zip.c' script in the zip extension improperly interacts with the unserialize implementation and garbage collection. - The php_wddx_process_data function in 'wddx.c' script in the WDDX extension mishandled data in a wddx_deserialize call. - The multiple integer overflows in 'mcrypt.c' script in the mcrypt extension. - The double free vulnerability in the '_php_mb_regex_ereg_replace_exec' function in 'php_mbregex.c' script in the mbstring extension. - An integer overflow in the '_gd2GetHeader' function in 'gd_gd2.c' script in the GD Graphics Library. - An integer overflow in the 'gdImageCreate' function in 'gd.c' script in the GD Graphics Library.

Vulnerability Detection Method
Get the installed version with the help of detect NVT and check the version is vulnerable or not.
Details:`PHP Multiple Vulnerabilities - 01 - Aug16 (Linux)`
OID:1.3.6.1.4.1.25623.1.0.808788
Version used: `$Revision: 5083 $`

Product Detection Result
Product: `cpe:/a:php:php:5.2.4`
Method: `PHP Version Detection (Remote)`
OID: 1.3.6.1.4.1.25623.1.0.800109)

References
```
CVE: CVE-2016-5773, CVE-2016-5772, CVE-2016-5769, CVE-2016-5768, CVE-2016-5766,
↪CVE-2016-5767
BID:91397, 91398, 91399, 91396, 91395
Other:
  URL:http://www.php.net/ChangeLog-5.php
   URL:http://www.php.net/ChangeLog-7.php
```

High (CVSS: 7.5)
NVT: PHP Multiple Vulnerabilities - 01 - Jul16 (Linux)

Product detection result
```
cpe:/a:php:php:5.2.4
Detected by PHP Version Detection (Remote) (OID: 1.3.6.1.4.1.25623.1.0.800109)
```

... continues on next page ...

... continued from previous page ...

Summary
This host is installed with PHP and is prone to multiple vulnerabilities.

Vulnerability Detection Result
`Installed version: 5.2.4`
`Fixed version: 5.5.34`

Impact
Successfully exploiting this issue allow remote attackers to cause a denial of service (buffer overflow and application crash) or possibly execute arbitrary code.
Impact Level: Application

Solution
Solution type: VendorFix
Upgrade to PHP version 5.5.34, or 5.6.20, or 7.0.5, or later. For updates refer to http://www.php.net

Affected Software/OS
PHP versions prior to 5.5.34, 5.6.x before 5.6.20, and 7.x before 7.0.5 on Linux

Vulnerability Insight
Multiple flaws are due to, - Multiple integer overflows in the mbfl_strcut function in 'ext/mbstring/libmbfl/mbfl/mbfilter.c' script. - A format string vulnerability in the php_snmp_error function in 'ext/snmp/snmp.c' script. - An improper handling of '\0' characters by the 'phar_analyze_path' function in 'ext/phar/phar.c' script. - An integer overflow in the 'php_raw_url_encode' function in 'ext/standard/url.c' script - An improper handling of continuation-level jumps in 'file_check_mem' function in 'funcs.c' script.

Vulnerability Detection Method
Get the installed version with the help of detect NVT and check the version is vulnerable or not.
Details:`PHP Multiple Vulnerabilities - 01 - Jul16 (Linux)`
OID:1.3.6.1.4.1.25623.1.0.808199
Version used: `$Revision: 5083 $`

Product Detection Result
Product: `cpe:/a:php:php:5.2.4`
Method: `PHP Version Detection (Remote)`
OID: 1.3.6.1.4.1.25623.1.0.800109)

References
`CVE: CVE-2016-4070, CVE-2016-4071, CVE-2016-4072, CVE-2016-4073, CVE-2015-8865`
`BID:85800, 85801, 85802, 85991, 85993`
`Other:`
`URL:http://www.php.net/ChangeLog-5.php`

... continues on next page ...

... continued from previous page ...

URL:http://www.php.net/ChangeLog-7.php

High (CVSS: 7.5)
NVT: PHP Multiple Vulnerabilities - 01 - Mar16 (Linux)

Product detection result
cpe:/a:php:php:5.2.4
Detected by PHP Version Detection (Remote) (OID: 1.3.6.1.4.1.25623.1.0.800109)

Summary
This host is installed with PHP and is prone to multiple vulnerabilities.

Vulnerability Detection Result
Installed version: 5.2.4
Fixed version: 5.4.44

Impact
Successfully exploiting this issue allow remote attackers to execute arbitrary code and to create or overwrite arbitrary files on the system and this may lead to launch further attacks.
Impact Level: Application

Solution
Solution type: VendorFix
Upgrade to PHP version 5.4.44 or 5.5.28 or 5.6.12 or later. For updates refer to http://www.php.net

Affected Software/OS
PHP versions before 5.4.44, 5.5.x before 5.5.28, and 5.6.x before 5.6.12 on Linux

Vulnerability Insight
Multiple flaws are due to, - The multiple use-after-free vulnerabilities in SPL unserialize implementation. - An insufficient validation of user supplied input by 'phar/phar_object.c' script.

Vulnerability Detection Method
Get the installed version with the help of detect NVT and check the version is vulnerable or not.
Details:PHP Multiple Vulnerabilities - 01 - Mar16 (Linux)
OID:1.3.6.1.4.1.25623.1.0.807503
Version used: $Revision: 5083 $

Product Detection Result
Product: cpe:/a:php:php:5.2.4
Method: PHP Version Detection (Remote)
OID: 1.3.6.1.4.1.25623.1.0.800109)

... continues on next page ...

... continued from previous page ...

References
CVE: CVE-2015-6831, CVE-2015-6832, CVE-2015-6833
BID:76737, 76739, 76735
Other:
URL:https://bugs.php.net/bug.php?id=70068
URL:http://www.openwall.com/lists/oss-security/2015/08/19/3

High (CVSS: 7.5)
NVT: PHP Multiple Vulnerabilities - 02 - Aug16 (Linux)

Product detection result
cpe:/a:php:php:5.2.4
Detected by PHP Version Detection (Remote) (OID: 1.3.6.1.4.1.25623.1.0.800109)

Summary
This host is installed with PHP and is prone to multiple vulnerabilities.

Vulnerability Detection Result
Installed version: 5.2.4
Fixed version: 5.5.37

Impact
Successfully exploiting this issue allow remote attackers to cause a denial of service (use-after-free and application crash) or possibly execute arbitrary code or possibly have unspecified other impact via a large integer argument.
Impact Level: Application

Solution
Solution type: VendorFix
Upgrade to PHP version 5.5.37, or 5.6.23, or later. For updates refer to http://www.php.net

Affected Software/OS
PHP versions prior to 5.5.37 and 5.6.x before 5.6.23 on Linux

Vulnerability Insight
Multiple flaws are due to, - The 'spl_array.c' in the SPL extension improperly interacts with the unserialize implementation and garbage collection. - The integer overflow in the 'SplFileObject::fread' function in 'spl_directory.c' in the SPL extension.

Vulnerability Detection Method
Get the installed version with the help of detect NVT and check the version is vulnerable or not.
Details:PHP Multiple Vulnerabilities - 02 - Aug16 (Linux)
OID:1.3.6.1.4.1.25623.1.0.808790
Version used: $Revision: 5083 $

... continues on next page ...

... continued from previous page ...

Product Detection Result
Product: cpe:/a:php:php:5.2.4
Method: PHP Version Detection (Remote)
OID: 1.3.6.1.4.1.25623.1.0.800109)

References
CVE: CVE-2016-5771, CVE-2016-5770
BID:91401, 91403
Other:
URL:http://www.php.net/ChangeLog-5.php

High (CVSS: 7.5)
NVT: PHP Multiple Vulnerabilities - 02 - Jan15

Product detection result
cpe:/a:php:php:5.2.4
Detected by PHP Version Detection (Remote) (OID: 1.3.6.1.4.1.25623.1.0.800109)

Summary
This host is installed with PHP and is prone to multiple vulnerbilities.

Vulnerability Detection Result
Installed version: 5.2.4
Fixed version: 5.6.5

Impact
Successful exploitation will allow remote attackers to cause a denial of service or possibly have unspecified other impact.
Impact Level: Application

Solution
Solution type: VendorFix
Upgrade to PHP version 5.6.5 or later

Affected Software/OS
PHP versions before 5.6.5

Vulnerability Insight
The flaw is due to a free operation on a stack-based character array by The apprentice_load function in libmagic/apprentice.c in the Fileinfo component.

Vulnerability Detection Method
Get the installed version with the help of detect NVT and check the version is vulnerable or not.
Details:PHP Multiple Vulnerabilities - 02 - Jan15

... continues on next page ...

... continued from previous page ...

OID:1.3.6.1.4.1.25623.1.0.805413
Version used: $Revision: 4498 $

Product Detection Result
Product: cpe:/a:php:php:5.2.4
Method: PHP Version Detection (Remote)
OID: 1.3.6.1.4.1.25623.1.0.800109)

References
CVE: CVE-2014-9426
Other:
URL:https://bugs.php.net/bug.php?id=68665
URL:http://securitytracker.com/id/1031480

High (CVSS: 7.5)
NVT: PHP Multiple Vulnerabilities - 02 - Sep16 (Linux)

Product detection result
cpe:/a:php:php:5.2.4
Detected by PHP Version Detection (Remote) (OID: 1.3.6.1.4.1.25623.1.0.800109)

Summary
This host is installed with PHP and is prone to multiple vulnerabilities.

Vulnerability Detection Result
Installed version: 5.2.4
Fixed version: 5.6.25

Impact
Successfully exploiting this issue allow remote attackers to cause a denial of service, to obtain sensitive information from process memory, to inject arbitrary-type session data by leveraging control of a session name.
Impact Level: Application

Solution
Solution type: VendorFix
Upgrade to PHP version 5.6.25, or 7.0.10, or later. For updates refer to http://www.php.net

Affected Software/OS
PHP versions prior to 5.6.25 and 7.x before 7.0.10 on Linux

Vulnerability Insight

... continues on next page ...

... continued from previous page ...

Multiple flaws are due to - An invalid wddxPacket XML document that is mishandled in a wddx_deserialize call in 'ext/wddx/wddx.c' script. - An error in 'php_wddx_pop_element' function in 'ext/wddx/wddx.c' script. - An error in 'php_wddx_process_data' function in 'ext/wddx/wddx.c' script. - Improper handling of the case of a thumbnail offset that exceeds the file size in 'exif_process_IFD_in_TIFF' function in 'ext/exif/exif.c' script. - Improper validation of gamma values in 'imagegammacorrect' function in 'ext/gd/gd.c' script. - Improper validation of number of colors in 'imagegammacorrect' function in 'ext/gd/gd.c' script. - The script 'ext/session/session.c' skips invalid session names in a way that triggers incorrect parsing. - Improper handling of certain objects in 'ext/standard/var_unserializer.c' script.

Vulnerability Detection Method
Get the installed version with the help of detect NVT and check the version is vulnerable or not.
Details:`PHP Multiple Vulnerabilities - 02 - Sep16 (Linux)`
OID:1.3.6.1.4.1.25623.1.0.809319
Version used: `$Revision: 5083 $`

Product Detection Result
Product: `cpe:/a:php:php:5.2.4`
Method: `PHP Version Detection (Remote)`
OID: 1.3.6.1.4.1.25623.1.0.800109)

References
```
CVE: CVE-2016-7124, CVE-2016-7125, CVE-2016-7126, CVE-2016-7127, CVE-2016-7128,
↪CVE-2016-7129, CVE-2016-7130, CVE-2016-7131, CVE-2016-7132
BID:92756, 92552, 92755, 92757, 92564, 92758
Other:
  URL:http://www.php.net/ChangeLog-7.php
   URL:http://www.php.net/ChangeLog-5.php
```

High (CVSS: 7.5)
NVT: PHP Multiple Vulnerabilities - 03 - Aug16 (Linux)

Product detection result
```
cpe:/a:php:php:5.2.4
Detected by PHP Version Detection (Remote) (OID: 1.3.6.1.4.1.25623.1.0.800109)
```

Summary
This host is installed with PHP and is prone to multiple vulnerabilities.

Vulnerability Detection Result
```
Installed version: 5.2.4
Fixed version:     5.5.36
```

Impact

... continues on next page ...

... continued from previous page ...

Successfully exploiting this issue allow remote attackers to cause a denial of service or possibly have unspecified other impact.
Impact Level: Application

Solution
Solution type: VendorFix
Upgrade to PHP version 5.5.36, or 5.6.22, or later. For updates refer to http://www.php.net

Affected Software/OS
PHP versions prior to 5.5.36 and 5.6.x before 5.6.22 on Linux

Vulnerability Insight
Multiple flaws are due to, - An integer overflow in the fread function in 'ext/standard/file.c' script. - An integer overflow in the php_html_entities function in 'ext/standard/html.c' script. - An Integer overflow in the php_escape_html_entities_ex function in 'ext/standard/html.c' script.

Vulnerability Detection Method
Get the installed version with the help of detect NVT and check the version is vulnerable or not.
Details:`PHP Multiple Vulnerabilities - 03 - Aug16 (Linux)`
OID:1.3.6.1.4.1.25623.1.0.808792
Version used: `$Revision: 5083 $`

Product Detection Result
Product: `cpe:/a:php:php:5.2.4`
Method: `PHP Version Detection (Remote)`
OID: 1.3.6.1.4.1.25623.1.0.800109)

References
```
CVE: CVE-2016-5096 , CVE-2016-5094, CVE-2016-5095
BID:90861, 90857, 92144
Other:
  URL:http://www.php.net/ChangeLog-5.php
```

High (CVSS: 7.5)
NVT: PHP Multiple Vulnerabilities - 03 - Jul16 (Linux)

Product detection result
`cpe:/a:php:php:5.2.4`
`Detected by PHP Version Detection (Remote) (OID: 1.3.6.1.4.1.25623.1.0.800109)`

Summary
This host is installed with PHP and is prone to multiple vulnerabilities.

... continues on next page ...

... continued from previous page ...

Vulnerability Detection Result
Installed version: 5.2.4
Fixed version: 5.5.35

Impact
Successfully exploiting this issue allow remote attackers to cause a denial of service (out-of-bounds read) or possibly have unspecified other impact.
Impact Level: Application

Solution
Solution type: VendorFix
Upgrade to PHP version 5.5.35, or 5.6.21, or 7.0.6, or later. For updates refer to http://www.php.net

Affected Software/OS
PHP versions prior to 5.5.35, 5.6.x before 5.6.21, and 7.x before 7.0.6 on Linux.

Vulnerability Insight
The multiple flaws are due to, - An improper validation of TIFF start data in 'exif_process_TIFF_in_JPEG' function in 'ext/exif/exif.c' script. - An improper validation of IFD sizes in 'exif_process_TIFF_in_JPEG' function in 'ext/exif/exif.c' script. - An improper construction of spprintf arguments,in 'exif_process_TIFF_in_JPEG' function in 'ext/exif/exif.c' script. - An error in 'grapheme_strpos function' in 'ext/intl/grapheme/grapheme_string.c'. - An error in 'xml_parse_into_struct' function in 'ext/xml/xml.c' script. - The 'bcpowmod' function in 'ext/bcmath/bcmath.c' improperly modifies certain data structures. - An improper validation of input passed to 'bcpowmod' function in 'ext/bcmath/bcmath.c' script. - An error in 'grapheme_strpos' function in ext/intl/grapheme/grapheme_string.c script.

Vulnerability Detection Method
Get the installed version with the help of detect NVT and check the version is vulnerable or not.
Details:PHP Multiple Vulnerabilities - 03 - Jul16 (Linux)
OID:1.3.6.1.4.1.25623.1.0.808603
Version used: $Revision: 5083 $

Product Detection Result
Product: cpe:/a:php:php:5.2.4
Method: PHP Version Detection (Remote)
OID: 1.3.6.1.4.1.25623.1.0.800109)

References
CVE: CVE-2016-4537, CVE-2016-4538, CVE-2016-4539, CVE-2016-4540, CVE-2016-4541,
↪CVE-2016-4542, CVE-2016-4543, CVE-2016-4544
BID:89844, 90172, 90173, 90174
Other:
URL:http://www.php.net/ChangeLog-5.php

... continues on next page ...

... continued from previous page ...

URL:http://www.php.net/ChangeLog-7.php

High (CVSS: 7.5)
NVT: PHP Multiple Vulnerabilities - 03 - Sep16 (Linux)

Product detection result
cpe:/a:php:php:5.2.4
Detected by PHP Version Detection (Remote) (OID: 1.3.6.1.4.1.25623.1.0.800109)

Summary
This host is installed with PHP and is prone to multiple vulnerabilities.

Vulnerability Detection Result
Installed version: 5.2.4
Fixed version: 5.6.26

Impact
Successfully exploiting this issue allow remote attackers to cause a denial of service, or possibly have unspecified other impact.
Impact Level: Application

Solution
Solution type: VendorFix
Upgrade to PHP version 5.6.25, or 7.0.10, or later. For updates refer to http://www.php.net

Affected Software/OS
PHP versions prior to 5.6.25 and 7.x before 7.0.10 on Linux

Vulnerability Insight
Multiple flaws are due to, - Use-after-free vulnerability in the 'wddx_stack_destroy' function in 'ext/wddx/wddx.c' script. - Improper varification of a BIT field has the UNSIGNED_FLAG flag in 'ext/mysqlnd/mysqlnd_wireprotocol.c' script. - The ZIP signature-verification feature does not ensure that the uncompressed_filesize field is large enough. - The script 'ext/spl/spl_array.c' proceeds with SplArray unserialization without validating a return value and data type. - The script 'ext/intl/msgformat/msgformat_format.c' does not properly restrict the locale length provided to the Locale class in the ICU library. - An error in the php_wddx_push_element function in ext/wddx/wddx.c.

Vulnerability Detection Method
Get the installed version with the help of detect NVT and check the version is vulnerable or not.
Details:PHP Multiple Vulnerabilities - 03 - Sep16 (Linux)
OID:1.3.6.1.4.1.25623.1.0.809317
Version used: $Revision: 5083 $

Product Detection Result

... continues on next page ...

... continued from previous page ...

Product: cpe:/a:php:php:5.2.4
Method: PHP Version Detection (Remote)
OID: 1.3.6.1.4.1.25623.1.0.800109)

References

CVE: CVE-2016-7412, CVE-2016-7413, CVE-2016-7414, CVE-2016-7416, CVE-2016-7417, ↪CVE-2016-7418
BID:93005, 93006, 93004, 93022, 93008, 93007, 93011
Other:
URL:http://www.php.net/ChangeLog-7.php
URL:http://www.php.net/ChangeLog-5.php

High (CVSS: 7.5)
NVT: PHP Multiple Vulnerabilities - 04 - Aug16 (Linux)

Product detection result

cpe:/a:php:php:5.2.4
Detected by PHP Version Detection (Remote) (OID: 1.3.6.1.4.1.25623.1.0.800109)

Summary

This host is installed with PHP and is prone to multiple vulnerabilities.

Vulnerability Detection Result

Installed version: 5.2.4
Fixed version: 5.5.36

Impact

Successfully exploiting this issue allow remote attackers to cause a denial of service (out-of-bounds read) or possibly have unspecified other impact.
Impact Level: Application

Solution

Solution type: VendorFix
Upgrade to PHP version 5.5.36, or 5.6.22, or 7.0.7, or later. For updates refer to http://www.php.net

Affected Software/OS

PHP versions prior to 5.5.36, 5.6.x before 5.6.22, and 7.x before 7.0.7 on Linux

Vulnerability Insight

Multiple flaws are due to, - The 'get_icu_value_internal' function in 'ext/intl/locale/locale_methods.c' script does not ensure the presence of a '\0' character. - The 'gd_interpolation.c' script in the GD Graphics Library mishandled by the imagescale function.

... continues on next page ...

... continued from previous page ...

Vulnerability Detection Method
Get the installed version with the help of detect NVT and check the version is vulnerable or not.
Details:PHP Multiple Vulnerabilities - 04 - Aug16 (Linux)
OID:1.3.6.1.4.1.25623.1.0.808794
Version used: $Revision: 5083 $

Product Detection Result
Product: cpe:/a:php:php:5.2.4
Method: PHP Version Detection (Remote)
OID: 1.3.6.1.4.1.25623.1.0.800109)

References
CVE: CVE-2013-7456, CVE-2016-5093
BID:90946, 90859
Other:
URL:http://www.php.net/ChangeLog-5.php
URL:http://www.php.net/ChangeLog-7.php

High (CVSS: 7.5)
NVT: PHP Multiple Vulnerabilities - 04 - Jul16 (Linux)

Product detection result
cpe:/a:php:php:5.2.4
Detected by PHP Version Detection (Remote) (OID: 1.3.6.1.4.1.25623.1.0.800109)

Summary
This host is installed with PHP and is prone to multiple vulnerabilities.

Vulnerability Detection Result
Installed version: 5.2.4
Fixed version: 5.4.44

Impact
Successfully exploiting this issue allow remote attackers to cause a denial of service (NULL pointer dereference and application crash) or trigger unintended method execution to defeat cryptographic protection mechanisms.
Impact Level: Application

Solution
Solution type: VendorFix
Upgrade to PHP version 5.4.44, or 5.5.28, or 5.6.12, or later. For updates refer to http://www.php.net

Affected Software/OS

... continues on next page ...

... continued from previous page ...

PHP versions prior to 5.4.44, 5.5.x before 5.5.28, and 5.6.x before 5.6.12 on Linux

Vulnerability Insight
The multiple flaws are due to, - An improper validation of certain Exception objects in 'Zend/zend_exceptions.c' script. - The 'openssl_random_pseudo_bytes' function in 'ext/openssl/openssl.c' incorrectly relies on the deprecated 'RAND_pseudo_bytes' function.

Vulnerability Detection Method
Get the installed version with the help of detect NVT and check the version is vulnerable or not.
Details:`PHP Multiple Vulnerabilities - 04 - Jul16 (Linux)`
OID:1.3.6.1.4.1.25623.1.0.808604
Version used: `$Revision: 5083 $`

Product Detection Result
Product: `cpe:/a:php:php:5.2.4`
Method: `PHP Version Detection (Remote)`
OID: 1.3.6.1.4.1.25623.1.0.800109)

References
`CVE: CVE-2015-8867, CVE-2015-8876, CVE-2015-8873, CVE-2015-8835`
`BID:87481, 90867, 84426, 90712`
`Other:`
`URL:http://www.php.net/ChangeLog-5.php`

High (CVSS: 7.5)
NVT: PHP Multiple Vulnerabilities - 05 - Aug16 (Linux)

Product detection result
`cpe:/a:php:php:5.2.4`
`Detected by PHP Version Detection (Remote) (OID: 1.3.6.1.4.1.25623.1.0.800109)`

Summary
This host is installed with PHP and is prone to multiple vulnerabilities.

Vulnerability Detection Result
`Installed version: 5.2.4`
`Fixed version: 5.4.42`

Impact
Successfully exploiting this issue allow remote attackers to cause a denial of service, to read or write to arbitrary files, also execute arbitrary code via a long reply to a LIST command, leading to a heap-based buffer overflow.
Impact Level: Application

... continues on next page ...

... continued from previous page ...

Solution
Solution type: VendorFix
Upgrade to PHP version 5.4.42, or 5.5.26, or 5.6.10, or later. For updates refer to http://www.php.net

Affected Software/OS
PHP versions prior to 5.4.42, 5.5.x before 5.5.26, and 5.6.x before 5.6.10 on Linux

Vulnerability Insight
The multiple flaws are due to, - Improper validation of token extraction for table names, in the php_pgsql_meta_data function in pgsql.c in the PostgreSQL extension. - Integer overflow in the ftp_genlist function in ext/ftp/ftp.c - PHP does not ensure that pathnames lack %00 sequences.

Vulnerability Detection Method
Get the installed version with the help of detect NVT and check the version is vulnerable or not.
Details:`PHP Multiple Vulnerabilities - 05 - Aug16 (Linux)`
OID:1.3.6.1.4.1.25623.1.0.808675
Version used: `$Revision: 5083 $`

Product Detection Result
Product: `cpe:/a:php:php:5.2.4`
Method: `PHP Version Detection (Remote)`
OID: 1.3.6.1.4.1.25623.1.0.800109)

References
`CVE: CVE-2015-4644, CVE-2015-4643, CVE-2015-4598`
`BID:75291, 75292, 75244`
`Other:`
`URL:http://www.php.net/ChangeLog-5.php`

High (CVSS: 7.5)
NVT: PHP Multiple Vulnerabilities - 05 - Jul16 (Linux)

Product detection result
`cpe:/a:php:php:5.2.4`
`Detected by PHP Version Detection (Remote) (OID: 1.3.6.1.4.1.25623.1.0.800109)`

Summary
This host is installed with PHP and is prone to multiple vulnerabilities.

Vulnerability Detection Result
`Installed version: 5.2.4`
`Fixed version: 5.5.38`

... continues on next page ...

... continued from previous page ...

Impact
Successfully exploiting this issue may allow attackers to cause a denial of service obtain sensitive information from process memory, or possibly have unspecified other impact.
Impact Level: Application

Solution
Solution type: VendorFix
Upgrade to PHP version 5.5.38, or 5.6.24, or 7.0.9, or later. For updates refer to http://www.php.net

Affected Software/OS
PHP versions before 5.5.38, 5.6.x before 5.6.24, and 7.x before 7.0.9 on Linux

Vulnerability Insight
Multiple flaws are due to - An integer overflow in the 'php_stream_zip_opener' function in 'ext/zip/zip_stream.c' script. - An integer signedness error in the 'simplestring_addn' function in 'simplestring.c' in xmlrpc-epi. - The 'ext/snmp/snmp.c' script improperly interacts with the unserialize implementation and garbage collection. - The 'locale_accept_from_http' function in 'ext/intl/locale/locale_methods.c' script does not properly restrict calls to the ICU 'uloc_acceptLanguageFromHTTP' function. - An error in the 'exif_process_user_comment' function in 'ext/exif/exif.c' script. - An error in the 'exif_process_IFD_in_MAKERNOTE' function in 'ext/exif/exif.c' script. - The 'ext/session/session.c' does not properly maintain a certain hash data structure. - An integer overflow in the 'virtual_file_ex' function in 'TSRM/tsrm_virtual_cwd.c' script. - An error in the 'php_url_parse_ex' function in 'ext/standard/url.c' script.

Vulnerability Detection Method
Get the installed version with the help of detect NVT and check the version is vulnerable or not.
Details:`PHP Multiple Vulnerabilities - 05 - Jul16 (Linux)`
OID:1.3.6.1.4.1.25623.1.0.808634
Version used: `$Revision: 5083 $`

Product Detection Result
Product: `cpe:/a:php:php:5.2.4`
Method: `PHP Version Detection (Remote)`
OID: 1.3.6.1.4.1.25623.1.0.800109)

References
`CVE: CVE-2016-6288, CVE-2016-6289, CVE-2016-6290, CVE-2016-6291, CVE-2016-6292,`
`↪CVE-2016-6294, CVE-2016-6295, CVE-2016-6296, CVE-2016-6297`
`BID:92111, 92074, 92097, 92073, 92078, 92115, 92094, 92095, 92099`
`Other:`
`URL:http://php.net/ChangeLog-5.php`
`URL:http://php.net/ChangeLog-7.php`
`URL:http://openwall.com/lists/oss-security/2016/07/24/2`

High (CVSS: 10.0)
NVT: PHP Multiple Vulnerabilities - Aug08

Product detection result
cpe:/a:php:php:5.2.4
Detected by PHP Version Detection (Remote) (OID: 1.3.6.1.4.1.25623.1.0.800109)

Summary
The host is installed with PHP, that is prone to multiple vulnerabilities.

Vulnerability Detection Result
Installed version: 5.2.4
Fixed version: 5.2.6

Impact
Successful exploitation could result in remote arbitrary code execution, security restrictions bypass, access to restricted files, denial of service.
Impact Level: System

Solution
Solution type: VendorFix
Upgrade to PHP version 5.2.6 or above, http://www.php.net/downloads.php

Affected Software/OS
PHP version prior to 5.2.6

Vulnerability Insight
The flaws are caused by, - an unspecified stack overflow error in FastCGI SAPI (fastcgi.c). - an error during path translation in cgi_main.c. - an error with an unknown impact/attack vectors. - an unspecified error within the processing of incomplete multibyte characters in escapeshellcmd() API function. - error in curl/interface.c in the cURL library(libcurl), which could be exploited by attackers to bypass safe_mode security restrictions. - an error in PCRE. i.e buffer overflow error when handling a character class containing a very large number of characters with codepoints greater than 255(UTF-8 mode).

Vulnerability Detection Method
Details:PHP Multiple Vulnerabilities - Aug08
OID:1.3.6.1.4.1.25623.1.0.800110
Version used: $Revision: 4505 $

Product Detection Result
Product: cpe:/a:php:php:5.2.4
Method: PHP Version Detection (Remote)
OID: 1.3.6.1.4.1.25623.1.0.800109)

References
. . . continues on next page . . .

... continued from previous page ...

CVE: CVE-2008-2050, CVE-2008-2051, CVE-2007-4850, CVE-2008-0599, CVE-2008-0674
BID:29009, 27413, 27786
Other:
CB-A:08-0118
URL:http://pcre.org/changelog.txt
URL:http://www.php.net/ChangeLog-5.php
URL:http://wiki.rpath.com/wiki/Advisories:rPSA-2008-0176
URL:http://wiki.rpath.com/wiki/Advisories:rPSA-2008-0178
URL:http://wiki.rpath.com/wiki/Advisories:rPSA-2008-0086

High (CVSS: 7.5)
NVT: PHP Multiple Vulnerabilities - Dec09

Product detection result
cpe:/a:php:php:5.2.4
Detected by PHP Version Detection (Remote) (OID: 1.3.6.1.4.1.25623.1.0.800109)

Summary
This host is running PHP and is prone to multiple vulnerabilities.

Vulnerability Detection Result
Installed version: 5.2.4
Fixed version: 5.2.11

Impact
Successful exploitation could allow local attackers to bypass certain security restrictions and cause denial of service.
Impact Level: Network

Solution
Solution type: VendorFix
Upgrade to PHP version 5.3.1, http://www.php.net/downloads.php

Affected Software/OS
PHP version 5.2.10 and prior. PHP version 5.3.x before 5.3.1

Vulnerability Insight
Multiple flaws are due to: - Error in 'proc_open()' function in 'ext/standard/proc_open.c' that does not enforce the 'safe_mode_allowed_env_vars' and 'safe_mode_protected_env_vars' directives, which allows attackers to execute programs with an arbitrary environment via the env parameter. - Error in 'zend_restore_ini_entry_cb()' function in 'zend_ini.c', which allows attackers to obtain sensitive information.

Vulnerability Detection Method
Get the installed version of PHP with the help of detect NVT and check the version is vulnerable or not.

... continues on next page ...

... continued from previous page ...

Details:PHP Multiple Vulnerabilities - Dec09
OID:1.3.6.1.4.1.25623.1.0.801060
Version used: $Revision: 4504 $

Product Detection Result
Product: cpe:/a:php:php:5.2.4
Method: PHP Version Detection (Remote)
OID: 1.3.6.1.4.1.25623.1.0.800109)

References
CVE: CVE-2009-4018, CVE-2009-2626
BID:37138, 36009
Other:
URL:http://secunia.com/advisories/37482
URL:http://bugs.php.net/bug.php?id=49026
URL:http://securityreason.com/achievement_securityalert/65
URL:http://www.openwall.com/lists/oss-security/2009/11/23/15

High (CVSS: 7.5)
NVT: PHP Multiple Vulnerabilities - Sep09

Product detection result
cpe:/a:php:php:5.2.4
Detected by PHP Version Detection (Remote) (OID: 1.3.6.1.4.1.25623.1.0.800109)

Summary
This host is running PHP and is prone to multiple vulnerabilities.

Vulnerability Detection Result
Installed version: 5.2.4
Fixed version: 5.2.11

Impact
Successful exploitation will allow attackers to spoof certificates and can cause unknown impacts in the context of the web application.
Impact Level: Application

Solution
Solution type: VendorFix
Upgrade to version 5.2.11 or later http://www.php.net/downloads.php

Affected Software/OS
PHP version prior to 5.2.11

... continues on next page ...

... continued from previous page ...

Vulnerability Insight
- An error in 'php_openssl_apply_verification_policy' function that does not properly perform certificate validation. - An input validation error exists in the processing of 'exif' data. - An unspecified error exists related to the sanity check for the color index in the 'imagecolortransparent' function.

Vulnerability Detection Method
Details:PHP Multiple Vulnerabilities - Sep09
OID:1.3.6.1.4.1.25623.1.0.900871
Version used: $Revision: 4505 $

Product Detection Result
Product: cpe:/a:php:php:5.2.4
Method: PHP Version Detection (Remote)
OID: 1.3.6.1.4.1.25623.1.0.800109)

References
CVE: CVE-2009-3291, CVE-2009-3292, CVE-2009-3293
BID:36449
Other:
URL:http://secunia.com/advisories/36791
URL:http://www.php.net/releases/5_2_11.php
URL:http://www.php.net/ChangeLog-5.php#5.2.11
URL:http://www.openwall.com/lists/oss-security/2009/09/20/1

High (CVSS: 7.5)
NVT: PHP Out of Bounds Read Multiple Vulnerabilities - Jan15

Product detection result
cpe:/a:php:php:5.2.4
Detected by PHP Version Detection (Remote) (OID: 1.3.6.1.4.1.25623.1.0.800109)

Summary
This host is installed with PHP and is prone to denial of service vulnerability.

Vulnerability Detection Result
Installed version: 5.2.4
Fixed version: 5.4.37/5.5.21/5.6.5

Impact
Successful exploitation will allow remote attackers to obtain sensitive information and trigger unexpected code execution .
Impact Level: Application

Solution

... continues on next page ...

... continued from previous page ...

Solution type: VendorFix
Upgrade to PHP version 5.4.37 or 5.5.21 or 5.6.5 or later

Affected Software/OS
PHP versions through 5.4.36, 5.5.x through 5.5.20, and 5.6.x through 5.6.4

Vulnerability Insight
The flaw is due to an out-of-bounds read error in sapi/cgi/cgi_main.c in the CGI component in PHP.

Vulnerability Detection Method
Get the installed version with the help of detect NVT and check the version is vulnerable or not.
Details:`PHP Out of Bounds Read Multiple Vulnerabilities - Jan15`
OID:1.3.6.1.4.1.25623.1.0.805414
Version used: `$Revision: 4498 $`

Product Detection Result
Product: `cpe:/a:php:php:5.2.4`
Method: `PHP Version Detection (Remote)`
OID: 1.3.6.1.4.1.25623.1.0.800109)

References
`CVE: CVE-2014-9427`
`BID:71833`
`Other:`
`URL:https://bugs.php.net/bug.php?id=68618`

High (CVSS: 7.5)
NVT: PHP Remote Code Execution and Denial of Service Vulnerabilities - Dec13

Product detection result
`cpe:/a:php:php:5.2.4`
`Detected by PHP Version Detection (Remote) (OID: 1.3.6.1.4.1.25623.1.0.800109)`

Summary
This host is installed with PHP and is prone to remote code execution vulnerability.

Vulnerability Detection Result
`Installed version: 5.2.4`
`Fixed version: 5.3.28/5.4.23/5.5.7`

Impact
Successful exploitation will allow remote attackers to execute arbitrary code or cause a denial of service (memory corruption).

... continues on next page ...

... continued from previous page ...

Impact Level: Application

Solution
Solution type: VendorFix
Update to PHP version 5.3.28 or 5.4.23 or 5.5.7 or later. For updates refer to http://www.php.net

Affected Software/OS
PHP versions before 5.3.28, 5.4.x before 5.4.23, and 5.5.x before 5.5.7.

Vulnerability Insight
The flaw is due to a boundary error within the 'asn1_time_to_time_t' function in 'ext/openssl/openssl.c' when parsing X.509 certificates.

Vulnerability Detection Method
Get the installed version of PHP with the help of detect NVT and check the version is vulnerable or not.
Details:`PHP Remote Code Execution and Denial of Service Vulnerabilities - Dec13`
OID:1.3.6.1.4.1.25623.1.0.804174
Version used: `$Revision: 4500 $`

Product Detection Result
Product: `cpe:/a:php:php:5.2.4`
Method: `PHP Version Detection (Remote)`
OID: 1.3.6.1.4.1.25623.1.0.800109)

References
`CVE: CVE-2013-6420`
`Other:`
`URL:http://secunia.com/advisories/56055`
`URL:http://packetstormsecurity.com/files/124436/PHP-openssl_x509_parse-Memory-Corruption.html`

High (CVSS: 7.5)
NVT: PHP Security Bypass and File Writing Vulnerability - Dec08

Product detection result
`cpe:/a:php:php:5.2.4`
`Detected by PHP Version Detection (Remote) (OID: 1.3.6.1.4.1.25623.1.0.800109)`

Summary
The host is running PHP and is prone to Security Bypass and File Writing vulnerability.

Vulnerability Detection Result
`Installed version: 5.2.4`

... continues on next page ...

... continued from previous page ...

Fixed version: 5.2.7

Impact
Successful exploitation could allow remote attackers to write arbitrary file, bypass security restrictions and cause directory traversal attacks.
Impact Level: System/Application

Solution
Solution type: VendorFix
Upgrade to version 5.2.7 or later http://www.php.net/downloads.php

Affected Software/OS
PHP versions prior to 5.2.7.

Vulnerability Insight
The flaw is due to, - An error in initialization of 'page_uid' and 'page_gid' global variables for use by the SAPI 'php_getuid' function, which bypass the safe_mode restrictions. - When 'safe_mode' is enabled through a 'php_admin_flag' setting in 'httpd.conf' file, which does not enforce the 'error_log', 'safe_mode restrictions. - In 'ZipArchive::extractTo' function which allows attacker to write files via a ZIP file.

Vulnerability Detection Method
Details:PHP Security Bypass and File Writing Vulnerability - Dec08
OID:1.3.6.1.4.1.25623.1.0.900184
Version used: $Revision: 4505 $

Product Detection Result
Product: cpe:/a:php:php:5.2.4
Method: PHP Version Detection (Remote)
OID: 1.3.6.1.4.1.25623.1.0.800109)

References
CVE: CVE-2008-5624, CVE-2008-5625, CVE-2008-5658
BID:32383, 32625, 32688
Other:
URL:http://www.php.net/ChangeLog-5.php#5.2.7
URL:http://www.php.net/archive/2008.php#id2008-12-07-1
URL:http://www.securityfocus.com/archive/1/archive/1/498985/100/0/threaded

High (CVSS: 7.5)
NVT: PHP Version < 5.2.11 Multiple Vulnerabilities

Product detection result
cpe:/a:php:php:5.2.4
Detected by PHP Version Detection (Remote) (OID: 1.3.6.1.4.1.25623.1.0.800109)

... continues on next page ...

... continued from previous page ...

Summary
PHP version smaller than 5.2.11 suffers from multiple vulnerabilities.

Vulnerability Detection Result
`Installed version: 5.2.4`
`Fixed version: 5.2.11`

Solution
Solution type: VendorFix
Update PHP to version 5.2.11 or later.

Vulnerability Detection Method
Details:`PHP Version < 5.2.11 Multiple Vulnerabilities`
OID:1.3.6.1.4.1.25623.1.0.110176
Version used: `$Revision: 4506 $`

Product Detection Result
Product: `cpe:/a:php:php:5.2.4`
Method: `PHP Version Detection (Remote)`
OID: 1.3.6.1.4.1.25623.1.0.800109)

References
`CVE: CVE-2009-3291, CVE-2009-3292, CVE-2009-3293, CVE-2009-3294, CVE-2009-4018,`
`↪CVE-2009-5016`
`BID:36449, 44889`

High (CVSS: 9.3)
NVT: PHP Version < 5.2.14 Multiple Vulnerabilities

Product detection result
`cpe:/a:php:php:5.2.4`
`Detected by PHP Version Detection (Remote) (OID: 1.3.6.1.4.1.25623.1.0.800109)`

Summary
PHP version smaller than 5.2.14 suffers from multiple vulnerabilities.

Vulnerability Detection Result
`Installed version: 5.2.4`
`Fixed version: 5.2.14`

Solution
Solution type: VendorFix

... continues on next page ...

... continued from previous page ...

Update PHP to version 5.2.14 or later.

Vulnerability Detection Method
Details:PHP Version < 5.2.14 Multiple Vulnerabilities
OID:1.3.6.1.4.1.25623.1.0.110171
Version used: $Revision: 4506 $

Product Detection Result
Product: cpe:/a:php:php:5.2.4
Method: PHP Version Detection (Remote)
OID: 1.3.6.1.4.1.25623.1.0.800109)

References
CVE: CVE-2007-1581, CVE-2010-0397, CVE-2010-1860, CVE-2010-1862, CVE-2010-1864,
↪CVE-2010-2097, CVE-2010-2100, CVE-2010-2101, CVE-2010-2190, CVE-2010-2191, CVE
↪-2010-2225, CVE-2010-2484, CVE-2010-2531, CVE-2010-3065
BID:38708, 40948, 41991

High (CVSS: 9.3)
NVT: PHP Version < 5.2.5 Multiple Vulnerabilities

Product detection result
cpe:/a:php:php:5.2.4
Detected by PHP Version Detection (Remote) (OID: 1.3.6.1.4.1.25623.1.0.800109)

Summary
PHP version smaller than 5.2.5 suffers from multiple vulnerabilities.

Vulnerability Detection Result
Installed version: 5.2.4
Fixed version: 5.2.5

Solution
Solution type: VendorFix
Update PHP to version 5.2.5 or later.

Vulnerability Detection Method
Details:PHP Version < 5.2.5 Multiple Vulnerabilities
OID:1.3.6.1.4.1.25623.1.0.110179
Version used: $Revision: 4506 $

Product Detection Result
Product: cpe:/a:php:php:5.2.4
Method: PHP Version Detection (Remote)

... continues on next page ...

... continued from previous page ...

OID: 1.3.6.1.4.1.25623.1.0.800109)

References

CVE: CVE-2007-3996, CVE-2007-4782, CVE-2007-4783, CVE-2007-4784, CVE-2007-4825, ↪CVE-2007-4840, CVE-2007-4887, CVE-2007-4889, CVE-2007-5447, CVE-2007-5653, CVE ↪-2007-5898, CVE-2007-5899, CVE-2007-5900, CVE-2008-2107, CVE-2008-2108, CVE-20 ↪08-4107
BID:26403

High (CVSS: 10.0)
NVT: PHP Version < 5.2.6 Multiple Vulnerabilities

Product detection result

cpe:/a:php:php:5.2.4
Detected by PHP Version Detection (Remote) (OID: 1.3.6.1.4.1.25623.1.0.800109)

Summary

PHP version smaller than 5.2.6 suffers from multiple vulnerabilities.

Vulnerability Detection Result

Installed version: 5.2.4
Fixed version: 5.2.6

Solution

Solution type: VendorFix
Update PHP to version 5.2.6 or later.

Vulnerability Detection Method

Details:PHP Version < 5.2.6 Multiple Vulnerabilities
OID:1.3.6.1.4.1.25623.1.0.110183
Version used: $Revision: 4506 $

Product Detection Result

Product: cpe:/a:php:php:5.2.4
Method: PHP Version Detection (Remote)
OID: 1.3.6.1.4.1.25623.1.0.800109)

References

CVE: CVE-2007-4850, CVE-2007-6039, CVE-2008-0599, CVE-2008-1384, CVE-2008-2050, ↪CVE-2008-2051
BID:27413, 28392, 29009

High (CVSS: 10.0)
NVT: PHP Version < 5.2.7 Multiple Vulnerabilities

Product detection result
cpe:/a:php:php:5.2.4
Detected by PHP Version Detection (Remote) (OID: 1.3.6.1.4.1.25623.1.0.800109)

Summary
PHP version smaller than 5.2.7 suffers from multiple vulnerabilities.

Vulnerability Detection Result
Installed version: 5.2.4
Fixed version: 5.2.7

Solution
Solution type: VendorFix
Update PHP to version 5.2.7 or later.

Vulnerability Detection Method
Details:PHP Version < 5.2.7 Multiple Vulnerabilities
OID:1.3.6.1.4.1.25623.1.0.110172
Version used: $Revision: 4506 $

Product Detection Result
Product: cpe:/a:php:php:5.2.4
Method: PHP Version Detection (Remote)
OID: 1.3.6.1.4.1.25623.1.0.800109)

References
CVE: CVE-2008-2371, CVE-2008-2665, CVE-2008-2666, CVE-2008-2829, CVE-2008-3658,
↪CVE-2008-3659, CVE-2008-3660, CVE-2008-5557, CVE-2008-5624, CVE-2008-5625, CVE
↪-2008-5658
BID:29796, 29797, 29829, 30087, 30649, 31612, 32383, 32625, 32688, 32948

High (CVSS: 7.5)
NVT: PHP Version < 5.2.8 Multiple Vulnerabilities

Product detection result
cpe:/a:php:php:5.2.4
Detected by PHP Version Detection (Remote) (OID: 1.3.6.1.4.1.25623.1.0.800109)

Summary
PHP version smaller than 5.2.8 suffers from multiple vulnerabilities.

. . . continues on next page . . .

... continued from previous page ...

Vulnerability Detection Result
Installed version: 5.2.4
Fixed version: 5.2.8

Solution
Solution type: VendorFix
Update PHP to version 5.2.8 or later.

Vulnerability Detection Method
Details:PHP Version < 5.2.8 Multiple Vulnerabilities
OID:1.3.6.1.4.1.25623.1.0.110180
Version used: $Revision: 4506 $

Product Detection Result
Product: cpe:/a:php:php:5.2.4
Method: PHP Version Detection (Remote)
OID: 1.3.6.1.4.1.25623.1.0.800109)

References
CVE: CVE-2008-5814, CVE-2008-5844
BID:32673

High (CVSS: 7.5)
NVT: PHP Version < 5.3.1 Multiple Vulnerabilities

Product detection result
cpe:/a:php:php:5.2.4
Detected by PHP Version Detection (Remote) (OID: 1.3.6.1.4.1.25623.1.0.800109)

Summary
PHP version smaller than 5.3.1 suffers from multiple vulnerabilities.

Vulnerability Detection Result
Installed version: 5.2.4
Fixed version: 5.3.1

Solution
Solution type: VendorFix
Update PHP to version 5.3.1 or later.

Vulnerability Detection Method
Details:PHP Version < 5.3.1 Multiple Vulnerabilities
OID:1.3.6.1.4.1.25623.1.0.110178
Version used: $Revision: 4506 $

... continues on next page ...

... continued from previous page ...

Product Detection Result
Product: cpe:/a:php:php:5.2.4
Method: PHP Version Detection (Remote)
OID: 1.3.6.1.4.1.25623.1.0.800109)

References
CVE: CVE-2009-3557, CVE-2009-3559, CVE-2009-4017, CVE-2009-4018, CVE-2010-1128
BID:36554, 36555, 37079, 37138

High (CVSS: 9.3)
NVT: PHP Version < 5.3.3 Multiple Vulnerabilities

Product detection result
cpe:/a:php:php:5.2.4
Detected by PHP Version Detection (Remote) (OID: 1.3.6.1.4.1.25623.1.0.800109)

Summary
PHP version smaller than 5.3.3 suffers from multiple vulnerabilities.

Vulnerability Detection Result
Installed version: 5.2.4
Fixed version: 5.3.3

Solution
Solution type: VendorFix
Update PHP to version 5.3.3 or later.

Vulnerability Detection Method
Details:PHP Version < 5.3.3 Multiple Vulnerabilities
OID:1.3.6.1.4.1.25623.1.0.110182
Version used: $Revision: 4506 $

Product Detection Result
Product: cpe:/a:php:php:5.2.4
Method: PHP Version Detection (Remote)
OID: 1.3.6.1.4.1.25623.1.0.800109)

References
CVE: CVE-2007-1581, CVE-2010-0397, CVE-2010-1860, CVE-2010-1862, CVE-2010-1864,
↪CVE-2010-1917, CVE-2010-2097, CVE-2010-2100, CVE-2010-2101, CVE-2010-2190, CVE
↪-2010-2191, CVE-2010-2225, CVE-2010-2484, CVE-2010-2531, CVE-2010-3062, CVE-20
↪10-3063, CVE-2010-3064, CVE-2010-3065
BID:38708, 40461, 40948, 41991

High (CVSS: 7.5)
NVT: PHP Versions Prior to 5.3.1 Multiple Vulnerabilities

Product detection result
cpe:/a:php:php:5.2.4
Detected by PHP Version Detection (Remote) (OID: 1.3.6.1.4.1.25623.1.0.800109)

Summary
PHP is prone to multiple security vulnerabilities.

Vulnerability Detection Result
Installed version: 5.2.4
Fixed version: 5.3.2

Impact
Some of these issues may be exploited to bypass security restrictions and create arbitrary files or cause denial-of-service conditions. The impact of the other issues has not been specified.

Solution
Solution type: VendorFix
Updates are available. Please see the references for more information.

Affected Software/OS
These issues affect PHP versions prior to 5.3.1.

Vulnerability Detection Method
Details:PHP Versions Prior to 5.3.1 Multiple Vulnerabilities
OID:1.3.6.1.4.1.25623.1.0.100359
Version used: $Revision: 4505 $

Product Detection Result
Product: cpe:/a:php:php:5.2.4
Method: PHP Version Detection (Remote)
OID: 1.3.6.1.4.1.25623.1.0.800109)

References
BID:37079
Other:
URL:http://www.securityfocus.com/bid/37079
URL:http://securityreason.com/securityalert/6601
URL:http://securityreason.com/securityalert/6600
URL:http://www.php.net/releases/5_3_1.php
URL:http://www.php.net/
URL:http://seclists.org/fulldisclosure/2009/Nov/228
URL:http://www.securityfocus.com/archive/1/507982

High (CVSS: 7.5)
NVT: PHP-CGI-based setups vulnerability when parsing query string parameters from php files.

Summary
PHP is prone to an information-disclosure vulnerability.

Vulnerability Detection Result
`Vulnerable url: http://192.168.8.102/cgi-bin/php`

Impact
Exploiting this issue allows remote attackers to view the source code of files in the context of the server process. This may allow the attacker to obtain sensitive information and to run arbitrary PHP code on the affected computer other attacks are also possible.

Solution
Solution type: VendorFix
PHP has released version 5.4.3 and 5.3.13 to address this vulnerability. PHP is recommending that users upgrade to the latest version of PHP.

Vulnerability Insight
When PHP is used in a CGI-based setup (such as Apache's mod_cgid), the php-cgi receives a processed query string parameter as command line arguments which allows command-line switches, such as -s, -d or -c to be passed to the php-cgi binary, which can be exploited to disclose source code and obtain arbitrary code execution.
An example of the -s command, allowing an attacker to view the source code of index.php is below:
http://localhost/index.php?-s

Vulnerability Detection Method
Details:`PHP-CGI-based setups vulnerability when parsing query string parameters from ph.`
`↪..`
OID:1.3.6.1.4.1.25623.1.0.103482
Version used: `$Revision: 5958 $`

References
```
CVE: CVE-2012-1823, CVE-2012-2311, CVE-2012-2336, CVE-2012-2335
BID:53388
Other:
  URL:http://www.h-online.com/open/news/item/Critical-open-hole-in-PHP-creates-r
↪isks-Update-1567532.html
   URL:http://www.kb.cert.org/vuls/id/520827
   URL:http://eindbazen.net/2012/05/php-cgi-advisory-cve-2012-1823/
   URL:https://bugs.php.net/bug.php?id=61910
   URL:http://www.php.net/manual/en/security.cgi-bin.php
   URL:http://www.securityfocus.com/bid/53388
```

High (CVSS: 7.5)
NVT: phpinfo() output accessible

Summary
Many PHP installation tutorials instruct the user to create a file called phpinfo.php or similar containing the phpinfo() statement. Such a file is often times left in webserver directory after completion.

Vulnerability Detection Result
```
The following files are calling the function phpinfo() which disclose potentiall
↪y sensitive information to the remote attacker:
http://192.168.8.102/phpinfo.php
http://192.168.8.102/mutillidae/phpinfo.php
```

Impact
Some of the information that can be gathered from this file includes: The username of the user who installed php, if they are a SUDO user, the IP address of the host, the web server version, the system version(unix / linux), and the root directory of the web server.

Solution
Solution type: Workaround
Delete them or restrict access to the listened files.

Vulnerability Detection Method
Details:`phpinfo() output accessible`
OID:1.3.6.1.4.1.25623.1.0.11229
Version used: `$Revision: 5815 $`

High (CVSS: 7.5)
NVT: phpMyAdmin BLOB Streaming Multiple Input Validation Vulnerabilities

Product detection result
```
cpe:/a:phpmyadmin:phpmyadmin:3.1.1
Detected by phpMyAdmin Detection (OID: 1.3.6.1.4.1.25623.1.0.900129)
```

Summary
phpMyAdmin is prone to multiple input-validation vulnerabilities, including an HTTP response-splitting vulnerability and a local file-include vulnerability.
These issues can be leveraged to view or execute arbitrary local scripts, or misrepresent how web content is served, cached, or interpreted. This could aid in various attacks that try to entice client users into a false sense of trust. Other attacks are also possible.
Versions prior to phpMyAdmin 3.1.3.1 are vulnerable.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

. . . continues on next page . . .

... continued from previous page ...

Solution
Vendor updates are available. Please see http://www.phpmyadmin.net for more Information.

Vulnerability Detection Method
Details:`phpMyAdmin BLOB Streaming Multiple Input Validation Vulnerabilities`
OID:1.3.6.1.4.1.25623.1.0.100078
Version used: `$Revision: 5016 $`

Product Detection Result
Product: `cpe:/a:phpmyadmin:phpmyadmin:3.1.1`
Method: `phpMyAdmin Detection`
OID: 1.3.6.1.4.1.25623.1.0.900129)

References
`BID:34253`
`Other:`
`URL:http://www.securityfocus.com/bid/34253`

High (CVSS: 7.5)
NVT: phpMyAdmin Code Injection and XSS Vulnerability

Product detection result
`cpe:/a:phpmyadmin:phpmyadmin:3.1.1`
`Detected by phpMyAdmin Detection (OID: 1.3.6.1.4.1.25623.1.0.900129)`

Summary
phpMyAdmin is prone to a remote PHP code-injection vulnerability and to a cross-site scripting vulnerability.
An attacker can exploit this issue to inject and execute arbitrary malicious PHP code in the context of the webserver process. This may facilitate a compromise of the application and the underlying system other attacks are also possible.
Versions prior to phpMyAdmin 2.11.9.5 and 3.1.3.1 are vulnerable.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Solution
Vendor updates are available. Please see http://www.phpmyadmin.net for more Information.

Vulnerability Detection Method
Details:`phpMyAdmin Code Injection and XSS Vulnerability`
OID:1.3.6.1.4.1.25623.1.0.100077
Version used: `$Revision: 5016 $`

... continues on next page ...

... continued from previous page ...

Product Detection Result
Product: cpe:/a:phpmyadmin:phpmyadmin:3.1.1
Method: phpMyAdmin Detection
OID: 1.3.6.1.4.1.25623.1.0.900129)

References
CVE: CVE-2009-1151
BID:34236, 34251
Other:
URL:http://www.securityfocus.com/bid/34236
URL:http://www.securityfocus.com/bid/34251

High (CVSS: 7.5)
NVT: phpMyAdmin Configuration File PHP Code Injection Vulnerability

Product detection result
cpe:/a:phpmyadmin:phpmyadmin:3.1.1
Detected by phpMyAdmin Detection (OID: 1.3.6.1.4.1.25623.1.0.900129)

Summary
According to its version number, the remote version of phpMyAdmin is prone to a remote PHP code-injection vulnerability.
An attacker can exploit this issue to inject and execute arbitrary malicious PHP code in the context of the webserver process. This may facilitate a compromise of the application and the underlying system other attacks are also possible.
phpMyAdmin 3.x versions prior to 3.1.3.2 are vulnerable.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Solution
Vendor updates are available. Please see http://www.phpmyadmin.net for more Information.

Vulnerability Detection Method
Details:phpMyAdmin Configuration File PHP Code Injection Vulnerability
OID:1.3.6.1.4.1.25623.1.0.100144
Version used: $Revision: 5016 $

Product Detection Result
Product: cpe:/a:phpmyadmin:phpmyadmin:3.1.1
Method: phpMyAdmin Detection
OID: 1.3.6.1.4.1.25623.1.0.900129)

References

... continues on next page ...

... continued from previous page ...

CVE: CVE-2009-1285
BID:34526
Other:
URL:http://www.securityfocus.com/bid/34526

High (CVSS: 7.5)
NVT: Test HTTP dangerous methods

Summary
Misconfigured web servers allows remote clients to perform dangerous HTTP methods such as PUT and DELETE. This script checks if they are enabled and can be misused to upload or delete files.

Vulnerability Detection Result
We could upload the following files via the PUT method at this web server:
http://192.168.8.102/dav/puttest1011049548.html
We could delete the following files via the DELETE method at this web server:
http://192.168.8.102/dav/puttest1011049548.html

Impact
- Enabled PUT method: This might allow an attacker to upload and run arbitrary code on this web server.
- Enabled DELETE method: This might allow an attacker to delete additional files on this web server.

Solution
Solution type: Mitigation
Use access restrictions to these dangerous HTTP methods or disable them completely.

Vulnerability Detection Method
Details:Test HTTP dangerous methods
OID:1.3.6.1.4.1.25623.1.0.10498
Version used: $Revision: 4295 $

References
BID:12141
Other:
OWASP:OWASP-CM-001

High (CVSS: 7.5)
NVT: Tiki Wiki CMS Groupware < 4.2 Multiple Unspecified Vulnerabilities

Product detection result
cpe:/a:tiki:tikiwiki_cms/groupware:1.9.5
Detected by Tiki Wiki CMS Groupware Version Detection (OID: 1.3.6.1.4.1.25623.1.

... continues on next page ...

... continued from previous page ...

↪0.901001)

Summary
Tiki Wiki CMS Groupware is prone to multiple unspecified vulnerabilities, including:
- An unspecified SQL-injection vulnerability - An unspecified authentication-bypass vulnerability
- An unspecified vulnerability

Vulnerability Detection Result
Installed version: 1.9.5
Fixed version: 4.2

Impact
Exploiting these issues could allow an attacker to compromise the application, access or modify data, exploit latent vulnerabilities in the underlying database, and gain unauthorized access to the affected application. Other attacks are also possible.

Solution
Solution type: VendorFix
The vendor has released an advisory and fixes. Please see the references for details.

Affected Software/OS
Versions prior to Tiki Wiki CMS Groupware 4.2 are vulnerable.

Vulnerability Detection Method
Details:Tiki Wiki CMS Groupware < 4.2 Multiple Unspecified Vulnerabilities
OID:1.3.6.1.4.1.25623.1.0.100537
Version used: $Revision: 5144 $

Product Detection Result
Product: cpe:/a:tiki:tikiwiki_cms/groupware:1.9.5
Method: Tiki Wiki CMS Groupware Version Detection
OID: 1.3.6.1.4.1.25623.1.0.901001)

References
CVE: CVE-2010-1135, CVE-2010-1134, CVE-2010-1133, CVE-2010-1136
BID:38608
Other:
URL:http://www.securityfocus.com/bid/38608
URL:http://tikiwiki.svn.sourceforge.net/viewvc/tikiwiki?view=rev&revision=247
↪34
URL:http://tikiwiki.svn.sourceforge.net/viewvc/tikiwiki?view=rev&revision=250
↪46
URL:http://tikiwiki.svn.sourceforge.net/viewvc/tikiwiki?view=rev&revision=254
↪24
URL:http://tikiwiki.svn.sourceforge.net/viewvc/tikiwiki?view=rev&revision=254

... continues on next page ...

... continued from previous page ...

↪35
URL:http://info.tikiwiki.org/article86-Tiki-Announces-3-5-and-4-2-Releases
URL:http://info.tikiwiki.org/tiki-index.php?page=homepage

High (CVSS: 10.0)
NVT: TWiki XSS and Command Execution Vulnerabilities

Product detection result
cpe:/a:twiki:twiki:01.Feb.2003
Detected by TWiki Version Detection (OID: 1.3.6.1.4.1.25623.1.0.800399)

Summary
The host is running TWiki and is prone to Cross-Site Scripting (XSS) and Command Execution Vulnerabilities.

Vulnerability Detection Result
Installed version: 01.Feb.2003
Fixed version: 4.2.4

Impact
Successful exploitation could allow execution of arbitrary script code or commands. This could let attackers steal cookie-based authentication credentials or compromise the affected application.
Impact Level: Application

Solution
Solution type: VendorFix
Upgrade to version 4.2.4 or later, http://twiki.org/cgi-bin/view/Codev/TWikiRelease04x02x04

Affected Software/OS
TWiki, TWiki version prior to 4.2.4.

Vulnerability Insight
The flaws are due to, - %URLPARAM}}% variable is not properly sanitized which lets attackers conduct cross-site scripting attack. - %SEARCH}}% variable is not properly sanitised before being used in an eval() call which lets the attackers execute perl code through eval injection attack.

Vulnerability Detection Method
Details:TWiki XSS and Command Execution Vulnerabilities
OID:1.3.6.1.4.1.25623.1.0.800320
Version used: $Revision: 4227 $

Product Detection Result
Product: cpe:/a:twiki:twiki:01.Feb.2003
Method: TWiki Version Detection

... continues on next page ...

... continued from previous page ...

OID: 1.3.6.1.4.1.25623.1.0.800399)

References
CVE: CVE-2008-5304, CVE-2008-5305
BID:32668, 32669
Other:
URL:http://twiki.org/cgi-bin/view/Codev.SecurityAlert-CVE-2008-5304
URL:http://twiki.org/cgi-bin/view/Codev/SecurityAlert-CVE-2008-5305

[return to 192.168.8.102]

2.1.13 High 1099/tcp

High (CVSS: 10.0)
NVT: Java RMI Server Insecure Default Configuration Remote Code Execution Vulnerability

Summary
Multiple Java products that implement the RMI Server contain a vulnerability that could allow an unauthenticated, remote attacker to execute arbitrary code on a targeted system with elevated privileges.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Solution
Solution type: Workaround
Disable class-loading.

Vulnerability Insight
The vulnerability exists because of an incorrect default configuration of the Remote Method Invocation (RMI) Server in the affected software. An unauthenticated, remote attacker could exploit the vulnerability by transmitting crafted packets to the affected software. When the packets are processed, the attacker could execute arbitrary code on the system with elevated privileges.

Vulnerability Detection Method
Check if the target tries to load a Java class via a remote HTTP URL.
Details:Java RMI Server Insecure Default Configuration Remote Code Execution Vulnerabil.
↪..
OID:1.3.6.1.4.1.25623.1.0.140051
Version used: $Revision: 4422 $

References
Other:
URL:https://tools.cisco.com/security/center/viewAlert.x?alertId=23665

[return to 192.168.8.102]

2.1.14 Medium 6667/tcp

Medium (CVSS: 6.8)
NVT: UnrealIRCd Authentication Spoofing Vulnerability

Product detection result
`cpe:/a:unrealircd:unrealircd:3.2.8.1`
`Detected by UnrealIRCd Detection (OID: 1.3.6.1.4.1.25623.1.0.809884)`

Summary
This host is installed with UnrealIRCd and is prone to authentication spoofing vulnerability.

Vulnerability Detection Result
`Installed version: 3.2.8.1`
`Fixed version: 3.2.10.7`

Impact
Successful exploitation of this vulnerability will allows remote attackers to spoof certificate fingerprints and consequently log in as another user.
Impact Level: Application.

Solution
Solution type: VendorFix
Upgrade to UnrealIRCd 3.2.10.7, or 4.0.6, or later. For updates refer to https://bugs.unrealircd.org/main_page.php

Affected Software/OS
UnrealIRCd before 3.2.10.7 and 4.x before 4.0.6.

Vulnerability Insight
The flaw exists due to an error in the 'm_authenticate' function in 'modules/m_sasl.c' script.

Vulnerability Detection Method
Get the installed version with the help of detect NVT and check the version is vulnerable or not.
Details:`UnrealIRCd Authentication Spoofing Vulnerability`
OID:1.3.6.1.4.1.25623.1.0.809883
Version used: `$Revision: 5287 $`

Product Detection Result
Product: `cpe:/a:unrealircd:unrealircd:3.2.8.1`
Method: `UnrealIRCd Detection`
OID: 1.3.6.1.4.1.25623.1.0.809884)

... continues on next page ...

... continued from previous page ...

References
CVE: CVE-2016-7144
BID:92763
Other:
URL:http://seclists.org/oss-sec/2016/q3/420
URL:http://www.openwall.com/lists/oss-security/2016/09/05/8
URL:https://github.com/unrealircd/unrealircd/commit/f473e355e1dc422c4f019dbf8
↪6bc50ba1a34a766

[return to 192.168.8.102]

2.1.15 Medium 5432/tcp

Medium (CVSS: 6.5)
NVT: PostgreSQL 'bitsubstr' Buffer Overflow Vulnerability

Product detection result
cpe:/a:postgresql:postgresql:8.3.1
Detected by PostgreSQL Detection (OID: 1.3.6.1.4.1.25623.1.0.100151)

Summary
PostgreSQL is prone to a buffer-overflow vulnerability because the application fails to perform adequate boundary checks on user- supplied data.
Attackers can exploit this issue to execute arbitrary code with elevated privileges or crash the affected application.
PostgreSQL version 8.0.x, 8.1.x, 8.3.x is vulnerable other versions may also be affected.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Vulnerability Detection Method
Details:PostgreSQL 'bitsubstr' Buffer Overflow Vulnerability
OID:1.3.6.1.4.1.25623.1.0.100470
Version used: $Revision: 5394 $

Product Detection Result
Product: cpe:/a:postgresql:postgresql:8.3.1
Method: PostgreSQL Detection
OID: 1.3.6.1.4.1.25623.1.0.100151)

References
CVE: CVE-2010-0442
BID:37973
Other:

... continues on next page ...

... continued from previous page ...

URL:http://www.postgresql.org/
URL:http://www.securityfocus.com/bid/37973
URL:http://xforce.iss.net/xforce/xfdb/55902
URL:http://intevydis.blogspot.com/2010/01/postgresql-8023-bitsubstr-overflow.html

Medium (CVSS: 6.5)
NVT: PostgreSQL 'intarray' Module 'gettoken()' Buffer Overflow Vulnerability

Product detection result
cpe:/a:postgresql:postgresql:8.3.1
Detected by PostgreSQL Detection (OID: 1.3.6.1.4.1.25623.1.0.100151)

Summary
PostgreSQL is prone to a buffer-overflow vulnerability because the application fails to perform adequate boundary checks on user-supplied data. The issue affects the 'intarray' module.
An authenticated attacker can leverage this issue to execute arbitrary code within the context of the vulnerable application. Failed exploit attempts will result in a denial-of-service condition.
The issue affect versions prior to 8.2.20, 8.3.14, 8.4.7, and 9.0.3.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Solution
Updates are available. Please see the references for more information.

Vulnerability Detection Method
Details:PostgreSQL 'intarray' Module 'gettoken()' Buffer Overflow Vulnerability
OID:1.3.6.1.4.1.25623.1.0.103054
Version used: $Revision: 3911 $

Product Detection Result
Product: cpe:/a:postgresql:postgresql:8.3.1
Method: PostgreSQL Detection
OID: 1.3.6.1.4.1.25623.1.0.100151)

References
CVE: CVE-2010-4015
BID:46084
Other:
URL:https://www.securityfocus.com/bid/46084
URL:http://www.postgresql.org/
URL:http://www.postgresql.org/about/news.1289

Medium (CVSS: 5.5)
NVT: PostgreSQL 'RESET ALL' Unauthorized Access Vulnerability

Product detection result
cpe:/a:postgresql:postgresql:8.3.1
Detected by PostgreSQL Detection (OID: 1.3.6.1.4.1.25623.1.0.100151)

Summary
PostgreSQL is prone to an unauthorized-access vulnerability.
Attackers can exploit this issue to reset special parameter settings only a root user should be able to modify. This may aid in further attacks.
This issue affects versions prior to the following PostgreSQL versions:
7.4.29, 8.0.25 8.1.21, 8.2.17 8.3.11 8.4.4

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Solution
Updates are available. Please see the references for more information.

Vulnerability Detection Method
Details:PostgreSQL 'RESET ALL' Unauthorized Access Vulnerability
OID:1.3.6.1.4.1.25623.1.0.100648
Version used: $Revision: 5373 $

Product Detection Result
Product: cpe:/a:postgresql:postgresql:8.3.1
Method: PostgreSQL Detection
OID: 1.3.6.1.4.1.25623.1.0.100151)

References
CVE: CVE-2010-1975
BID:40304
Other:
URL:http://www.securityfocus.com/bid/40304
URL:http://www.postgresql.org/docs/current/static/release-8-4-4.html
URL:http://www.postgresql.org/docs/current/static/release-8-2-17.html
URL:http://www.postgresql.org/docs/current/static/release-8-1-21.html
URL:http://www.postgresql.org/docs/current/static/release-8-3-11.html
URL:http://www.postgresql.org/
URL:http://www.postgresql.org/docs/current/static/release-8-0-25.html
URL:http://www.postgresql.org/docs/current/static/release-7-4-29.html

... continues on next page ...

... continued from previous page ...

Medium (CVSS: 6.5)
NVT: PostgreSQL Code Injection and Denial of Service Vulnerabilities (Linux)

Product detection result
`cpe:/a:postgresql:postgresql:8.3.1`
`Detected by PostgreSQL Detection (OID: 1.3.6.1.4.1.25623.1.0.100151)`

Summary
This host is running PostgreSQL and is prone to code injection and denial of service vulnerabilities.

Vulnerability Detection Result
`Installed version: 8.3.1`
`Fixed version: 9.1.23`

Impact
Successful exploitation will allow a remote attacker to inject code and cause the server to crash.
Impact Level: Application

Solution
Solution type: VendorFix
Upgrade to version 9.1.23 or 9.2.18 or 9.3.14 or 9.4.9 or 9.5.4 or higher, For updates refer to http://www.postgresql.org/download

Affected Software/OS
PostgreSQL version before 9.1.23, 9.2.x before 9.2.18, 9.3.x before 9.3.14, 9.4.x before 9.4.9, and 9.5.x before 9.5.4 on linux.

Vulnerability Insight
Multiple flaws are due to - An error in certain nested CASE expressions. - Improper sanitization of input passed to database and role names.

Vulnerability Detection Method
Get the installed version with the help of detect NVT and check the version is vulnerable or not.
Details:`PostgreSQL Code Injection and Denial of Service Vulnerabilities (Linux)`
OID:1.3.6.1.4.1.25623.1.0.808665
Version used: `$Revision: 5650 $`

Product Detection Result
Product: `cpe:/a:postgresql:postgresql:8.3.1`
Method: `PostgreSQL Detection`
OID: 1.3.6.1.4.1.25623.1.0.100151)

References

... continues on next page ...

... continued from previous page ...

CVE: CVE-2016-5423, CVE-2016-5424
BID:92433, 92435
Other:
URL:https://www.postgresql.org/about/news/1688/

Medium (CVSS: 4.0)
NVT: PostgreSQL Conversion Encoding Remote Denial of Service Vulnerability

Product detection result
cpe:/a:postgresql:postgresql:8.3.1
Detected by PostgreSQL Detection (OID: 1.3.6.1.4.1.25623.1.0.100151)

Summary
PostgreSQL is prone to a remote denial-of-service vulnerability.
Exploiting this issue may allow attackers to terminate connections to the PostgreSQL server, denying service to legitimate users.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Solution
Updates are available. Update to newer Version.

Vulnerability Detection Method
Details:PostgreSQL Conversion Encoding Remote Denial of Service Vulnerability
OID:1.3.6.1.4.1.25623.1.0.100157
Version used: $Revision: 5016 $

Product Detection Result
Product: cpe:/a:postgresql:postgresql:8.3.1
Method: PostgreSQL Detection
OID: 1.3.6.1.4.1.25623.1.0.100151)

References
CVE: CVE-2009-0922
BID:34090
Other:
URL:http://www.securityfocus.com/bid/34090
URL:http://www.postgresql.org/

Medium (CVSS: 6.8)
NVT: PostgreSQL Multiple Security Vulnerabilities

... continues on next page ...

... continued from previous page ...

Product detection result
cpe:/a:postgresql:postgresql:8.3.1
Detected by PostgreSQL Detection (OID: 1.3.6.1.4.1.25623.1.0.100151)

Summary
PostgreSQL is prone to multiple security vulnerabilities, including a denial-of-service issue, a privilege-escalation issue, and an authentication- bypass issue.
Attackers can exploit these issues to shut down affected servers, perform certain actions with elevated privileges, and bypass authentication mechanisms to perform unauthorized actions. Other attacks may also be possible.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Solution
Updates are available. Please see the references for more information.

Vulnerability Detection Method
Details:PostgreSQL Multiple Security Vulnerabilities
OID:1.3.6.1.4.1.25623.1.0.100273
Version used: $Revision: 5016 $

Product Detection Result
Product: cpe:/a:postgresql:postgresql:8.3.1
Method: PostgreSQL Detection
OID: 1.3.6.1.4.1.25623.1.0.100151)

References
CVE: CVE-2009-3229, CVE-2009-3230, CVE-2009-3231
BID:36314
Other:
URL:http://www.securityfocus.com/bid/36314
URL:https://bugzilla.redhat.com/show_bug.cgi?id=522085#c1
URL:http://www.postgresql.org/
URL:http://www.postgresql.org/support/security
URL:http://permalink.gmane.org/gmane.comp.security.oss.general/2088

Medium (CVSS: 6.5)
NVT: PostgreSQL NULL Character CA SSL Certificate Validation Security Bypass Vulnerability

Product detection result
cpe:/a:postgresql:postgresql:8.3.1
Detected by PostgreSQL Detection (OID: 1.3.6.1.4.1.25623.1.0.100151)

... continues on next page ...

... continued from previous page ...

Summary
PostgreSQL is prone to a security-bypass vulnerability because the application fails to properly validate the domain name in a signed CA certificate, allowing attackers to substitute malicious SSL certificates for trusted ones.
Successfully exploiting this issue allows attackers to perform man-in-the- middle attacks or impersonate trusted servers, which will aid in further attacks.
PostgreSQL is also prone to a local privilege-escalation vulnerability. Exploiting this issue allows local attackers to gain elevated privileges.
PostgreSQL versions prior to 8.4.2, 8.3.9, 8.2.15, 8.1.19, 8.0.23, and 7.4.27 are vulnerable to this issue.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Solution
Updates are available. Please see the references for more information.

Vulnerability Detection Method
Details:`PostgreSQL NULL Character CA SSL Certificate Validation Security Bypass Vulnera.`
`↪..`
OID:1.3.6.1.4.1.25623.1.0.100400
Version used: `$Revision: 5016 $`

Product Detection Result
Product: `cpe:/a:postgresql:postgresql:8.3.1`
Method: `PostgreSQL Detection`
OID: 1.3.6.1.4.1.25623.1.0.100151)

References
```
CVE: CVE-2009-4034, CVE-2009-4136
BID:37334, 37333
Other:
  URL:http://www.securityfocus.com/bid/37334
   URL:http://www.securityfocus.com/bid/37333
   URL:http://www.postgresql.org
   URL:http://www.postgresql.org/support/security
   URL:http://www.postgresql.org/about/news.1170
```

Medium (CVSS: 6.0)
NVT: PostgreSQL PL/Perl and PL/Tcl Local Privilege Escalation Vulnerability

Product detection result
`cpe:/a:postgresql:postgresql:8.3.1`
`Detected by PostgreSQL Detection (OID: 1.3.6.1.4.1.25623.1.0.100151)`

... continues on next page ...

... continued from previous page ...

Summary
PostgreSQL is prone to a local privilege-escalation vulnerability.
Exploiting this issue allows local attackers to gain elevated privileges and execute arbitrary commands with the privileges of the victim.
Versions prior to PostgreSQL 9.0.1 are vulnerable.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Solution
Updates are available. Please see the references for more information.

Vulnerability Detection Method
Details:`PostgreSQL PL/Perl and PL/Tcl Local Privilege Escalation Vulnerability`
OID:1.3.6.1.4.1.25623.1.0.100843
Version used: `$Revision: 5373 $`

Product Detection Result
Product: `cpe:/a:postgresql:postgresql:8.3.1`
Method: `PostgreSQL Detection`
OID: 1.3.6.1.4.1.25623.1.0.100151)

References
```
CVE: CVE-2010-3433
BID:43747
Other:
  URL:https://www.securityfocus.com/bid/43747
   URL:http://www.postgresql.org/docs/9.0/static/release-9-0-1.html
   URL:http://www.postgresql.org
   URL:http://www.postgresql.org/support/security
```

Medium (CVSS: 4.3)
NVT: PostgreSQL Remote Denial Of Service Vulnerability June15 (Linux)

Product detection result
`cpe:/a:postgresql:postgresql:8.3.1`
`Detected by PostgreSQL Detection (OID: 1.3.6.1.4.1.25623.1.0.100151)`

Summary
This host is running PostgreSQL and is prone to remote denial of service vulnerability.

Vulnerability Detection Result

... continues on next page ...

... continued from previous page ...

Vulnerability was detected according to the Vulnerability Detection Method.

Impact
Successful exploitation will allow a remote attacker to crash the program.
Impact Level: Application

Solution
Solution type: VendorFix
Upgrade to version 9.0.20, 9.1.16, 9.2.11, 9.3.7, 9.4.2 or higher, For updates refer to http://www.postgresql.org/download

Affected Software/OS
PostgreSQL version before 9.0.20, 9.1.x before 9.1.16, 9.2.x before 9.2.11, 9.3.x before 9.3.7, and 9.4.x before 9.4.2 on Linux.

Vulnerability Insight
Flaw is triggered when a timeout interrupt is fired partway through the session shutdown sequence.

Vulnerability Detection Method
Get the installed version with the help of detect NVT and check the version is vulnerable or not.
Details:`PostgreSQL Remote Denial Of Service Vulnerability June15 (Linux)`
OID:1.3.6.1.4.1.25623.1.0.805805
Version used: `$Revision: 5082 $`

Product Detection Result
Product: `cpe:/a:postgresql:postgresql:8.3.1`
Method: `PostgreSQL Detection`
OID: 1.3.6.1.4.1.25623.1.0.100151)

References
`CVE: CVE-2015-3165`
`BID:74787`
`Other:`
`URL:http://www.postgresql.org/about/news/1587`

Medium (CVSS: 5.0)
NVT: SSL/TLS: Certificate Expired

Summary
The remote server's SSL/TLS certificate has already expired.

Vulnerability Detection Result
`The certificate of the remote service expired on 2010-04-16 14:07:45.`
`Certificate details:`

... continues on next page ...

... continued from previous page ...

```
subject ...: 1.2.840.113549.1.9.1=#726F6F74407562756E74753830342D626173652E6C6F6
↪3616C646F6D61696E,CN=ubuntu804-base.localdomain,OU=Office for Complication of
↪Otherwise Simple Affairs,O=OCOSA,L=Everywhere,ST=There is no such thing outsid
↪e US,C=XX
subject alternative names (SAN):
None
issued by .: 1.2.840.113549.1.9.1=#726F6F74407562756E74753830342D626173652E6C6F6
↪3616C646F6D61696E,CN=ubuntu804-base.localdomain,OU=Office for Complication of
↪Otherwise Simple Affairs,O=OCOSA,L=Everywhere,ST=There is no such thing outsid
↪e US,C=XX
serial ....: 00FAF93A4C7FB6B9CC
valid from : 2010-03-17 14:07:45 UTC
valid until: 2010-04-16 14:07:45 UTC
fingerprint (SHA-1): ED093088706603BFD5DC237399B498DA2D4D31C6
fingerprint (SHA-256): E7A7FA0D63E457C7C4A59B38B70849C6A70BDA6F830C7AF1E32DEE436
↪DE813CC
```

Solution
Solution type: Mitigation
Replace the SSL/TLS certificate by a new one.

Vulnerability Insight
This script checks expiry dates of certificates associated with SSL/TLS-enabled services on the target and reports whether any have already expired.

Vulnerability Detection Method
Details:`SSL/TLS: Certificate Expired`
OID:1.3.6.1.4.1.25623.1.0.103955
Version used: `$Revision: 4765 $`

Medium (CVSS: 4.0)
NVT: SSL/TLS: Certificate Signed Using A Weak Signature Algorithm

Summary
The remote service is using a SSL/TLS certificate chain that has been signed using a cryptographically weak hashing algorithm.

Vulnerability Detection Result

```
The following certificates are part of the certificate chain but using insecure
↪signature algorithms:
Subject:              1.2.840.113549.1.9.1=#726F6F74407562756E74753830342D626173
↪652E6C6F63616C646F6D61696E,CN=ubuntu804-base.localdomain,OU=Office for Complic
↪ation of Otherwise Simple Affairs,O=OCOSA,L=Everywhere,ST=There is no such thi
↪ng outside US,C=XX
Signature Algorithm:  sha1WithRSAEncryption
```

Solution

... continues on next page ...

... continued from previous page ...

Solution type: Mitigation
Servers that use SSL/TLS certificates signed using an SHA-1 signature will need to obtain new SHA-2 signed SSL/TLS certificates to avoid these web browser SSL/TLS certificate warnings.

Vulnerability Insight
Secure Hash Algorithm 1 (SHA-1) is considered cryptographically weak and not secure enough for ongoing use. Beginning as late as January 2017 and as early as June 2016, browser developers such as Microsoft and Google will begin warning users when users visit web sites that use SHA-1 signed Secure Socket Layer (SSL) certificates.

Vulnerability Detection Method
Check which algorithm was used to sign the remote SSL/TLS Certificate.
Details:`SSL/TLS: Certificate Signed Using A Weak Signature Algorithm`
OID:1.3.6.1.4.1.25623.1.0.105880
Version used: `$Revision: 4781 $`

References
```
Other:
  URL:https://blog.mozilla.org/security/2014/09/23/phasing-out-certificates-with
↪-sha-1-based-signature-algorithms/
```

Medium (CVSS: 4.3)
NVT: SSL/TLS: Deprecated SSLv2 and SSLv3 Protocol Detection

Summary
It was possible to detect the usage of the deprecated SSLv2 and/or SSLv3 protocol on this system.

Vulnerability Detection Result
```
In addition to TLSv1.0+ the service is also providing the deprecated SSLv3 proto
↪col and supports one or more ciphers. Those supported ciphers can be found in
↪the 'SSL/TLS: Report Weak and Supported Ciphers' (OID: 1.3.6.1.4.1.25623.1.0.8
↪02067) NVT.
```

Impact
An attacker might be able to use the known cryptographic flaws to eavesdrop the connection between clients and the service to get access to sensitive data transferred within the secured connection.

Solution
Solution type: Mitigation
It is recommended to disable the deprecated SSLv2 and/or SSLv3 protocols in favor of the TLSv1+ protocols. Please see the references for more information.

Affected Software/OS
All services providing an encrypted communication using the SSLv2 and/or SSLv3 protocols.

... continues on next page ...

... continued from previous page ...

Vulnerability Insight
The SSLv2 and SSLv3 protocols containing known cryptographic flaws like:
- Padding Oracle On Downgraded Legacy Encryption (POODLE, CVE-2014-3566)
- Decrypting RSA with Obsolete and Weakened eNcryption (DROWN, CVE-2016-0800)

Vulnerability Detection Method
Check the used protocols of the services provided by this system.
Details:SSL/TLS: Deprecated SSLv2 and SSLv3 Protocol Detection
OID:1.3.6.1.4.1.25623.1.0.111012
Version used: $Revision: 5547 $

References
CVE: CVE-2016-0800, CVE-2014-3566
Other:
URL:https://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/algorithms-key-sizes-and-parameters-report
URL:https://bettercrypto.org/
URL:https://mozilla.github.io/server-side-tls/ssl-config-generator/
URL:https://drownattack.com/
URL:https://www.imperialviolet.org/2014/10/14/poodle.html

Medium (CVSS: 4.0)
NVT: SSL/TLS: Diffie-Hellman Key Exchange Insufficient DH Group Strength Vulnerability

Summary
The SSL/TLS service uses Diffie-Hellman groups with insufficient strength (key size < 2048).

Vulnerability Detection Result
Server Temporary Key Size: 1024 bits

Impact
An attacker might be able to decrypt the SSL/TLS communication offline.

Solution
Solution type: Workaround
Deploy (Ephemeral) Elliptic-Curve Diffie-Hellman (ECDHE) or use a 2048-bit or stronger Diffie-Hellman group. (see https://weakdh.org/sysadmin.html)

Vulnerability Insight
The Diffie-Hellman group are some big numbers that are used as base for the DH computations. They can be, and often are, fixed. The security of the final secret depends on the size of these parameters. It was found that 512 and 768 bits to be weak, 1024 bits to be breakable by really powerful attackers like governments.

Vulnerability Detection Method

... continues on next page ...

... continued from previous page ...

Checks the DHE temporary public key size.
Details:SSL/TLS: Diffie-Hellman Key Exchange Insufficient DH Group Strength Vulnerabili.
↪..
OID:1.3.6.1.4.1.25623.1.0.106223
Version used: $Revision: 5825 $

References
Other:
URL:https://weakdh.org/
URL:https://weakdh.org/sysadmin.html

Medium (CVSS: 6.8)
NVT: SSL/TLS: OpenSSL CCS Man in the Middle Security Bypass Vulnerability

Summary
OpenSSL is prone to security-bypass vulnerability.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact
Successfully exploiting this issue may allow attackers to obtain sensitive information by conducting a man-in-the-middle attack. This may lead to other attacks.

Solution
Solution type: VendorFix
Updates are available.

Affected Software/OS
OpenSSL before 0.9.8za, 1.0.0 before 1.0.0m and 1.0.1 before 1.0.1h

Vulnerability Insight
OpenSSL does not properly restrict processing of ChangeCipherSpec messages, which allows man-in-the-middle attackers to trigger use of a zero-length master key in certain OpenSSL-to-OpenSSL communications, and consequently hijack sessions or obtain sensitive information, via a crafted TLS handshake, aka the 'CCS Injection' vulnerability.

Vulnerability Detection Method
Send two SSL ChangeCipherSpec request and check the response.
Details:SSL/TLS: OpenSSL CCS Man in the Middle Security Bypass Vulnerability
OID:1.3.6.1.4.1.25623.1.0.105042
Version used: $Revision: 5537 $

References
CVE: CVE-2014-0224
BID:67899

... continues on next page ...

... continued from previous page ...

```
Other:
  URL:http://www.securityfocus.com/bid/67899
   URL:http://openssl.org/
```

Medium (CVSS: 4.3)
NVT: SSL/TLS: Report Weak Cipher Suites

Summary
This routine reports all Weak SSL/TLS cipher suites accepted by a service.
NOTE: No severity for SMTP services with 'Opportunistic TLS' and weak cipher suites on port 25/tcp is reported. If too strong cipher suites are configured for this service the alternative would be to fall back to an even more insecure cleartext communication.

Vulnerability Detection Result

```
'Weak' cipher suites accepted by this service via the SSLv3 protocol:
TLS_RSA_WITH_RC4_128_SHA
'Weak' cipher suites accepted by this service via the TLSv1.0 protocol:
TLS_RSA_WITH_RC4_128_SHA
```

Solution
Solution type: Mitigation
The configuration of this services should be changed so that it does not accept the listed weak cipher suites anymore.
Please see the references for more resources supporting you with this task.

Vulnerability Insight
These rules are applied for the evaluation of the cryptographic strength:
- RC4 is considered to be weak (CVE-2013-2566, CVE-2015-2808).
- Ciphers using 64 bit or less are considered to be vulnerable to brute force methods and therefore considered as weak (CVE-2015-4000).
- 1024 bit RSA authentication is considered to be insecure and therefore as weak.
- Any cipher considered to be secure for only the next 10 years is considered as medium
- Any other cipher is considered as strong

Vulnerability Detection Method
Details:SSL/TLS: Report Weak Cipher Suites
OID:1.3.6.1.4.1.25623.1.0.103440
Version used: $Revision: 5525 $

References

```
CVE: CVE-2013-2566, CVE-2015-2808, CVE-2015-4000
Other:
  URL:https://www.bsi.bund.de/SharedDocs/Warnmeldungen/DE/CB/warnmeldung_cb-k16-
↪1465_update_6.html
   URL:https://bettercrypto.org/
   URL:https://mozilla.github.io/server-side-tls/ssl-config-generator/
```

Medium (CVSS: 4.3)
NVT: SSL/TLS: SSLv3 Protocol CBC Cipher Suites Information Disclosure Vulnerability (POODLE)

Summary
This host is prone to an information disclosure vulnerability.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact
Successful exploitation will allow a man-in-the-middle attackers gain access to the plain text data stream.
Impact Level: Application

Solution
Solution type: Mitigation
Possible Mitigations are:
- Disable SSLv3
- Disable cipher suites supporting CBC cipher modes
- Enable TLS_FALLBACK_SCSV if the service is providing TLSv1.0+

Vulnerability Insight
The flaw is due to the block cipher padding not being deterministic and not covered by the Message Authentication Code

Vulnerability Detection Method
Evaluate previous collected information about this service.
Details:SSL/TLS: SSLv3 Protocol CBC Cipher Suites Information Disclosure Vulnerability .
↪..
OID:1.3.6.1.4.1.25623.1.0.802087
Version used: $Revision: 4749 $

References
CVE: CVE-2014-3566
BID:70574
Other:
URL:https://www.openssl.org/~bodo/ssl-poodle.pdf
URL:https://www.imperialviolet.org/2014/10/14/poodle.html
URL:https://www.dfranke.us/posts/2014-10-14-how-poodle-happened.html
URL:http://googleonlinesecurity.blogspot.in/2014/10/this-poodle-bites-exploit
↪ing-ssl-30.html

[return to 192.168.8.102]

2.1.16 Medium 22/tcp

Medium (CVSS: 5.0)
NVT: OpenSSH Denial of Service Vulnerability

Summary
OpenSSH is prone to a remote denial-of-service vulnerability.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact
Exploiting this issue allows remote attackers to trigger denial-of- service conditions.

Solution
Updates are available.

Affected Software/OS
OpenSSH 6.1 and prior

Vulnerability Insight
The default configuration of OpenSSH through 6.1 enforces a fixed time limit between establishing a TCP connection and completing a login, which makes it easier for remote attackers to cause a denial of service (connection-slot exhaustion) by periodically making many new TCP connections.

Vulnerability Detection Method
Compare the version retrieved from the banner with the affected range.
Details:`OpenSSH Denial of Service Vulnerability`
OID:1.3.6.1.4.1.25623.1.0.103939
Version used: `$Revision: 4336 $`

References
`CVE: CVE-2010-5107`
`BID:58162`
`Other:`
`URL:http://www.securityfocus.com/bid/58162`
`URL:http://www.openssh.com`

Medium (CVSS: 5.8)
NVT: OpenSSH 'child_set_env()' Function Security Bypass Vulnerability

Summary
OpenSSH is prone to a security-bypass vulnerability.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact
. . . continues on next page . . .

... continued from previous page ...

The security bypass allows remote attackers to bypass intended environment restrictions by using a substring located before a wildcard character.

Solution
Updates are available.

Affected Software/OS
Versions prior to OpenSSH 6.6 are vulnerable.

Vulnerability Insight
sshd in OpenSSH before 6.6 does not properly support wildcards on AcceptEnv lines in sshd_config.

Vulnerability Detection Method
Check the version.
Details:`OpenSSH 'child_set_env()' Function Security Bypass Vulnerability`
OID:1.3.6.1.4.1.25623.1.0.105003
Version used: `$Revision: 4336 $`

References
`CVE: CVE-2014-2532`
`BID:66355`
`Other:`
`URL:http://www.securityfocus.com/bid/66355`
`URL:http://www.openssh.com`

Medium (CVSS: 5.5)
NVT: OpenSSH <= 7.2p1 - Xauth Injection

Product detection result
`cpe:/a:openbsd:openssh:4.7p1`
`Detected by SSH Server type and version (OID: 1.3.6.1.4.1.25623.1.0.10267)`

Summary
openssh xauth command injection may lead to forced-command and /bin/false bypass

Vulnerability Detection Result
```
Installed version: 4.7p1
Fixed version:     7.2p2
```

Impact
By injecting xauth commands one gains limited* read/write arbitrary files, information leakage or xauth-connect capabilities.

Solution

... continues on next page ...

... continued from previous page ...

Solution type: VendorFix
Upgrade to OpenSSH version 7.2p2 or later. For updates refer to http://www.openssh.com

Affected Software/OS
OpenSSH versions before 7.2p2

Vulnerability Insight
An authenticated user may inject arbitrary xauth commands by sending an x11 channel request that includes a newline character in the x11 cookie. The newline acts as a command separator to the xauth binary. This attack requires the server to have 'X11Forwarding yes' enabled. Disabling it, mitigates this vector.

Vulnerability Detection Method
Get the installed version with the help of detect NVT and check the version is vulnerable or not.
Details:`OpenSSH <= 7.2p1 - Xauth Injection`
OID:1.3.6.1.4.1.25623.1.0.105581
Version used: `$Revision: 5745 $`

Product Detection Result
Product: `cpe:/a:openbsd:openssh:4.7p1`
Method: `SSH Server type and version`
OID: 1.3.6.1.4.1.25623.1.0.10267)

References
`CVE: CVE-2016-3115`
`Other:`
`URL:http://www.openssh.com/txt/release-7.2p2`

Medium (CVSS: 5.8)
NVT: OpenSSH Certificate Validation Security Bypass Vulnerability

Summary
OpenSSH is prone to a security-bypass vulnerability.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact
Attackers can exploit this issue to bypass certain security restrictions and perform unauthorized actions. This may aid in further attacks.

Solution
Updates are available.

Affected Software/OS

... continues on next page ...

... continued from previous page ...

OpenSSH 6.6 and prior are vulnerable.

Vulnerability Insight
The verify_host_key function in sshconnect.c in the client in OpenSSH 6.6 and earlier allows remote servers to trigger the skipping of SSHFP DNS RR checking by presenting an unacceptable HostCertificate.

Vulnerability Detection Method
Check the version
Details:`OpenSSH Certificate Validation Security Bypass Vulnerability`
OID:1.3.6.1.4.1.25623.1.0.105004
Version used: `$Revision: 4336 $`

References
`CVE: CVE-2014-2653`
`BID:66459`
`Other:`
`URL:http://www.securityfocus.com/bid/66459`
`URL:http://www.openssh.com`

Medium (CVSS: 5.0)
NVT: OpenSSH Denial of Service Vulnerability - Jan16

Product detection result
`cpe:/a:openbsd:openssh:4.7p1`
`Detected by SSH Server type and version (OID: 1.3.6.1.4.1.25623.1.0.10267)`

Summary
This host is installed with openssh and is prone to denial of service vulnerability.

Vulnerability Detection Result
`Installed version: 4.7p1`
`Fixed version: 7.1p2`

Impact
Successfully exploiting this issue allow remote attackers to cause a denial of service (out-of-bounds read and application crash).
Impact Level: Application

Solution
Solution type: VendorFix
Upgrade to OpenSSH version 7.1p2 or later. For updates refer to http://www.openssh.com

Affected Software/OS
OpenSSH versions before 7.1p2

... continues on next page ...

... continued from previous page ...

Vulnerability Insight
The flaw exists due to an error in 'ssh_packet_read_poll2' function within 'packet.c' script.

Vulnerability Detection Method
Get the installed version with the help of detect NVT and check the version is vulnerable or not.
Details:`OpenSSH Denial of Service Vulnerability - Jan16`
OID:1.3.6.1.4.1.25623.1.0.806671
Version used: `$Revision: 5650 $`

Product Detection Result
Product: `cpe:/a:openbsd:openssh:4.7p1`
Method: `SSH Server type and version`
OID: 1.3.6.1.4.1.25623.1.0.10267)

References
`CVE: CVE-2016-1907`
`Other:`
`URL:http://www.openssh.com/txt/release-7.1p2`
`URL:https://anongit.mindrot.org/openssh.git/commit/?id=2fecfd486bdba9f51b3a78`
`↪9277bb0733ca36e1c0`

Medium (CVSS: 4.3)
NVT: OpenSSH Security Bypass Vulnerability

Product detection result
`cpe:/a:openbsd:openssh:4.7p1`
`Detected by SSH Server type and version (OID: 1.3.6.1.4.1.25623.1.0.10267)`

Summary
This host is running OpenSSH and is prone to security bypass vulnerability.

Vulnerability Detection Result
`Installed version: 4.7p1`
`Fixed version: 6.9`

Impact
Successful exploitation will allow remote attackers to bypass intended access restrictions.
Impact Level: Application

Solution
Solution type: VendorFix
Upgrade to OpenSSH version 6.9 or later. For updates refer to http://www.openssh.com

... continues on next page ...

... continued from previous page ...

Affected Software/OS
OpenSSH versions before 6.9

Vulnerability Insight
The flaw is due to the refusal deadline was not checked within the x11_open_helper function.

Vulnerability Detection Method
Get the installed version with the help of detect NVT and check the version is vulnerable or not.
Details:`OpenSSH Security Bypass Vulnerability`
OID:1.3.6.1.4.1.25623.1.0.806049
Version used: `$Revision: 4336 $`

Product Detection Result
Product: `cpe:/a:openbsd:openssh:4.7p1`
Method: `SSH Server type and version`
OID: 1.3.6.1.4.1.25623.1.0.10267)

References
`CVE: CVE-2015-5352`
`Other:`
`URL:http://openwall.com/lists/oss-security/2015/07/01/10`

Medium (CVSS: 4.3)
NVT: SSH Weak Encryption Algorithms Supported

Summary
The remote SSH server is configured to allow weak encryption algorithms.

Vulnerability Detection Result
```
The following weak client-to-server encryption algorithms are supported by the r
↪emote service:
3des-cbc
aes128-cbc
aes192-cbc
aes256-cbc
arcfour
arcfour128
arcfour256
blowfish-cbc
cast128-cbc
rijndael-cbc@lysator.liu.se
The following weak server-to-client encryption algorithms are supported by the r
↪emote service:
3des-cbc
aes128-cbc
aes192-cbc
```

... continues on next page ...

... continued from previous page ...

aes256-cbc
arcfour
arcfour128
arcfour256
blowfish-cbc
cast128-cbc
rijndael-cbc@lysator.liu.se

Solution
Solution type: Mitigation
Disable the weak encryption algorithms.

Vulnerability Insight
The 'arcfour' cipher is the Arcfour stream cipher with 128-bit keys. The Arcfour cipher is believed to be compatible with the RC4 cipher [SCHNEIER]. Arcfour (and RC4) has problems with weak keys, and should not be used anymore.
The 'none' algorithm specifies that no encryption is to be done. Note that this method provides no confidentiality protection, and it is NOT RECOMMENDED to use it.
A vulnerability exists in SSH messages that employ CBC mode that may allow an attacker to recover plaintext from a block of ciphertext.

Vulnerability Detection Method
Check if remote ssh service supports Arcfour, none or CBC ciphers.
Details:SSH Weak Encryption Algorithms Supported
OID:1.3.6.1.4.1.25623.1.0.105611
Version used: $Revision: 4490 $

References
Other:
URL:https://tools.ietf.org/html/rfc4253#section-6.3
URL:https://www.kb.cert.org/vuls/id/958563

[return to 192.168.8.102]

2.1.17 Medium general/tcp

Medium (CVSS: 5.0)
NVT: TCP Sequence Number Approximation Reset Denial of Service Vulnerability

Summary
The host is running TCP services and is prone to denial of service vulnerability.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact

... continues on next page ...

... continued from previous page ...

Successful exploitation will allow remote attackers to guess sequence numbers and cause a denial of service to persistent TCP connections by repeatedly injecting a TCP RST packet.

Solution
Please see the referenced advisories for more information on obtaining and applying fixes.

Affected Software/OS
TCP/IP v4

Vulnerability Insight
The flaw is triggered when spoofed TCP Reset packets are received by the targeted TCP stack and will result in loss of availability for the attacked TCP services.

Vulnerability Detection Method
A TCP Reset packet with a different sequence number is sent to the target. A previously open connection is then checked to see if the target closed it or not.
Details:`TCP Sequence Number Approximation Reset Denial of Service Vulnerability`
OID:1.3.6.1.4.1.25623.1.0.902815
Version used: `$Revision: 5912 $`

References
`CVE: CVE-2004-0230`
`BID:10183`
`Other:`
`URL:http://xforce.iss.net/xforce/xfdb/15886`
`URL:http://www.us-cert.gov/cas/techalerts/TA04-111A.html`
`URL:http://www-01.ibm.com/support/docview.wss?uid=isg1IY55949`
`URL:http://www-01.ibm.com/support/docview.wss?uid=isg1IY55950`
`URL:http://www-01.ibm.com/support/docview.wss?uid=isg1IY62006`
`URL:http://www.microsoft.com/technet/security/Bulletin/MS05-019.mspx`
`URL:http://www.microsoft.com/technet/security/bulletin/ms06-064.mspx`
`URL:http://www.cisco.com/en/US/products/csa/cisco-sa-20040420-tcp-nonios.html`
`URL:http://www.cisco.com/en/US/products/csa/cisco-sa-20040420-tcp-nonios.html`

[return to 192.168.8.102]

2.1.18 Medium 445/tcp

Medium (CVSS: 5.0)
NVT: Samba 'FD_SET' Memory Corruption Vulnerability

Product detection result
`cpe:/a:samba:samba:3.0.20`
`Detected by SMB NativeLanMan (OID: 1.3.6.1.4.1.25623.1.0.102011)`

... continues on next page ...

... continued from previous page ...

Summary
Samba is prone to a memory-corruption vulnerability.

Vulnerability Detection Result
`Installed version: 3.0.20`
`Fixed version: 3.5.7`

Impact
An attacker can exploit this issue to crash the application or cause the application to enter an infinite loop. Due to the nature of this issue, arbitrary code execution may be possible this has not been confirmed.

Solution
Solution type: VendorFix
Updates are available. Please see the references for more information.

Affected Software/OS
Samba versions prior to 3.5.7 are vulnerable.

Vulnerability Detection Method
Details:`Samba 'FD_SET' Memory Corruption Vulnerability`
OID:1.3.6.1.4.1.25623.1.0.103095
Version used: `$Revision: 4398 $`

Product Detection Result
Product: `cpe:/a:samba:samba:3.0.20`
Method: `SMB NativeLanMan`
OID: 1.3.6.1.4.1.25623.1.0.102011)

References
`CVE: CVE-2011-0719`
`BID:46597`
`Other:`
`URL:https://www.securityfocus.com/bid/46597`
`URL:http://www.samba.org`
`URL:http://samba.org/samba/security/CVE-2011-0719.html`

Medium (CVSS: 6.8)
NVT: Samba 'mount.cifs' Utility Local Privilege Escalation Vulnerability

Product detection result
`cpe:/a:samba:samba:3.0.20`
`Detected by SMB NativeLanMan (OID: 1.3.6.1.4.1.25623.1.0.102011)`

... continues on next page ...

... continued from previous page ...

Summary
Samba is prone to a local privilege-escalation vulnerability in the 'mount.cifs' utility.

Vulnerability Detection Result
`Installed version: 3.0.20`
`Fixed version: 3.4.6`

Impact
Local attackers can exploit this issue to gain elevated privileges on affected computers.

Solution
Solution type: VendorFix
Updates are available. Please see the references for more information.

Vulnerability Detection Method
Details:`Samba 'mount.cifs' Utility Local Privilege Escalation Vulnerability`
OID:1.3.6.1.4.1.25623.1.0.100476
Version used: `$Revision: 4396 $`

Product Detection Result
Product: `cpe:/a:samba:samba:3.0.20`
Method: `SMB NativeLanMan`
OID: 1.3.6.1.4.1.25623.1.0.102011)

References
`CVE: CVE-2009-3297, CVE-2010-0787`
`BID:37992`
`Other:`
`URL:http://www.securityfocus.com/bid/37992`
`URL:http://www.samba.org`

Medium (CVSS: 6.8)
NVT: Samba Badlock Critical Vulnerability

Product detection result
`cpe:/a:samba:samba:3.0.20`
`Detected by SMB NativeLanMan (OID: 1.3.6.1.4.1.25623.1.0.102011)`

Summary
This host is running Samba and is prone to badlock vulnerability.

Vulnerability Detection Result
`Installed version: 3.0.20`

... continues on next page ...

... continued from previous page ...

Fixed version: 4.2.11 or 4.3.8 or 4.4.2, or later

Impact
Successful exploitation of this vulnerability leads to Man-in-the-middle (MITM) attacks, to causes denial of service, to spoof and to obtain sensitive session information.
Impact Level: Application

Solution
Solution type: VendorFix
Upgrade to samba version 4.2.11, or 4.3.8, or 4.4.2, or later.

Affected Software/OS
Samba versions 3.0.x through 4.4.1 — NOTE: Samba versions 4.2.11, 4.3.8 are not affected —

Vulnerability Insight
The multiple flaws are due to - The Multiple errors in DCE-RPC code. - A spoofing Vulnerability in NETLOGON. - The LDAP implementation did not enforce integrity protection for LDAP connections. - The SSL/TLS certificates are not validated in certain connections. - Not enforcing Server Message Block (SMB) signing for clients using the SMB1 protocol. - An integrity protection for IPC traffic is not enabled by default - The MS-SAMR and MS-LSAD protocol implementations mishandle DCERPC connections. - An error in the implementation of NTLMSSP authentication. -

Vulnerability Detection Method
Get the installed version with the help of detect NVT and check the version is vulnerable or not.
Details:Samba Badlock Critical Vulnerability
OID:1.3.6.1.4.1.25623.1.0.807646
Version used: $Revision: 4401 $

Product Detection Result
Product: cpe:/a:samba:samba:3.0.20
Method: SMB NativeLanMan
OID: 1.3.6.1.4.1.25623.1.0.102011)

References
CVE: CVE-2016-2118, CVE-2015-5370, CVE-2016-2110, CVE-2016-2111, CVE-2016-2112,
↪CVE-2016-2113, CVE-2016-2114, CVE-2016-2115, CVE-2016-0128
Other:
URL:http://badlock.org/
URL:http://thehackernews.com/2016/03/windows-samba-vulnerability.html

Medium (CVSS: 5.8)
NVT: Samba Format String Vulnerability

Product detection result
cpe:/a:samba:samba:3.0.20

... continues on next page ...

... continued from previous page ...

Detected by SMB NativeLanMan (OID: 1.3.6.1.4.1.25623.1.0.102011)

Summary
The host has Samba installed and is prone to Security Bypass Vulnerability.

Vulnerability Detection Result
Installed version: 3.0.20
Fixed version: 3.0.35/3.2.13/3.3.6

Impact
When dos filemode is set to yes in the smb.conf, attackers can exploit this issue to bypass certain security restrictions and compromise a user's system.
Impact Level: System

Solution
Solution type: VendorFix
Upgrade to 3.3.6 of Samba, http://us3.samba.org/samba/

Affected Software/OS
Samba 3.0.0 before 3.0.35 on Linux. Samba 3.1.x on Linux. Samba 3.2.4 before 3.2.13 on Linux. Samba 3.3.0 before 3.3.6 on Linux.

Vulnerability Insight
The flaw is due to uninitialised memory access error in 'smbd' when denying attempts to modify a restricted access control list. This can be exploited to modify the ACL of an already writable file without required permissions.

Vulnerability Detection Method
Details:Samba Format String Vulnerability
OID:1.3.6.1.4.1.25623.1.0.900685
Version used: $Revision: 4393 $

Product Detection Result
Product: cpe:/a:samba:samba:3.0.20
Method: SMB NativeLanMan
OID: 1.3.6.1.4.1.25623.1.0.102011)

References
CVE: CVE-2009-1888
BID:35472
Other:
URL:http://secunia.com/advisories/35539
URL:http://www.vupen.com/english/advisories/2009/1664

Medium (CVSS: 6.0)
NVT: Samba MS-RPC Remote Shell Command Execution Vulnerability (Active Check)

Product detection result
cpe:/a:samba:samba:3.0.20
Detected by SMB NativeLanMan (OID: 1.3.6.1.4.1.25623.1.0.102011)

Summary
Samba is prone to a vulnerability that allows attackers to execute arbitrary shell commands because the software fails to sanitize user-supplied input.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact
An attacker may leverage this issue to execute arbitrary shell commands on an affected system with the privileges of the application.

Solution
Solution type: VendorFix
Updates are available. Please see the referenced vendor advisory.

Affected Software/OS
This issue affects Samba 3.0.0 to 3.0.25rc3.

Vulnerability Detection Method
Send a crafted command to the samba server and check for a remote command execution.
Details:Samba MS-RPC Remote Shell Command Execution Vulnerability (Active Check)
OID:1.3.6.1.4.1.25623.1.0.108011
Version used: $Revision: 4401 $

Product Detection Result
Product: cpe:/a:samba:samba:3.0.20
Method: SMB NativeLanMan
OID: 1.3.6.1.4.1.25623.1.0.102011)

References
CVE: CVE-2007-2447
BID:23972
Other:
URL:http://www.securityfocus.com/bid/23972
URL:https://www.samba.org/samba/security/CVE-2007-2447.html

... continues on next page ...

... continued from previous page ...

Medium (CVSS: 6.0)
NVT: Samba MS-RPC Remote Shell Command Execution Vulnerability (Version Check)

Product detection result
cpe:/a:samba:samba:3.0.20
Detected by SMB NativeLanMan (OID: 1.3.6.1.4.1.25623.1.0.102011)

Summary
Samba is prone to a vulnerability that allows attackers to execute arbitrary shell commands because the software fails to sanitize user-supplied input.

Vulnerability Detection Result
Installed version: 3.0.20
Fixed version: See referenced vendor advisory

Impact
An attacker may leverage this issue to execute arbitrary shell commands on an affected system with the privileges of the application.

Solution
Solution type: VendorFix
Updates are available. Please see the referenced vendor advisory.

Affected Software/OS
This issue affects Samba 3.0.0 to 3.0.25rc3.

Vulnerability Detection Method
Get the installed version with the help of the Detection NVT and check if the version is vulnerable or not.
Details:Samba MS-RPC Remote Shell Command Execution Vulnerability (Version Check)
OID:1.3.6.1.4.1.25623.1.0.108012
Version used: $Revision: 5933 $

Product Detection Result
Product: cpe:/a:samba:samba:3.0.20
Method: SMB NativeLanMan
OID: 1.3.6.1.4.1.25623.1.0.102011)

References
CVE: CVE-2007-2447
BID:23972
Other:
URL:http://www.securityfocus.com/bid/23972
URL:https://www.samba.org/samba/security/CVE-2007-2447.html

Medium (CVSS: 6.0)
NVT: Samba multiple vulnerabilities

Product detection result
cpe:/a:samba:samba:3.0.20
Detected by SMB NativeLanMan (OID: 1.3.6.1.4.1.25623.1.0.102011)

Summary
Samba is prone to multiple vulnerabilities including a vulnerability that may allow attackers to bypass certain security restrictions, an information-disclosure vulnerability and a remote denial-of-service vulnerability.

Vulnerability Detection Result
Installed version: 3.0.20
Fixed version: 3.0.37/3.2.15/3.3.8/3.4.2

Impact
Successful exploits may allow attackers to gain access to resources that aren't supposed to be shared, allow attackers to obtain sensitive information that may aid in further attacks and to cause the application to consume excessive CPU resources, denying service to legitimate users.

Solution
Solution type: VendorFix
Updates are available. Please see the references for more information.

Affected Software/OS
Versions prior to Samba 3.4.2, 3.3.8, 3.2.15, and 3.0.37 are vulnerable.

Vulnerability Detection Method
Details:Samba multiple vulnerabilities
OID:1.3.6.1.4.1.25623.1.0.100306
Version used: $Revision: 4393 $

Product Detection Result
Product: cpe:/a:samba:samba:3.0.20
Method: SMB NativeLanMan
OID: 1.3.6.1.4.1.25623.1.0.102011)

References
CVE: CVE-2009-2813, CVE-2009-2948, CVE-2009-2906
BID:36363, 36572, 36573
Other:
URL:http://www.securityfocus.com/bid/36363
URL:http://www.securityfocus.com/bid/36573
URL:http://www.securityfocus.com/bid/36572
URL:http://www.samba.org/samba/security/CVE-2009-2813.html

... continues on next page ...

... continued from previous page ...

URL:http://www.samba.org/samba/security/CVE-2009-2948.html
URL:http://www.samba.org/samba/security/CVE-2009-2906.html
URL:http://www.samba.org/samba/history/security.html
URL:http://us1.samba.org/samba/

Medium (CVSS: 5.0)
NVT: Samba winbind Daemon Denial of Service Vulnerability

Product detection result
cpe:/a:samba:samba:3.0.20
Detected by SMB NativeLanMan (OID: 1.3.6.1.4.1.25623.1.0.102011)

Summary
This host is installed with Samba for Linux and is prone to Winbind daemon Denial of Service Vulnerability.

Vulnerability Detection Result
Installed version: 3.0.20
Fixed version: 3.0.32

Impact
Successful exploitation will let the attacker crash the application.
Impact level: Application

Solution
Solution type: VendorFix
Upgrade to the latest version 3.0.32 http://us1.samba.org/samba

Affected Software/OS
Samba version prior to 3.0.32

Vulnerability Insight
This flaw is due to a race condition in the winbind daemon which allows remote attackers to cause denial of service through unspecified vectors related to an unresponsive child process.

Vulnerability Detection Method
Details:Samba winbind Daemon Denial of Service Vulnerability
OID:1.3.6.1.4.1.25623.1.0.800711
Version used: $Revision: 4393 $

Product Detection Result
Product: cpe:/a:samba:samba:3.0.20
Method: SMB NativeLanMan
OID: 1.3.6.1.4.1.25623.1.0.102011)

... continues on next page ...

... continued from previous page ...

References
Other:
URL:http://wiki.rpath.com/wiki/Advisories:rPSA-2008-0308
URL:http://www.samba.org/samba/history/samba-3.0.32.html
URL:http://www.securityfocus.com/archive/1/archive/1/497941/100/0/threaded

[return to 192.168.8.102]

2.1.19 Medium 21/tcp

Medium (CVSS: 6.4)
NVT: Check for Anonymous FTP Login

Summary
This FTP Server allows anonymous logins.

Vulnerability Detection Result
It was possible to login to the remote FTP service with the following anonymous
↪account:
anonymous:openvas@example.com
ftp:openvas@example.com

Impact
Based on the files accessible via this anonymous FTP login and the permissions of this account an attacker might be able to:
- gain access to sensitive files
- upload or delete files

Solution
Solution type: Mitigation
If you do not want to share files, you should disable anonymous logins.

Vulnerability Insight
A host that provides an FTP service may additionally provide Anonymous FTP access as well. Under this arrangement, users do not strictly need an account on the host. Instead the user typically enters 'anonymous' or 'ftp' when prompted for username. Although users are commonly asked to send their email address as their password, little to no verification is actually performed on the supplied data.

Vulnerability Detection Method
Try to login with an anonymous account at the remove FTP service.
Details:Check for Anonymous FTP Login
OID:1.3.6.1.4.1.25623.1.0.900600
Version used: $Revision: 4987 $

... continues on next page ...

... continued from previous page ...

References
Other:
URL:https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-1999-0497

Medium (CVSS: 5.1)
NVT: vsftpd '__tzfile_read()' Function Heap Based Buffer Overflow Vulnerability

Product detection result
cpe:/a:beasts:vsftpd:2.3.4
Detected by vsFTPd FTP Server Detection (OID: 1.3.6.1.4.1.25623.1.0.111050)

Summary
vsftpd is prone to a buffer-overflow vulnerability because it fails to perform adequate boundary checks on user-supplied data.

Vulnerability Detection Result
Installed version: 2.3.4
Fixed version: 2.3.5

Impact
Attackers may leverage this issue to execute arbitrary code in the context of the application. Failed attacks will cause denial-of-service conditions.

Solution
Solution type: VendorFix
A fixed version 2.3.5 is available. Please see the references for more information.

Affected Software/OS
vsftpd 2.3.4 is affected other versions may also be vulnerable.

Vulnerability Detection Method
Details:vsftpd '__tzfile_read()' Function Heap Based Buffer Overflow Vulnerability
OID:1.3.6.1.4.1.25623.1.0.103362
Version used: $Revision: 5026 $

Product Detection Result
Product: cpe:/a:beasts:vsftpd:2.3.4
Method: vsFTPd FTP Server Detection
OID: 1.3.6.1.4.1.25623.1.0.111050)

References
BID:51013
Other:

... continues on next page ...

... continued from previous page ...

URL:http://www.securityfocus.com/bid/51013
URL:http://dividead.wordpress.com/tag/heap-overflow/
URL:https://security.appspot.com/vsftpd/Changelog.txt
URL:https://security.appspot.com/vsftpd.html

Medium (CVSS: 5.0)
NVT: vsftpd < 3.0.3 Security Bypass Vulnerability

Product detection result
cpe:/a:beasts:vsftpd:2.3.4
Detected by vsFTPd FTP Server Detection (OID: 1.3.6.1.4.1.25623.1.0.111050)

Summary
vsftpd is prone to a security-bypass vulnerability.

Vulnerability Detection Result
Installed version: 2.3.4
Fixed version: 3.0.3

Impact
An attacker can exploit this issue to bypass certain security restrictions and perform unauthorized actions. This may aid in further attacks.

Solution
Solution type: VendorFix
A fixed version 3.0.3 is available. Please see the references for more information.

Affected Software/OS
vsftpd versions 3.0.2 and below are vulnerable.

Vulnerability Detection Method
Details:vsftpd < 3.0.3 Security Bypass Vulnerability
OID:1.3.6.1.4.1.25623.1.0.108045
Version used: $Revision: 5026 $

Product Detection Result
Product: cpe:/a:beasts:vsftpd:2.3.4
Method: vsFTPd FTP Server Detection
OID: 1.3.6.1.4.1.25623.1.0.111050)

References
CVE: CVE-2015-1419
BID:72451
Other:

... continues on next page ...

... continued from previous page ...

URL:http://www.securityfocus.com/bid/72451
URL:https://security.appspot.com/vsftpd/Changelog.txt
URL:https://security.appspot.com/vsftpd.html

[return to 192.168.8.102]

2.1.20 Medium 53/tcp

Medium (CVSS: 4.3)
NVT: ISC BIND 'lightweight resolver protocol' Denial of Service Vulnerability

Product detection result
cpe:/a:isc:bind:9.4.2
Detected by Determine which version of BIND name daemon is running (OID: 1.3.6.1
↪.4.1.25623.1.0.10028)

Summary
The host is installed with ISC BIND and is prone to denial of service vulnerability.

Vulnerability Detection Result
Installed version: 9.4.2
Fixed version: 9.9.9-P2

Impact
Successful exploitation will allow remote attackers to cause denial of service.
Impact Level: Application

Solution
Solution type: VendorFix
Upgrade to ISC BIND version 9.9.9-P2 or 9.10.4-P2 or 9.11.0b2 or later. For updates refer to https://www.isc.org

Affected Software/OS
ISC BIND versions 9.0.x through 9.9.9-P1, 9.10.0 through 9.10.4-P1, 9.11.0a3 through 9.11.0b1.

Vulnerability Insight
The flaw is due to an error in the BIND implementation of the lightweight resolver protocol which use alternate method to do name resolution.

Vulnerability Detection Method
Get the installed version with the help of detect NVT and check the version is vulnerable or not.
Details:ISC BIND 'lightweight resolver protocol' Denial of Service Vulnerability
OID:1.3.6.1.4.1.25623.1.0.808751
Version used: $Revision: 4429 $

... continues on next page ...

... continued from previous page ...

Product Detection Result
Product: cpe:/a:isc:bind:9.4.2
Method: Determine which version of BIND name daemon is running
OID: 1.3.6.1.4.1.25623.1.0.10028)

References
CVE: CVE-2016-2775
BID:92037
Other:
URL:https://kb.isc.org/article/AA-01393/74/CVE-2016-2775

Medium (CVSS: 4.3)
NVT: ISC BIND 9 Remote Dynamic Update Message Denial of Service Vulnerability

Product detection result
cpe:/a:isc:bind:9.4.2
Detected by Determine which version of BIND name daemon is running (OID: 1.3.6.1
↪.4.1.25623.1.0.10028)

Summary
ISC BIND is prone to a remote denial-of-service vulnerability because the application fails to properly handle specially crafted dynamic update requests.

Vulnerability Detection Result
OpenVAS only check the version number (from TXT record in the
Chaos class) because "safe checks" are enabled.

Impact
Successfully exploiting this issue allows remote attackers to crash affected DNS servers, denying further service to legitimate users.

Solution
Solution type: VendorFix
The vendor released an advisory and fixes to address this issue. Please see the references for more information.

Affected Software/OS
Versions prior to BIND 9.4.3-P3, 9.5.1-P3, and 9.6.1-P1 are vulnerable.

Vulnerability Detection Method
Details:ISC BIND 9 Remote Dynamic Update Message Denial of Service Vulnerability
OID:1.3.6.1.4.1.25623.1.0.100251
Version used: $Revision: 4436 $

... continues on next page ...

... continued from previous page ...

Product Detection Result
Product: cpe:/a:isc:bind:9.4.2
Method: Determine which version of BIND name daemon is running
OID: 1.3.6.1.4.1.25623.1.0.10028)

References
CVE: CVE-2009-0696
BID:35848
Other:
URL:http://www.securityfocus.com/bid/35848
URL:https://bugzilla.redhat.com/show_bug.cgi?id=514292
URL:http://bugs.debian.org/cgi-bin/bugreport.cgi?bug=538975
URL:http://www.isc.org/products/BIND/
URL:https://www.isc.org/node/474
URL:http://www.kb.cert.org/vuls/id/725188

Medium (CVSS: 4.0)
NVT: ISC BIND AXFR Response Denial of Service Vulnerability

Product detection result
cpe:/a:isc:bind:9.4.2
Detected by Determine which version of BIND name daemon is running (OID: 1.3.6.1
↪.4.1.25623.1.0.10028)

Summary
ISC BIND is prone to a denial of service vulnerability.

Vulnerability Detection Result
Installed version: 9.4.2
Fixed version: Workaround

Impact
An authenticated remote attacker may cause a denial of service condition.

Solution
Solution type: Workaround
As a workaround operators of servers which accept untrusted zone data can mitigate their risk by operating an intermediary server whose role it is to receive zone data and then (if successful) redistribute it to client-facing servers. Successful exploitation of the attack against the intermediary server may still occur but denial of service against the client-facing servers is significantly more difficult to achieve in this scenario.

Affected Software/OS

... continues on next page ...

... continued from previous page ...

Version <= 9.10.4-P1

Vulnerability Insight
Primary DNS servers may cause a denial of service (secondary DNS server crash) via a large AXFR response, and possibly allows IXFR servers to cause a denial of service (IXFR client crash) via a large IXFR response and allows remote authenticated users to cause a denial of service (primary DNS server crash) via a large UPDATE message

Vulnerability Detection Method
Checks the version.
Details:`ISC BIND AXFR Response Denial of Service Vulnerability`
OID:1.3.6.1.4.1.25623.1.0.106118
Version used: `$Revision: 4446 $`

Product Detection Result
Product: `cpe:/a:isc:bind:9.4.2`
Method: `Determine which version of BIND name daemon is running`
OID: 1.3.6.1.4.1.25623.1.0.10028)

References
`CVE: CVE-2016-6170`
`Other:`
`URL:http://www.openwall.com/lists/oss-security/2016/07/06/3`
`URL:https://lists.dns-oarc.net/pipermail/dns-operations/2016-July/015058.html`

Medium (CVSS: 5.0)
NVT: ISC BIND Denial of Service Vulnerability

Product detection result
`cpe:/a:isc:bind:9.4.2`
`Detected by Determine which version of BIND name daemon is running (OID: 1.3.6.1`
`↪.4.1.25623.1.0.10028)`

Summary
ISC BIND is prone to a denial of service vulnerability.

Vulnerability Detection Result
`Installed version: 9.4.2`
`Fixed version: 9.9.9-P4`

Impact
An remote attacker may cause a denial of service condition.

Solution

... continues on next page ...

... continued from previous page ...

Solution type: VendorFix
Upgrade to 9.9.9-P4, 9.9.9-S6, 9.10.4-P4, 9.11.0-P1 or later.

Affected Software/OS
BIND 9

Vulnerability Insight
A defect in BIND's handling of responses containing a DNAME answer can cause a resolver to exit after encountering an assertion failure in db.c or resolver.c

Vulnerability Detection Method
Checks the version.
Details:`ISC BIND Denial of Service Vulnerability`
OID:1.3.6.1.4.1.25623.1.0.106366
Version used: `$Revision: 4485 $`

Product Detection Result
Product: `cpe:/a:isc:bind:9.4.2`
Method: `Determine which version of BIND name daemon is running`
OID: 1.3.6.1.4.1.25623.1.0.10028)

References
`CVE: CVE-2016-8864`
`Other:`
`URL:https://kb.isc.org/article/AA-01434`

Medium (CVSS: 6.8)
NVT: ISC BIND Denial of Service Vulnerability - 02 - Jan16

Product detection result
`cpe:/a:isc:bind:9.4.2`
`Detected by Determine which version of BIND name daemon is running (OID: 1.3.6.1`
`↪.4.1.25623.1.0.10028)`

Summary
The host is installed with ISC BIND and is prone to remote denial of service vulnerability.

Vulnerability Detection Result
`Installed version: 9.4.2`
`Fixed version: 9.9.8-P3`

Impact
Successful exploitation will allow remote attackers to cause denial of service.
Impact Level: Application

... continues on next page ...

... continued from previous page ...

Solution
Solution type: VendorFix
Upgrade to ISC BIND version 9.9.8-P3 or 9.10.3-P3 or 9.9.8-S4 or later. For updates refer to https://www.isc.org

Affected Software/OS
ISC BIND versions 9.3.0 through 9.8.8, 9.9.0 through 9.9.8-P2, 9.9.3-S1 through 9.9.8-S3, 9.10.0 through 9.10.3-P2.

Vulnerability Insight
The flaw is due to an error in 'apl_42.c' script in ISC BIND.

Vulnerability Detection Method
Get the installed version with the help of detect NVT and check the version is vulnerable or not.
Details:`ISC BIND Denial of Service Vulnerability - 02 - Jan16`
OID:1.3.6.1.4.1.25623.1.0.806996
Version used: `$Revision: 4429 $`

Product Detection Result
Product: `cpe:/a:isc:bind:9.4.2`
Method: `Determine which version of BIND name daemon is running`
OID: 1.3.6.1.4.1.25623.1.0.10028)

References
`CVE: CVE-2015-8704`
`Other:`
`URL:https://kb.isc.org/article/AA-01335`

Medium (CVSS: 5.0)
NVT: ISC BIND Denial of Service Vulnerability - 03 - Jan16

Product detection result
`cpe:/a:isc:bind:9.4.2`
`Detected by Determine which version of BIND name daemon is running (OID: 1.3.6.1`
`↪.4.1.25623.1.0.10028)`

Summary
The host is installed with ISC BIND and is prone to remote denial of service vulnerability.

Vulnerability Detection Result
`Installed version: 9.4.2`
`Fixed version: 9.9.8-P2`

... continues on next page ...

... continued from previous page ...

Impact
Successful exploitation will allow remote attackers to cause denial of service.
Impact Level: Application

Solution
Solution type: VendorFix
Upgrade to ISC BIND version 9.9.8-P2 or 9.10.3-P2 or later. For updates refer to https://www.isc.org

Affected Software/OS
ISC BIND versions 9.0.x through 9.9.8, 9.10.0 through 9.10.3.

Vulnerability Insight
The flaw is due to an error in 'db.c' script in ISC BIND.

Vulnerability Detection Method
Get the installed version with the help of detect NVT and check the version is vulnerable or not.
Details:`ISC BIND Denial of Service Vulnerability - 03 - Jan16`
OID:1.3.6.1.4.1.25623.1.0.806997
Version used: `$Revision: 4429 $`

Product Detection Result
Product: `cpe:/a:isc:bind:9.4.2`
Method: `Determine which version of BIND name daemon is running`
OID: 1.3.6.1.4.1.25623.1.0.10028)

References
`CVE: CVE-2015-8000`
`BID:79349`
`Other:`
`URL:https://kb.isc.org/article/AA-01317`

Medium (CVSS: 4.3)
NVT: ISC BIND lwresd Denial of Service Vulnerability

Product detection result
`cpe:/a:isc:bind:9.4.2`
`Detected by Determine which version of BIND name daemon is running (OID: 1.3.6.1`
`↪.4.1.25623.1.0.10028)`

Summary
ISC BIND is prone to a denial of service vulnerability.

Vulnerability Detection Result

... continues on next page ...

... continued from previous page ...

```
Installed version: 9.4.2
Fixed version:     9.9.9-P2
```

Impact
An remote attacker may cause a denial of service condition.

Solution
Solution type: VendorFix
Upgrade to 9.9.9-P1, 9.10.4-P1, 9.11.0b1 or later.

Affected Software/OS
BIND 9

Vulnerability Insight
The lwresd component in BIND (which is not enabled by default) could crash while processing an overlong request name. This could lead to a denial of service.

Vulnerability Detection Method
Checks the version.
Details:`ISC BIND lwresd Denial of Service Vulnerability`
OID:1.3.6.1.4.1.25623.1.0.106292
Version used: `$Revision: 4429 $`

Product Detection Result
Product: `cpe:/a:isc:bind:9.4.2`
Method: `Determine which version of BIND name daemon is running`
OID: 1.3.6.1.4.1.25623.1.0.10028)

References
`CVE: CVE-2016-2775`
`Other:`
`URL:https://kb.isc.org/article/AA-01393`

Medium (CVSS: 5.0)
NVT: ISC BIND NSID Request Denial of Service Vulnerability (Linux)

Product detection result
`cpe:/a:isc:bind:9.4.2`
`Detected by Determine which version of BIND name daemon is running (OID: 1.3.6.1`
`↪.4.1.25623.1.0.10028)`

Summary
The host is installed with ISC BIND and is prone to denial of service vulnerability.

... continues on next page ...

... continued from previous page ...

Vulnerability Detection Result
Installed version: 9.4.2
Fixed version: 9.9.9-P3 or 9.10.4-P3 or 9.11.0

Impact
Successful exploitation will allow remote attackers to cause a denial of service.
Impact Level: Application

Solution
Solution type: VendorFix
Upgrade to ISC BIND version 9.9.9-P3 or 9.10.4-P3 or 9.11.0 or later on Linux. For updates refer to https://www.isc.org

Affected Software/OS
ISC BIND versions 9.1.0 through 9.8.4-P2 and 9.9.0 through 9.9.2-P2 on Linux.

Vulnerability Insight
The flaw exist due to mishandling of packets with malformed options. A remote attacker could use this flaw to make named exit unexpectedly with an assertion failure via a specially crafted DNS packet.

Vulnerability Detection Method
Get the installed version with the help of detect NVT and check the version is vulnerable or not.
Details:ISC BIND NSID Request Denial of Service Vulnerability (Linux)
OID:1.3.6.1.4.1.25623.1.0.809461
Version used: $Revision: 5083 $

Product Detection Result
Product: cpe:/a:isc:bind:9.4.2
Method: Determine which version of BIND name daemon is running
OID: 1.3.6.1.4.1.25623.1.0.10028)

References
CVE: CVE-2016-2848
BID:93814
Other:
URL:https://kb.isc.org/article/AA-01433/74/CVE-2016-2848

Medium (CVSS: 5.0)
NVT: ISC BIND Resolver Cache Vulnerability - Jan16

Product detection result
cpe:/a:isc:bind:9.4.2
Detected by Determine which version of BIND name daemon is running (OID: 1.3.6.1
↪.4.1.25623.1.0.10028)

... continues on next page ...

... continued from previous page ...

Summary
The host is installed with ISC BIND and is prone to resolver cache vulnerability.

Vulnerability Detection Result
`Installed version: 9.4.2`
`Fixed version: Workaround`

Impact
Successful exploitation will allow remote attackers to trigger continued resolvability of domain names that are no longer registered.
Impact Level: Application

Solution
Solution type: Workaround
As a workaround it is recommended to clear the cache, which will remove cached bad records but is not an effective or practical preventative approach. For updates refer to https://www.isc.org

Affected Software/OS
ISC BIND versions 9 through 9.8.1-P1.

Vulnerability Insight
The flaw exist due to the resolver overwrites cached server names and TTL values in NS records during the processing of a response to an A record query.

Vulnerability Detection Method
Get the installed version with the help of detect NVT and check the version is vulnerable or not.
Details:`ISC BIND Resolver Cache Vulnerability - Jan16`
OID:1.3.6.1.4.1.25623.1.0.807217
Version used: `$Revision: 4446 $`

Product Detection Result
Product: `cpe:/a:isc:bind:9.4.2`
Method: `Determine which version of BIND name daemon is running`
OID: 1.3.6.1.4.1.25623.1.0.10028)

References
`CVE: CVE-2012-1033`
`BID:51898`
`Other:`
`URL:https://www.kb.cert.org/vuls/id/542123`

Medium (CVSS: 5.0)
NVT: ISC BIND RTYPE ANY Query Denial of Service Vulnerability (Linux)

... continues on next page ...

... continued from previous page ...

Product detection result
cpe:/a:isc:bind:9.4.2
Detected by Determine which version of BIND name daemon is running (OID: 1.3.6.1
↪.4.1.25623.1.0.10028)

Summary
The host is installed with ISC BIND and is prone to denial of service vulnerability.

Vulnerability Detection Result
Installed version: 9.4.2
Fixed version: 9.9.9-P5

Impact
Successful exploitation will allow remote attackers to cause a denial of service (assertion failure and daemon exit) via crafted data.
Impact Level: Application

Solution
Solution type: VendorFix
Upgrade to ISC BIND version 9.9.9-P5 or 9.10.4-P5 or 9.11.0-P2 or 9.9.9-S7 or later on Linux. For updates refer to https://www.isc.org

Affected Software/OS
ISC BIND versions 9.4.0 through 9.6-ESV-R11-W1, 9.8.5 through 9.8.8, 9.9.3 through 9.9.9-P4, 9.9.9-S1 through 9.9.9-S6, 9.10.0 through 9.10.4-P4 and 9.11.0 through 9.11.0-P1 on Linux.

Vulnerability Insight
The flaw exist due to an error in the processing of a malformed query response received in response to a RTYPE ANY query.

Vulnerability Detection Method
Get the installed version with the help of detect NVT and check the version is vulnerable or not.
Details:ISC BIND RTYPE ANY Query Denial of Service Vulnerability (Linux)
OID:1.3.6.1.4.1.25623.1.0.810287
Version used: $Revision: 5287 $

Product Detection Result
Product: cpe:/a:isc:bind:9.4.2
Method: Determine which version of BIND name daemon is running
OID: 1.3.6.1.4.1.25623.1.0.10028)

References
CVE: CVE-2016-9131
BID:95386
Other:

... continues on next page ...

... continued from previous page ...

URL:https://kb.isc.org/article/AA-01439/0

Medium (CVSS: 6.8)
NVT: OpenSSL DSA_verify() Security Bypass Vulnerability in BIND

Product detection result
cpe:/a:isc:bind:9.4.2
Detected by Determine which version of BIND name daemon is running (OID: 1.3.6.1
↪.4.1.25623.1.0.10028)

Summary
The host is running BIND and is prone to Security Bypass Vulnerability.

Vulnerability Detection Result
Installed version: 9.4.2
Fixed version: 9.6.0 P1, 9.5.1 P1, 9.4.3 P1 or 9.3.6 P1

Impact
Successful exploitation could allow remote attackers to bypass the certificate validation checks and can cause man-in-the-middle attack via signature checks on DSA and ECDSA keys used with SSL/TLS.
Impact Level: Application

Solution
Solution type: VendorFix
Upgrade to version 9.6.0 P1, 9.5.1 P1, 9.4.3 P1, 9.3.6 P1 https://www.isc.org/downloadables/11

Affected Software/OS
ISC BIND version prior to 9.2 or 9.6.0 P1 or 9.5.1 P1 or 9.4.3 P1 or 9.3.6 P1/Linux

Vulnerability Insight
The flaw is due to improper validation of return value from OpenSSL's DSA_do_verify and VP_VerifyFinal functions.

Vulnerability Detection Method
Details:OpenSSL DSA_verify() Security Bypass Vulnerability in BIND
OID:1.3.6.1.4.1.25623.1.0.800338
Version used: $Revision: 4435 $

Product Detection Result
Product: cpe:/a:isc:bind:9.4.2
Method: Determine which version of BIND name daemon is running
OID: 1.3.6.1.4.1.25623.1.0.10028)

... continues on next page ...

... continued from previous page ...

References
CVE: CVE-2008-5077, CVE-2009-0025, CVE-2009-0265
BID:33150, 33151
Other:
URL:https://www.isc.org/node/373
URL:http://secunia.com/advisories/33404/
URL:http://www.ocert.org/advisories/ocert-2008-016.html

[return to 192.168.8.102]

2.1.21 Medium 80/tcp

Medium (CVSS: 5.0)
NVT: /doc directory browsable

Summary
The /doc directory is browsable. /doc shows the content of the /usr/doc directory and therefore it shows which programs and - important! - the version of the installed programs.

Vulnerability Detection Result
Vulnerable url: http://192.168.8.102/doc/

Solution
Solution type: Mitigation
Use access restrictions for the /doc directory. If you use Apache you might use this in your access.conf:
<Directory /usr/doc> AllowOverride None order deny,allow deny from all allow from localhost </Directory>

Vulnerability Detection Method
Details:/doc directory browsable
OID:1.3.6.1.4.1.25623.1.0.10056
Version used: $Revision: 4288 $

References
CVE: CVE-1999-0678
BID:318

Medium (CVSS: 4.9)
NVT: Apache 'Options' and 'AllowOverride' Directives Security Bypass Vulnerability

Summary
Apache HTTP server is prone to a security-bypass vulnerability related to the handling of specific configuration directives.

... continues on next page ...

... continued from previous page ...

A local attacker may exploit this issue to execute arbitrary code within the context of the webserver process. This may result in elevated privileges or aid in further attacks.
Versions prior to Apache 2.2.9 are vulnerable.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Solution
Updates are available. Please see http://httpd.apache.org/ for more Information.

Vulnerability Detection Method
Details:`Apache 'Options' and 'AllowOverride' Directives Security Bypass Vulnerability`
OID:1.3.6.1.4.1.25623.1.0.100211
Version used: `$Revision: 4574 $`

References
`CVE: CVE-2009-1195`
`BID:35115`
`Other:`
`URL:http://www.securityfocus.com/bid/35115`

Medium (CVSS: 4.3)
NVT: Apache HTTP Server 'httpOnly' Cookie Information Disclosure Vulnerability

Summary
This host is running Apache HTTP Server and is prone to cookie information disclosure vulnerability.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact
Successful exploitation will allow attackers to obtain sensitive information that may aid in further attacks.
Impact Level: Application

Solution
Solution type: VendorFix
Upgrade to Apache HTTP Server version 2.2.22 or later, For updates refer to http://httpd.apache.org/

Affected Software/OS
Apache HTTP Server versions 2.2.0 through 2.2.21

Vulnerability Insight

... continues on next page ...

... continued from previous page ...

The flaw is due to an error within the default error response for status code 400 when no custom ErrorDocument is configured, which can be exploited to expose 'httpOnly' cookies.

Vulnerability Detection Method
Details:Apache HTTP Server 'httpOnly' Cookie Information Disclosure Vulnerability
OID:1.3.6.1.4.1.25623.1.0.902830
Version used: $Revision: 5950 $

References
CVE: CVE-2012-0053
BID:51706
Other:
URL:http://secunia.com/advisories/47779
URL:http://www.exploit-db.com/exploits/18442
URL:http://rhn.redhat.com/errata/RHSA-2012-0128.html
URL:http://httpd.apache.org/security/vulnerabilities_22.html
URL:http://svn.apache.org/viewvc?view=revision&revision=1235454
URL:http://lists.opensuse.org/opensuse-security-announce/2012-02/msg00026.htm
↪l

Medium (CVSS: 5.1)
NVT: Apache HTTP Server Man-in-the-Middle attack Vulnerability - July16 (Linux)

Product detection result
cpe:/a:apache:http_server:2.2.8
Detected by Apache Web Server Version Detection (OID: 1.3.6.1.4.1.25623.1.0.9004
↪98)

Summary
This host is installed with Apache HTTP Server and is prone to man-in-the-middle attack vulnerability.

Vulnerability Detection Result
Installed version: 2.2.8
Fixed version: 2.4.24

Impact
Successful exploitation will allow remote attackers to redirect an application's outbound HTTP traffic to an arbitrary proxy server via a crafted proxy header in an HTTP request.
Impact Level: Application

Solution
Solution type: VendorFix
Upgrade to version 2.4.24, or 2.2.32, or newer. For updates refer http://www.apache.org

... continues on next page ...

... continued from previous page ...

Affected Software/OS
Apache HTTP Server through 2.4.23 on Linux —- NOTE: Apache HTTP Server 2.2.32 is not vulnerable —-

Vulnerability Insight
The flaw is due to 'CGI Servlet' does not protect applications from the presence of untrusted client data in the 'HTTP_PROXY' environment variable.

Vulnerability Detection Method
Get the installed version with the help of detect NVT and check the version is vulnerable or not.
Details:`Apache HTTP Server Man-in-the-Middle attack Vulnerability - July16 (Linux)`
OID:1.3.6.1.4.1.25623.1.0.808632
Version used: `$Revision: 5588 $`

Product Detection Result
Product: `cpe:/a:apache:http_server:2.2.8`
Method: `Apache Web Server Version Detection`
OID: 1.3.6.1.4.1.25623.1.0.900498)

References
`CVE: CVE-2016-5387`
`BID:91816`
`Other:`
`URL:https://www.apache.org/security/asf-httpoxy-response.txt`

Medium (CVSS: 5.0)
NVT: Apache HTTP Server Mod_Lua Denial of service Vulnerability -01 May15

Product detection result
`cpe:/a:apache:http_server:2.2.8`
`Detected by Apache Web Server Version Detection (OID: 1.3.6.1.4.1.25623.1.0.9004`
`↪98)`

Summary
This host is installed with Apache HTTP Server and is prone to denial of service vulnerability.

Vulnerability Detection Result
`Installed version: 2.2.8`
`Fixed version: 2.4.13`

Impact
Successful exploitation will allow a remote attackers to cause a denial of service via some crafted dimension.
Impact Level: Application

... continues on next page ...

... continued from previous page ...

Solution
Solution type: VendorFix
Upgrade to version 2.4.13 or later, For updates refer http://www.apache.org

Affected Software/OS
Apache HTTP Server versions through 2.4.12.

Vulnerability Insight
Flaw is due to vulnerability in lua_websocket_read function in lua_request.c in the mod_lua module.

Vulnerability Detection Method
Get the installed version with the help of detect NVT and check the version is vulnerable or not.
Details:`Apache HTTP Server Mod_Lua Denial of service Vulnerability -01 May15`
OID:1.3.6.1.4.1.25623.1.0.805616
Version used: `$Revision: 3496 $`

Product Detection Result
Product: `cpe:/a:apache:http_server:2.2.8`
Method: `Apache Web Server Version Detection`
OID: 1.3.6.1.4.1.25623.1.0.900498)

References
`CVE: CVE-2015-0228`
`BID:73041`
`Other:`
`URL:https://bugs.mageia.org/show_bug.cgi?id=15428`
`URL:http://svn.apache.org/repos/asf/httpd/httpd/branches/2.4.x/CHANGES`

Medium (CVSS: 5.0)
NVT: Apache HTTP Server Multiple Remote Denial of Service Vulnerabilities

Summary
Apache HTTP Server is prone to multiple remote denial-of-service vulnerabilities.
An attacker can exploit these issues to deny service to legitimate users.
Versions prior to Apache 2.2.16 are vulnerable.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Solution
These issues have been fixed in Apache 2.2.16. Please see the references for more information.

Vulnerability Detection Method

... continues on next page ...

... continued from previous page ...

Details:Apache HTTP Server Multiple Remote Denial of Service Vulnerabilities
OID:1.3.6.1.4.1.25623.1.0.100725
Version used: $Revision: 5263 $

References
CVE: CVE-2010-1452
BID:41963
Other:
URL:https://www.securityfocus.com/bid/41963
URL:http://httpd.apache.org/download.cgi
URL:http://httpd.apache.org/
URL:http://www.apache.org/dist/httpd/Announcement2.2.html
URL:http://www.apache.org/dist/httpd/CHANGES_2.2.16

Medium (CVSS: 5.0)
NVT: Apache mod_proxy_ajp Information Disclosure Vulnerability

Summary
This host is running Apache Web Server and is prone to Information Disclosure Vulnerability.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact
Successful exploitation will let the attacker craft a special HTTP POST request and gain sensitive information about the web server.
Impact level: Application

Solution
Upgrade to Apache HTTP Version 2.2.15 or later For further updates refer, http://httpd.apache.org/download.cgi

Affected Software/OS
Apache HTTP Version 2.2.11
Workaround: Update mod_proxy_ajp.c through SVN Repository (Revision 767089) http://www.apache.org/dist/httpd/patches/apply_to_2.2.11/PR46949.diff

Vulnerability Insight
This flaw is due to an error in 'mod_proxy_ajp' when handling improperly malformed POST requests.

Vulnerability Detection Method
Details:Apache mod_proxy_ajp Information Disclosure Vulnerability
OID:1.3.6.1.4.1.25623.1.0.900499
Version used: $Revision: 5055 $

... continues on next page ...

... continued from previous page ...

References

CVE: CVE-2009-1191
BID:34663
Other:
URL:http://secunia.com/advisories/34827
URL:http://xforce.iss.net/xforce/xfdb/50059
URL:http://svn.apache.org/viewvc/httpd/httpd/trunk/CHANGES?r1=766938&r2=76708
↪9

Medium (CVSS: 4.3)
NVT: Apache mod_proxy_ftp Wildcard Characters XSS Vulnerability

Product detection result

cpe:/a:apache:http_server:2.2.8
Detected by Apache Web Server Version Detection (OID: 1.3.6.1.4.1.25623.1.0.9004
↪98)

Summary

The host is running Apache, which is prone to cross-site scripting vulnerability.

Vulnerability Detection Result

Installed version: 2.2.8
Fixed version: See reference

Impact

Remote attackers can execute arbitrary script code.
Impact Level : Application

Solution

Solution type: VendorFix
Fixed is available in the SVN repository, http://svn.apache.org/viewvc?view=rev&revision=682871
http://svn.apache.org/viewvc?view=rev&revision=682868

Affected Software/OS

Apache 2.0.0 to 2.0.63 and Apache 2.2.0 to 2.2.9 on All Platform
* Note: The script might report a False Positive as it is only checking for the vulnerable version of Apache. Vulnerability is only when mod_proxy and mod_proxy_ftp is configured with the installed Apache version. ***

Vulnerability Insight

Input passed to the module mod_proxy_ftp with wildcard character is not properly sanitized before returning to the user.

Vulnerability Detection Method

Details:Apache mod_proxy_ftp Wildcard Characters XSS Vulnerability

... continues on next page ...

... continued from previous page ...

OID:1.3.6.1.4.1.25623.1.0.900107
Version used: $Revision: 4334 $

Product Detection Result
Product: cpe:/a:apache:http_server:2.2.8
Method: Apache Web Server Version Detection
OID: 1.3.6.1.4.1.25623.1.0.900498)

References
CVE: CVE-2008-2939
BID:30560
Other:
URL:http://httpd.apache.org/
URL:http://www.securityfocus.com/archive/1/495180
URL:http://httpd.apache.org/docs/2.0/mod/mod_proxy_ftp.html

Medium (CVSS: 5.0)
NVT: awiki Multiple Local File Include Vulnerabilities

Summary
awiki is prone to multiple local file-include vulnerabilities because it fails to properly sanitize user-supplied input.

Vulnerability Detection Result
Vulnerable url: http://192.168.8.102/mutillidae/index.php?page=/etc/passwd

Impact
An attacker can exploit this vulnerability to obtain potentially sensitive information and execute arbitrary local scripts in the context of the webserver process. This may allow the attacker to compromise the application and the host other attacks are also possible.

Solution
Solution type: WillNotFix
No solution or patch was made available for at least one year since disclosure of this vulnerability. Likely none will be provided anymore. General solution options are to upgrade to a newer release, disable respective features, remove the product or replace the product by another one.

Affected Software/OS
awiki 20100125 is vulnerable other versions may also be affected.

Vulnerability Detection Method
Details:awiki Multiple Local File Include Vulnerabilities
OID:1.3.6.1.4.1.25623.1.0.103210
Version used: $Revision: 5651 $

... continues on next page ...

... continued from previous page ...

References
BID:49187
Other:
URL:http://www.securityfocus.com/bid/49187
URL:http://www.kobaonline.com/awiki/

Medium (CVSS: 5.0)
NVT: Enabled Directory Listing Detection

Summary
The script attempts to identify directories with an enabled directory listing.

Vulnerability Detection Result
The following directories with an enabled directory listing were identified:
http://192.168.8.102/dav
http://192.168.8.102/doc
http://192.168.8.102/mutillidae/documentation
http://192.168.8.102/test
http://192.168.8.102/test/testoutput
Please review the content manually.

Impact
Based on the information shown an attacker might be able to gather additional info about the structure of this application.

Solution
Solution type: Mitigation
If not needed disable the directory listing within the webservers config.

Affected Software/OS
Webservers with an enabled directory listing.

Vulnerability Detection Method
Check the detected directories if a directory listing is enabled.
Details:Enabled Directory Listing Detection
OID:1.3.6.1.4.1.25623.1.0.111074
Version used: $Revision: 5440 $

References
Other:
URL:https://www.owasp.org/index.php/OWASP_Periodic_Table_of_Vulnerabilities_-_Directory_Indexing

... continues on next page ...

... continued from previous page ...

Medium (CVSS: 5.8)
NVT: http TRACE XSS attack

Summary
Debugging functions are enabled on the remote HTTP server.
The remote webserver supports the TRACE and/or TRACK methods. TRACE and TRACK are HTTP methods which are used to debug web server connections.
It has been shown that servers supporting this method are subject to cross-site-scripting attacks, dubbed XST for Cross-Site-Tracing, when used in conjunction with various weaknesses in browsers.
An attacker may use this flaw to trick your legitimate web users to give him their credentials.

Vulnerability Detection Result
```
Solution:
Add the following lines for each virtual host in your configuration file :
    RewriteEngine on
    RewriteCond %{REQUEST_METHOD} ^(TRACE|TRACK)
    RewriteRule .* - [F]
See also http://httpd.apache.org/docs/current/de/mod/core.html#traceenable
```

Solution
Disable these methods.

Vulnerability Detection Method
Details:`http TRACE XSS attack`
OID:1.3.6.1.4.1.25623.1.0.11213
Version used: `$Revision: 3362 $`

References
```
CVE: CVE-2004-2320, CVE-2003-1567
BID:9506, 9561, 11604
Other:
  URL:http://www.kb.cert.org/vuls/id/867593
```

Medium (CVSS: 4.3)
NVT: PHP 'exif_read_data()' JPEG Image Processing Denial Of Service Vulnerability

Product detection result
```
cpe:/a:php:php:5.2.4
Detected by PHP Version Detection (Remote) (OID: 1.3.6.1.4.1.25623.1.0.800109)
```

Summary
PHP is prone to a denial-of-service vulnerability in its exif_read_data()' function.

... continues on next page ...

... continued from previous page ...

Vulnerability Detection Result
Installed version: 5.2.4
Fixed version: 5.2.10

Impact
Successful exploits may allow remote attackers to cause denial-of- service conditions in applications that use the vulnerable function.

Solution
Solution type: VendorFix
Updates are available. Please see the references for more information.

Affected Software/OS
Versions prior to PHP 5.2.10 are affected.

Vulnerability Detection Method
Details:PHP 'exif_read_data()' JPEG Image Processing Denial Of Service Vulnerability
OID:1.3.6.1.4.1.25623.1.0.100581
Version used: $Revision: 4503 $

Product Detection Result
Product: cpe:/a:php:php:5.2.4
Method: PHP Version Detection (Remote)
OID: 1.3.6.1.4.1.25623.1.0.800109)

References
CVE: CVE-2009-2687
BID:35440
Other:
URL:http://www.securityfocus.com/bid/35440
URL:http://www.php.net/releases/5_2_10.php
URL:http://www.php.net/
URL:http://lists.debian.org/debian-security-announce/2009/msg00263.html
URL:http://archives.neohapsis.com/archives/fulldisclosure/2009-08/0339.html
URL:http://support.avaya.com/css/P8/documents/100072880

Medium (CVSS: 5.0)
NVT: PHP 'ext/imap/php_imap.c' Use After Free Denial of Service Vulnerability

Product detection result
cpe:/a:php:php:5.2.4
Detected by PHP Version Detection (Remote) (OID: 1.3.6.1.4.1.25623.1.0.800109)

Summary

... continues on next page ...

... continued from previous page ...

This host is running PHP and is prone to denial of service vulnerability.

Vulnerability Detection Result
`Installed version: 5.2.4`
`Fixed version: 5.2.15/5.3.4`

Impact
Successful exploitation could allow local attackers to crash the affected application, denying service to legitimate users.
Impact Level: Application/Network

Solution
Solution type: VendorFix
Upgrade to PHP 5.2.15 or 5.3.4 For updates refer to http://www.php.net/downloads.php

Affected Software/OS
PHP version 5.2 before 5.2.15 and 5.3 before 5.3.4

Vulnerability Insight
The flaw is due to an erron in 'imap_do_open' function in the IMAP extension 'ext/imap/php_imap.c'.

Vulnerability Detection Method
Details:`PHP 'ext/imap/php_imap.c' Use After Free Denial of Service Vulnerability`
OID:1.3.6.1.4.1.25623.1.0.801583
Version used: `$Revision: 4502 $`

Product Detection Result
Product: `cpe:/a:php:php:5.2.4`
Method: `PHP Version Detection (Remote)`
OID: 1.3.6.1.4.1.25623.1.0.800109)

References
`CVE: CVE-2010-4150`
`BID:44980`
`Other:`
`URL:http://xforce.iss.net/xforce/xfdb/63390`
`URL:http://svn.php.net/viewvc?view=revision&revision=305032`

Medium (CVSS: 5.0)
NVT: PHP 'extract()' Function Security Bypass Vulnerability

Product detection result
`cpe:/a:php:php:5.2.4`
`Detected by PHP Version Detection (Remote) (OID: 1.3.6.1.4.1.25623.1.0.800109)`

... continues on next page ...

... continued from previous page ...

Summary
This host is running PHP and is prone to security bypass vulnerability.

Vulnerability Detection Result
`Installed version: 5.2.4`
`Fixed version: 5.2.15`

Impact
Successful exploitation could allows remote attackers to bypass intended access restrictions by modifying data structures that were not intended to depend on external input.
Impact Level: Network

Solution
Solution type: VendorFix
Upgrade to PHP version 5.2.15 or later For updates refer to http://www.php.net/downloads.php

Affected Software/OS
PHP version prior to 5.2.15

Vulnerability Insight
The flaw is due to error in 'extract()' function, it does not prevent use of the 'EXTR_OVERWRITE' parameter to overwrite the GLOBALS superglobal array.

Vulnerability Detection Method
Details:`PHP 'extract()' Function Security Bypass Vulnerability`
OID:1.3.6.1.4.1.25623.1.0.801731
Version used: `$Revision: 4502 $`

Product Detection Result
Product: `cpe:/a:php:php:5.2.4`
Method: `PHP Version Detection (Remote)`
OID: 1.3.6.1.4.1.25623.1.0.800109)

References
`CVE: CVE-2011-0752`
`Other:`
`URL:http://www.php.net/releases/5_2_15.php`
`URL:http://www.openwall.com/lists/oss-security/2010/12/13/4`

Medium (CVSS: 4.3)
NVT: PHP 'filter_var()' function Stack Consumption Vulnerability

Product detection result

... continues on next page ...

... continued from previous page ...

cpe:/a:php:php:5.2.4
Detected by PHP Version Detection (Remote) (OID: 1.3.6.1.4.1.25623.1.0.800109)

Summary
This host is running PHP and is prone to stack consumption vulnerability

Vulnerability Detection Result
Installed version: 5.2.4
Fixed version: 5.2.15/5.3.4

Impact
Successful exploitation could allows remote attackers to cause a denial of service (memory consumption and application crash) via a long e-mail address string.
Impact Level: Network

Solution
Solution type: VendorFix
Upgrade to PHP version 5.2.15/5.3.4 or later, For updates refer to http://www.php.net/downloads.php

Affected Software/OS
PHP version 5.2 through 5.2.14 and 5.3 through 5.3.3

Vulnerability Insight
- The flaw exists due to error in 'filter_var()' function, when FILTER_VALIDATE_EMAIL mode is used while processing the long e-mail address string. - A NULL pointer dereference vulnerability is exists in 'ZipArchive::getArchiveComment'.

Vulnerability Detection Method
Details:PHP 'filter_var()' function Stack Consumption Vulnerability
OID:1.3.6.1.4.1.25623.1.0.801547
Version used: $Revision: 4503 $

Product Detection Result
Product: cpe:/a:php:php:5.2.4
Method: PHP Version Detection (Remote)
OID: 1.3.6.1.4.1.25623.1.0.800109)

References
CVE: CVE-2010-3710, CVE-2010-3709
Other:
URL:http://bugs.php.net/bug.php?id=52929
URL:https://bugzilla.redhat.com/show_bug.cgi?id=646684
URL:http://www.securityfocus.com/archive/1/514562/30/150/threaded

Medium (CVSS: 5.0)
NVT: PHP 'imageRotate()' Memory Information Disclosure Vulnerability

Product detection result
cpe:/a:php:php:5.2.4
Detected by PHP Version Detection (Remote) (OID: 1.3.6.1.4.1.25623.1.0.800109)

Summary
The host is running PHP and is prone to Memory Information Disclosure vulnerability.

Vulnerability Detection Result
Installed version: 5.2.4
Fixed version: 5.2.9

Impact
Successful exploitation could let the attacker read the contents of arbitrary memory locations through a crafted value for an indexed image.
Impact Level: Application

Solution
Solution type: VendorFix
Upgrade to PHP version 5.2.9 or later. For updates refer to http://www.php.net/

Affected Software/OS
PHP version 5.x to 5.2.8 on all running platform.

Vulnerability Insight
The flaw is due to improper validation of bgd_color or clrBack argument in imageRotate function.

Vulnerability Detection Method
Details:PHP 'imageRotate()' Memory Information Disclosure Vulnerability
OID:1.3.6.1.4.1.25623.1.0.900186
Version used: $Revision: 4505 $

Product Detection Result
Product: cpe:/a:php:php:5.2.4
Method: PHP Version Detection (Remote)
OID: 1.3.6.1.4.1.25623.1.0.800109)

References
CVE: CVE-2008-5498
BID:33002
Other:
URL:http://securitytracker.com/alerts/2008/Dec/1021494.html
URL:http://downloads.securityfocus.com/vulnerabilities/exploits/33002.php
URL:http://downloads.securityfocus.com/vulnerabilities/exploits/33002-2.php

Medium (CVSS: 4.3)
NVT: PHP 'LibGD' Denial of Service Vulnerability

Product detection result
cpe:/a:php:php:5.2.4
Detected by PHP Version Detection (Remote) (OID: 1.3.6.1.4.1.25623.1.0.800109)

Summary
This host is installed with PHP and is prone to denial of service vulnerability.

Vulnerability Detection Result
Installed version: 5.2.4
Fixed version: 5.4.32/5.5.16/5.6.0

Impact
Successful exploitation will allow remote attackers to conduct denial of service attacks.
Impact Level: Application

Solution
Solution type: VendorFix
Upgrade to PHP version 5.4.32 or 5.5.16 or 5.6.0 or later. For updates refer to http://php.net

Affected Software/OS
PHP version 5.x through 5.4.26 and probably other versions.

Vulnerability Insight
The flaw is due to a NULL pointer dereference error in 'gdImageCreateFromXpm' function within LibGD.

Vulnerability Detection Method
Get the installed version of PHP with the help of detect NVT and check the version is vulnerable or not.
Details:PHP 'LibGD' Denial of Service Vulnerability
OID:1.3.6.1.4.1.25623.1.0.804292
Version used: $Revision: 4499 $

Product Detection Result
Product: cpe:/a:php:php:5.2.4
Method: PHP Version Detection (Remote)
OID: 1.3.6.1.4.1.25623.1.0.800109)

References
CVE: CVE-2014-2497
BID:66233
Other:
URL:https://bugs.php.net/bug.php?id=66901

Medium (CVSS: 6.4)
NVT: PHP 'make_http_soap_request' Information Disclosure Vulnerability (Linux)

Product detection result
cpe:/a:php:php:5.2.4
Detected by PHP Version Detection (Remote) (OID: 1.3.6.1.4.1.25623.1.0.800109)

Summary
This host is installed with PHP and is prone to denial of service or information disclosure vulnerabilities

Vulnerability Detection Result
Installed version: 5.2.4
Fixed version: 5.4.44

Impact
Successfully exploiting this issue allow remote attackers to obtain sensitive information from process memory or cause a denial of service.
Impact Level: Application

Solution
Solution type: VendorFix
Upgrade to PHP version 5.4.44, or 5.5.28, or 5.6.12, or 7.0.4, or later. For updates refer to http://www.php.net

Affected Software/OS
PHP versions prior to 5.4.44, 5.5.x before 5.5.28, 5.6.x before 5.6.12, and 7.x before 7.0.4 on Linux

Vulnerability Insight
The flaw is due an error in the 'make_http_soap_request' function in 'ext/soap/php_http.c' script.

Vulnerability Detection Method
Get the installed version with the help of detect NVT and check the version is vulnerable or not.
Details:PHP 'make_http_soap_request' Information Disclosure Vulnerability (Linux)
OID:1.3.6.1.4.1.25623.1.0.808666
Version used: $Revision: 5083 $

Product Detection Result
Product: cpe:/a:php:php:5.2.4
Method: PHP Version Detection (Remote)
OID: 1.3.6.1.4.1.25623.1.0.800109)

References
CVE: CVE-2016-3185

. . . continues on next page . . .

... continued from previous page ...

Other:
URL:http://www.php.net/ChangeLog-5.php
URL:http://www.php.net/ChangeLog-7.php

Medium (CVSS: 5.0)
NVT: PHP 'mb_strcut()' Function Information Disclosure Vulnerability

Product detection result
cpe:/a:php:php:5.2.4
Detected by PHP Version Detection (Remote) (OID: 1.3.6.1.4.1.25623.1.0.800109)

Summary
PHP is prone to an information-disclosure vulnerability.

Vulnerability Detection Result
Installed version: 5.2.4
Fixed version: 5.3.4

Impact
Attackers can exploit this issue to obtain sensitive information that may lead to further attacks.

Solution
Solution type: VendorFix
Updates are available please see the references for more information.

Affected Software/OS
Versions prior to PHP 5.3.4 are vulnerable.

Vulnerability Detection Method
Details:PHP 'mb_strcut()' Function Information Disclosure Vulnerability
OID:1.3.6.1.4.1.25623.1.0.100898
Version used: $Revision: 4503 $

Product Detection Result
Product: cpe:/a:php:php:5.2.4
Method: PHP Version Detection (Remote)
OID: 1.3.6.1.4.1.25623.1.0.800109)

References
CVE: CVE-2010-4156
BID:44727
Other:
URL:https://www.securityfocus.com/bid/44727
URL:http://permalink.gmane.org/gmane.comp.security.oss.general/3715
URL:http://www.php.net/

Medium (CVSS: 5.0)
NVT: PHP 'open_basedir' Security Bypass Vulnerability

Product detection result
cpe:/a:php:php:5.2.4
Detected by PHP Version Detection (Remote) (OID: 1.3.6.1.4.1.25623.1.0.800109)

Summary
This host is installed with PHP and is prone to security bypass vulnerability.

Vulnerability Detection Result
Installed version: 5.2.4
Fixed version: N/A

Impact
Successful exploitation will allow remote attackers to read arbitrary files.
Impact Level: Application

Solution
Solution type: WillNotFix
No solution or patch was made available for at least one year since disclosure of this vulnerability. Likely none will be provided anymore. General solution options are to upgrade to a newer release, disable respective features, remove the product or replace the product by another one.

Affected Software/OS
PHP versions 5.x.0 to 5.0.5, 5.1.0 to 5.1.6, 5.2.0 to 5.2.17, 5.3.0 to 5.3.27, 5.4.0 to 5.4.23 and 5.5.0 to 5.5.6.

Vulnerability Insight
The flaw is in libxml RSHUTDOWN function which allows to bypass open_basedir protection mechanism through stream_close method call.

Vulnerability Detection Method
Get the installed version of PHP with the help of detect NVT and check the version is vulnerable or not.
Details:PHP 'open_basedir' Security Bypass Vulnerability
OID:1.3.6.1.4.1.25623.1.0.804241
Version used: $Revision: 4499 $

Product Detection Result
Product: cpe:/a:php:php:5.2.4
Method: PHP Version Detection (Remote)
OID: 1.3.6.1.4.1.25623.1.0.800109)

References
CVE: CVE-2012-1171

. . . continues on next page . . .

... continued from previous page ...

Other:
URL:https://bugzilla.redhat.com/show_bug.cgi?id=802591

Medium (CVSS: 5.0)
NVT: PHP 'strrchr()' Function Information Disclosure Vulnerability

Product detection result
cpe:/a:php:php:5.2.4
Detected by PHP Version Detection (Remote) (OID: 1.3.6.1.4.1.25623.1.0.800109)

Summary
PHP is prone to an information-disclosure vulnerability.

Vulnerability Detection Result
Installed version: 5.2.4
Fixed version: 5.3.3

Impact
Attackers can exploit this issue to obtain sensitive information that may lead to further attacks.

Solution
Solution type: VendorFix
Updates are available please see the references for details.

Affected Software/OS
PHP 5 through 5.3.2 are vulnerable.

Vulnerability Detection Method
Details:PHP 'strrchr()' Function Information Disclosure Vulnerability
OID:1.3.6.1.4.1.25623.1.0.100695
Version used: $Revision: 4503 $

Product Detection Result
Product: cpe:/a:php:php:5.2.4
Method: PHP Version Detection (Remote)
OID: 1.3.6.1.4.1.25623.1.0.800109)

References
BID:41265
Other:
URL:https://www.securityfocus.com/bid/41265
URL:http://permalink.gmane.org/gmane.comp.security.oss.general/3109
URL:http://www.php.net/

Medium (CVSS: 5.0)
NVT: PHP 'unserialize()' Function Denial of Service Vulnerability

Product detection result
cpe:/a:php:php:5.2.4
Detected by PHP Version Detection (Remote) (OID: 1.3.6.1.4.1.25623.1.0.800109)

Summary
The host is running PHP and is prone to Denial of Service vulnerability.

Vulnerability Detection Result
Installed version: 5.2.4
Fixed version: N/A

Impact
Successful exploitation could allow attackers to execute arbitrary PHP code and cause denial of service.
Impact Level: Application

Solution
Solution type: WillNotFix
No solution or patch was made available for at least one year since disclosure of this vulnerability. Likely none will be provided anymore. General solution options are to upgrade to a newer release, disable respective features, remove the product or replace the product by another one.

Affected Software/OS
PHP 5.3.0 and prior on all running platform.

Vulnerability Insight
An error in 'unserialize()' function while processing malformed user supplied data containing a long serialized string passed via the '__wakeup()' or '__destruct()' methods.

Vulnerability Detection Method
Details:PHP 'unserialize()' Function Denial of Service Vulnerability
OID:1.3.6.1.4.1.25623.1.0.900993
Version used: $Revision: 4505 $

Product Detection Result
Product: cpe:/a:php:php:5.2.4
Method: PHP Version Detection (Remote)
OID: 1.3.6.1.4.1.25623.1.0.800109)

References
CVE: CVE-2009-4418
Other:
URL:http://www.security-database.com/detail.php?alert=CVE-2009-4418

... continues on next page ...

... continued from previous page ...

URL:http://www.suspekt.org/downloads/POC2009-ShockingNewsInPHPExploitation.pdf

Medium (CVSS: 6.8)
NVT: PHP 'xml_utf8_decode()' UTF-8 Input Validation Vulnerability

Product detection result
cpe:/a:php:php:5.2.4
Detected by PHP Version Detection (Remote) (OID: 1.3.6.1.4.1.25623.1.0.800109)

Summary
PHP is prone to a vulnerability because it fails to sufficiently sanitize user-supplied input.

Vulnerability Detection Result
Installed version: 5.2.4
Fixed version: 5.3.4

Impact
Exploiting this issue can allow attackers to provide unexpected input and possibly bypass input-validation protection mechanisms. This can aid in further attacks that may utilize crafted user-supplied input.

Solution
Solution type: VendorFix
Updates are available. Please see the references for more information.

Affected Software/OS
Versions prior to PHP 5.3.4 are vulnerable.

Vulnerability Detection Method
Details:PHP 'xml_utf8_decode()' UTF-8 Input Validation Vulnerability
OID:1.3.6.1.4.1.25623.1.0.100901
Version used: $Revision: 4503 $

Product Detection Result
Product: cpe:/a:php:php:5.2.4
Method: PHP Version Detection (Remote)
OID: 1.3.6.1.4.1.25623.1.0.800109)

References
CVE: CVE-2010-3870
BID:44605
Other:
URL:https://www.securityfocus.com/bid/44605

... continues on next page ...

... continued from previous page ...

URL:http://bugs.php.net/bug.php?id=48230
URL:http://bugs.php.net/bug.php?id=49687
URL:http://svn.php.net/viewvc?view=revision&revision=304959
URL:http://www.php.net/
URL:http://comments.gmane.org/gmane.comp.security.oss.general/3684
URL:http://www.mandriva.com/en/security/advisories?name=MDVSA-2010:224

Medium (CVSS: 5.0)
NVT: PHP 'zend_strtod()' Function Floating-Point Value Denial of Service Vulnerability

Product detection result
cpe:/a:php:php:5.2.4
Detected by PHP Version Detection (Remote) (OID: 1.3.6.1.4.1.25623.1.0.800109)

Summary
PHP is prone to a remote denial-of-service vulnerability.

Vulnerability Detection Result
Installed version: 5.2.4
Fixed version: 5.2.17/5.3.5

Impact
Successful attacks will cause applications written in PHP to hang, creating a denial-of-service condition.

Solution
Solution type: VendorFix
Updates are available. Please see the references for more details.

Affected Software/OS
PHP 5.3.3 is vulnerable other versions may also be affected.

Vulnerability Insight
The vulnerability is due to the Floating-Point Value that exist in zend_strtod function

Vulnerability Detection Method
Details:PHP 'zend_strtod()' Function Floating-Point Value Denial of Service Vulnerabili.
↪..
OID:1.3.6.1.4.1.25623.1.0.103020
Version used: $Revision: 4502 $

Product Detection Result
Product: cpe:/a:php:php:5.2.4
Method: PHP Version Detection (Remote)
OID: 1.3.6.1.4.1.25623.1.0.800109)

... continues on next page ...

... continued from previous page ...

References

```
CVE: CVE-2010-4645
BID:45668
Other:
  URL:https://www.securityfocus.com/bid/45668
   URL:http://bugs.php.net/bug.php?id=53632
   URL:http://svn.php.net/viewvc/?view=revision&revision=307119
   URL:http://svn.php.net/viewvc?view=revision&revision=307095
   URL:http://www.exploringbinary.com/php-hangs-on-numeric-value-2-2250738585072
↪011e-308/
   URL:http://www.php.net/
```

Medium (CVSS: 5.0)
NVT: PHP 5.2.8 and Prior Versions Multiple Vulnerabilities

Product detection result

```
cpe:/a:php:php:5.2.4
Detected by PHP Version Detection (Remote) (OID: 1.3.6.1.4.1.25623.1.0.800109)
```

Summary

PHP is prone to multiple security vulnerabilities.

Vulnerability Detection Result

```
Installed version: 5.2.4
Fixed version:     5.2.9
```

Impact

Successful exploits could allow an attacker to cause a denial-of-service condition. An unspecified issue with an unknown impact was also reported.

Solution

Solution type: VendorFix

The vendor has released PHP 5.2.9 to address these issues. Please see http://www.php.net/ fore more information.

Affected Software/OS

These issues affect PHP 5.2.8 and prior versions.

Vulnerability Detection Method

Details:`PHP 5.2.8 and Prior Versions Multiple Vulnerabilities`
OID:1.3.6.1.4.1.25623.1.0.100146
Version used: `$Revision: 4505 $`

Product Detection Result

... continues on next page ...

... continued from previous page ...

Product: cpe:/a:php:php:5.2.4
Method: PHP Version Detection (Remote)
OID: 1.3.6.1.4.1.25623.1.0.800109)

References
CVE: CVE-2009-1271
BID:33927
Other:
URL:http://www.securityfocus.com/bid/33927

Medium (CVSS: 5.0)
NVT: PHP CDF File Parsing Denial of Service Vulnerabilities - 01 - Jun14

Product detection result
cpe:/a:php:php:5.2.4
Detected by PHP Version Detection (Remote) (OID: 1.3.6.1.4.1.25623.1.0.800109)

Summary
This host is installed with PHP and is prone to denial of service vulnerabilities.

Vulnerability Detection Result
Installed version: 5.2.4
Fixed version: 5.4.29/5.5.13

Impact
Successful exploitation will allow remote attackers to conduct denial of service attacks.
Impact Level: Application

Solution
Solution type: VendorFix
Upgrade to PHP version 5.4.29 or 5.5.13 or later. For updates refer to http://php.net

Affected Software/OS
PHP version 5.x before 5.4.29 and 5.5.x before 5.5.13

Vulnerability Insight
The flaw is due to - An error due to an infinite loop within the 'unpack_summary_info' function in src/cdf.c script. - An error within the 'cdf_read_property_info' function in src/cdf.c script.

Vulnerability Detection Method
Get the installed version of PHP with the help of detect NVT and check the version is vulnerable or not.
Details:PHP CDF File Parsing Denial of Service Vulnerabilities - 01 - Jun14
OID:1.3.6.1.4.1.25623.1.0.804639

... continues on next page ...

... continued from previous page ...

Version used: $Revision: 4499 $

Product Detection Result
Product: cpe:/a:php:php:5.2.4
Method: PHP Version Detection (Remote)
OID: 1.3.6.1.4.1.25623.1.0.800109)

References
CVE: CVE-2014-0237, CVE-2014-0238
BID:67759, 67765
Other:
URL:http://www.php.net/ChangeLog-5.php
URL:http://secunia.com/advisories/58804
URL:https://www.hkcert.org/my_url/en/alert/14060401

Medium (CVSS: 4.3)
NVT: PHP Cross-Site Scripting Vulnerability - Aug16 (Linux)

Product detection result
cpe:/a:php:php:5.2.4
Detected by PHP Version Detection (Remote) (OID: 1.3.6.1.4.1.25623.1.0.800109)

Summary
This host is installed with PHP and is prone to cross-site scripting (XSS) vulnerability.

Vulnerability Detection Result
Installed version: 5.2.4
Fixed version: 5.4.38

Impact
Successfully exploiting this issue allows remote attackers to conduct cross-site scripting (XSS) attacks against Internet Explorer by leveraging '%0A%20' or '%0D%0A%20' mishandling in the header function.
Impact Level: Application

Solution
Solution type: VendorFix
Upgrade to PHP version 5.4.38, or 5.5.22, or 5.6.6, or later. For updates refer to http://www.php.net

Affected Software/OS
PHP versions before 5.4.38, 5.5.x before 5.5.22, and 5.6.x before 5.6.6 on Linux

Vulnerability Insight

... continues on next page ...

... continued from previous page ...

The flaw is due to the 'sapi_header_op' function in 'main/SAPI.c' script supports deprecated line folding without considering browser compatibility.

Vulnerability Detection Method
Get the installed version with the help of detect NVT and check the version is vulnerable or not.
Details:`PHP Cross-Site Scripting Vulnerability - Aug16 (Linux)`
OID:1.3.6.1.4.1.25623.1.0.809137
Version used: `$Revision: 5083 $`

Product Detection Result
Product: `cpe:/a:php:php:5.2.4`
Method: `PHP Version Detection (Remote)`
OID: 1.3.6.1.4.1.25623.1.0.800109)

References
`CVE: CVE-2015-8935`
`BID:92356`
`Other:`
`URL:https://bugs.php.net/bug.php?id=68978`

Medium (CVSS: 6.8)
NVT: PHP Denial of Service And Unspecified Vulnerabilities - 02 - Jul16 (Linux)

Product detection result
`cpe:/a:php:php:5.2.4`
`Detected by PHP Version Detection (Remote) (OID: 1.3.6.1.4.1.25623.1.0.800109)`

Summary
This host is installed with PHP and is prone to denial of service and unspecified Vulnerabilities

Vulnerability Detection Result
`Installed version: 5.2.4`
`Fixed version: 5.6.18`

Impact
Successfully exploiting this issue allow remote attackers to cause a denial of service (heap memory corruption) or possibly have unspecified other impact.
Impact Level: Application

Solution
Solution type: VendorFix
Upgrade to PHP version 5.6.18, or 7.0.3, or later. For updates refer to http://www.php.net

Affected Software/OS

... continues on next page ...

... continued from previous page ...

PHP versions prior to 5.6.18 and 7.x before 7.0.3 on Linux

Vulnerability Insight
The flaw is due an improper handling of zero-size './/@LongLink' files by 'phar_make_dirstream' function in ext/phar/dirstream.c script.

Vulnerability Detection Method
Get the installed version with the help of detect NVT and check the version is vulnerable or not.
Details:`PHP Denial of Service And Unspecified Vulnerabilities - 02 - Jul16 (Linux)`
OID:1.3.6.1.4.1.25623.1.0.808609
Version used: `$Revision: 5083 $`

Product Detection Result
Product: `cpe:/a:php:php:5.2.4`
Method: `PHP Version Detection (Remote)`
OID: 1.3.6.1.4.1.25623.1.0.800109)

References
`CVE: CVE-2016-4343`
`BID:89179`
`Other:`
`URL:http://www.php.net/ChangeLog-5.php`
`URL:http://www.openwall.com/lists/oss-security/2016/04/28/2`

Medium (CVSS: 6.4)
NVT: PHP Denial of Service Vulnerability - 02 - Aug16 (Linux)

Product detection result
`cpe:/a:php:php:5.2.4`
`Detected by PHP Version Detection (Remote) (OID: 1.3.6.1.4.1.25623.1.0.800109)`

Summary
This host is installed with PHP and is prone to denial of service vulnerability.

Vulnerability Detection Result
`Installed version: 5.2.4`
`Fixed version: 5.5.31`

Impact
Successfully exploiting this issue allow attackers to obtain sensitive information from process memory or cause a denial of service (out-of-bounds read and buffer overflow) via a long string.
Impact Level: Application

Solution

... continues on next page ...

... continued from previous page ...

Solution type: VendorFix
Upgrade to PHP version 5.5.31, or 5.6.17, or 7.0.2, or later. For updates refer to http://www.php.net

Affected Software/OS
PHP versions before 5.5.31, 5.6.x before 5.6.17, and 7.x before 7.0.2 on Linux.

Vulnerability Insight
The flaw is due to the 'sapi/fpm/fpm/fpm_log.c' script misinterprets the semantics of the snprintf return value.

Vulnerability Detection Method
Get the installed version with the help of detect NVT and check the version is vulnerable or not.
Details:`PHP Denial of Service Vulnerability - 02 - Aug16 (Linux)`
OID:1.3.6.1.4.1.25623.1.0.809139
Version used: `$Revision: 5083 $`

Product Detection Result
Product: `cpe:/a:php:php:5.2.4`
Method: `PHP Version Detection (Remote)`
OID: 1.3.6.1.4.1.25623.1.0.800109)

References
`CVE: CVE-2016-5114`
`BID:81808`
`Other:`
`URL:http://www.php.net/ChangeLog-5.php`

Medium (CVSS: 5.0)
NVT: PHP Denial Of Service Vulnerability - April09

Product detection result
`cpe:/a:php:php:5.2.4`
`Detected by PHP Version Detection (Remote) (OID: 1.3.6.1.4.1.25623.1.0.800109)`

Summary
The host is installed with PHP and is prone to Denial of Service vulnerability.

Vulnerability Detection Result
`Installed version: 5.2.4`
`Fixed version: 5.2.10`

Impact
Successful exploitation could result in denial of service condition.

... continues on next page ...

... continued from previous page ...

Impact Level: Application

Solution
Solution type: VendorFix
Upgrade to PHP version 5.2.9 or above, http://www.php.net/downloads.php
Workaround: For workaround refer below link, http://cvs.php.net/viewvc.cgi/php-src/ext/json/JSON_parser.c?r1=1.1.2.14&r2=1.1.2.15

Affected Software/OS
PHP version prior to 5.2.9

Vulnerability Insight
Improper handling of .zip file while doing extraction via php_zip_make_relative_path function in php_zip.c file.

Vulnerability Detection Method
Details:`PHP Denial Of Service Vulnerability - April09`
OID:1.3.6.1.4.1.25623.1.0.800393
Version used: `$Revision: 4504 $`

Product Detection Result
Product: `cpe:/a:php:php:5.2.4`
Method: `PHP Version Detection (Remote)`
OID: 1.3.6.1.4.1.25623.1.0.800109)

References
`CVE: CVE-2009-1272`
`Other:`
`URL:http://www.php.net/releases/5_2_9.php`
`URL:http://www.openwall.com/lists/oss-security/2009/04/01/9`

Medium (CVSS: 5.0)
NVT: PHP FastCGI Module File Extension Denial Of Service Vulnerabilities

Product detection result
`cpe:/a:php:php:5.2.4`
`Detected by PHP Version Detection (Remote) (OID: 1.3.6.1.4.1.25623.1.0.800109)`

Summary
PHP is prone to a denial-of-service vulnerability because the application fails to handle certain file requests.

Vulnerability Detection Result
`Installed version: 5.2.4`

... continues on next page ...

... continued from previous page ...

Fixed version: 5.2.8

Impact
Attackers can exploit this issue to crash the affected application, denying service to legitimate users.

Solution
Solution type: VendorFix
Updates are available. Please see the references for more information.

Affected Software/OS
PHP 4.4 prior to 4.4.9 and PHP 5.2 through 5.2.6 are vulnerable.

Vulnerability Detection Method
Details:PHP FastCGI Module File Extension Denial Of Service Vulnerabilities
OID:1.3.6.1.4.1.25623.1.0.100582
Version used: $Revision: 4503 $

Product Detection Result
Product: cpe:/a:php:php:5.2.4
Method: PHP Version Detection (Remote)
OID: 1.3.6.1.4.1.25623.1.0.800109)

References
CVE: CVE-2008-3660
BID:31612
Other:
URL:http://www.securityfocus.com/bid/31612
URL:http://www.openwall.com/lists/oss-security/2008/08/08/2
URL:http://www.php.net/ChangeLog-5.php#5.2.8
URL:http://www.php.net
URL:http://support.avaya.com/elmodocs2/security/ASA-2009-161.htm

Medium (CVSS: 5.0)
NVT: PHP Fileinfo Component Denial of Service Vulnerability (Linux)

Product detection result
cpe:/a:php:php:5.2.4
Detected by PHP Version Detection (Remote) (OID: 1.3.6.1.4.1.25623.1.0.800109)

Summary
This host is installed with PHP and is prone to denial of service vulnerability.

Vulnerability Detection Result

... continues on next page ...

... continued from previous page ...

Installed version: 5.2.4
Fixed version: 5.6.0

Impact
Successfully exploiting this issue allow remote attackers to cause a denial of service.
Impact Level: Application

Solution
Solution type: VendorFix
Upgrade to PHP version 5.6.0 For updates refer to http://www.php.net

Affected Software/OS
PHP versions prior to 5.6.0 on Linux

Vulnerability Insight
The flaw is due an improper validation of input to zero root_storage value in a CDF file.

Vulnerability Detection Method
Get the installed version with the help of detect NVT and check the version is vulnerable or not.
Details:PHP Fileinfo Component Denial of Service Vulnerability (Linux)
OID:1.3.6.1.4.1.25623.1.0.808669
Version used: $Revision: 5083 $

Product Detection Result
Product: cpe:/a:php:php:5.2.4
Method: PHP Version Detection (Remote)
OID: 1.3.6.1.4.1.25623.1.0.800109)

References
CVE: CVE-2014-0236
BID:90957
Other:
URL:http://www.php.net/ChangeLog-5.php

Medium (CVSS: 5.1)
NVT: PHP Man-in-the-Middle Attack Vulnerability - Jul16 (Linux)

Product detection result
cpe:/a:php:php:5.2.4
Detected by PHP Version Detection (Remote) (OID: 1.3.6.1.4.1.25623.1.0.800109)

Summary
This host is installed with PHP and is prone to Man-in-the-middle attack vulnerability.

... continues on next page ...

... continued from previous page ...

Vulnerability Detection Result
Installed version: 5.2.4
Fixed version: 5.6.24/7.0.9

Impact
Successfully exploiting this issue may allow remote, unauthenticated to conduct MITM attacks on internal server subrequests or direct the server to initiate connections to arbitrary hosts or to cause a denial of service.
Impact Level: Application

Solution
Solution type: VendorFix
Update to PHP version 5.6.24 or 7.0.19. For updates refer to http://www.php.net

Affected Software/OS
PHP versions 5.x through 5.6.23 and 7.0.x through 7.0.8 on Linux

Vulnerability Insight
The web servers running in a CGI or CGI-like context may assign client request Proxy header values to internal HTTP_PROXY environment variables and 'HTTP_PROXY' is improperly trusted by some PHP libraries and applications and flaw exist in the gdImageCropThreshold function in 'gd_crop.c' in the GD Graphics Library.

Vulnerability Detection Method
Get the installed version with the help of detect NVT and check the version is vulnerable or not.
Details:PHP Man-in-the-Middle Attack Vulnerability - Jul16 (Linux)
OID:1.3.6.1.4.1.25623.1.0.808628
Version used: $Revision: 5083 $

Product Detection Result
Product: cpe:/a:php:php:5.2.4
Method: PHP Version Detection (Remote)
OID: 1.3.6.1.4.1.25623.1.0.800109)

References
CVE: CVE-2016-5385, CVE-2016-6128
BID:91821, 91509
Other:
URL:http://www.php.net/ChangeLog-5.php
URL:http://www.php.net/ChangeLog-7.php
URL:http://www.kb.cert.org/vuls/id/797896
URL:https://bugs.php.net/bug.php?id=72573
URL:https://bugs.php.net/bug.php?id=72494

Medium (CVSS: 5.0)
NVT: PHP Multiple Denial of Service Vulnerabilities (Linux)

Product detection result
cpe:/a:php:php:5.2.4
Detected by PHP Version Detection (Remote) (OID: 1.3.6.1.4.1.25623.1.0.800109)

Summary
This host is installed with PHP and is prone to multiple denial of service vulnerabilities.

Vulnerability Detection Result
Installed version: 5.2.4
Fixed version: 5.6.12

Impact
Successfully exploiting this issue allow remote attackers to cause a denial of service (application crash or memory consuption).
Impact Level: Application

Solution
Solution type: VendorFix
Upgrade to PHP version 5.6.12 or later. For updates refer to http://www.php.net

Affected Software/OS
PHP versions prior to 5.6.12 on Linux

Vulnerability Insight
Multiple flaws are due to - An improper handling of driver behavior for SQL_WVARCHAR columns in the 'odbc_bindcols function' in 'ext/odbc/php_odbc.c' script. - The 'gdImageScaleTwoPass' function in gd_interpolation.c script in the GD Graphics Library uses inconsistent allocate and free approaches.

Vulnerability Detection Method
Get the installed version with the help of detect NVT and check the version is vulnerable or not.
Details:PHP Multiple Denial of Service Vulnerabilities (Linux)
OID:1.3.6.1.4.1.25623.1.0.808611
Version used: $Revision: 5083 $

Product Detection Result
Product: cpe:/a:php:php:5.2.4
Method: PHP Version Detection (Remote)
OID: 1.3.6.1.4.1.25623.1.0.800109)

References
CVE: CVE-2015-8877, CVE-2015-8879, CVE-2015-8874
BID:90866, 90842, 90714

... continues on next page ...

... continued from previous page ...

```
Other:
  URL:http://www.php.net/ChangeLog-5.php
```

Medium (CVSS: 6.8)
NVT: PHP Multiple Denial of Service Vulnerabilities - 01 - Dec15 (Linux)

Product detection result
`cpe:/a:php:php:5.2.4`
`Detected by PHP Version Detection (Remote) (OID: 1.3.6.1.4.1.25623.1.0.800109)`

Summary
This host is installed with PHP and is prone to multiple denial of service vulnerabilities.

Vulnerability Detection Result
`Installed Version: 5.2.4`
`Fixed Version: 5.5.30`

Impact
Successfully exploiting this issue allow remote attackers to cause a denial of service (NULL pointer dereference and application crash).
Impact Level: Application

Solution
Solution type: VendorFix
Upgrade to PHP 5.5.30 or 5.6.14 or later. For updates refer to http://www.php.net

Affected Software/OS
PHP versions before 5.5.30 and 5.6.x before 5.6.14

Vulnerability Insight
Multiple flaws are due to, - An Off-by-one error in the 'phar_parse_zipfile' function within ext/phar/zip.c script. - An error in the 'phar_get_entry_data' function in ext/phar/util.c script.

Vulnerability Detection Method
Get the installed version with the help of detect NVT and check the version is vulnerable or not.
Details:`PHP Multiple Denial of Service Vulnerabilities - 01 - Dec15 (Linux)`
OID:1.3.6.1.4.1.25623.1.0.806649
Version used: `$Revision: 5082 $`

Product Detection Result
Product: `cpe:/a:php:php:5.2.4`
Method: `PHP Version Detection (Remote)`
OID: 1.3.6.1.4.1.25623.1.0.800109)

... continues on next page ...

... continued from previous page ...

References
CVE: CVE-2015-7804, CVE-2015-7803
BID:76959
Other:
URL:http://www.php.net/ChangeLog-5.php
URL:https://bugs.php.net/bug.php?id=70433
URL:http://www.openwall.com/lists/oss-security/2015/10/05/8

Medium (CVSS: 5.0)
NVT: PHP Multiple Denial of Service Vulnerabilities - 01 - Jan17 (Linux)

Product detection result
cpe:/a:php:php:5.2.4
Detected by PHP Version Detection (Remote) (OID: 1.3.6.1.4.1.25623.1.0.800109)

Summary
This host is installed with PHP and is prone to multiple denial of service vulnerabilities.

Vulnerability Detection Result
Installed version: 5.2.4
Fixed version: 5.6.30

Impact
Successfully exploiting this issue allow remote attackers to cause a denial of service (buffer over-read or application crash).
Impact Level: Application

Solution
Solution type: VendorFix
Upgrade to PHP version 5.6.30, 7.0.15, 7.1.1 or later. For updates refer to http://www.php.net

Affected Software/OS
PHP versions before 5.6.30, 7.0.x before 7.0.15, and 7.1.x before 7.1.1.

Vulnerability Insight
Multiple flaws are due to - The exif_convert_any_to_int function in ext/exif/exif.c tries to divide the minimum representable negative integer by -1.
- A mishandled serialized data in a finish_nested_data call within the object_common1 function in ext/standard/var_unserializer.c.

Vulnerability Detection Method
Get the installed version with the help of the detect NVT and check if the version is vulnerable or not.
Details:PHP Multiple Denial of Service Vulnerabilities - 01 - Jan17 (Linux)

... continues on next page ...

... continued from previous page ...

OID:1.3.6.1.4.1.25623.1.0.108052
Version used: $Revision: 5099 $

Product Detection Result
Product: cpe:/a:php:php:5.2.4
Method: PHP Version Detection (Remote)
OID: 1.3.6.1.4.1.25623.1.0.800109)

References
CVE: CVE-2016-10161, CVE-2016-10158
Other:
URL:http://www.php.net/ChangeLog-5.php
URL:http://www.php.net/ChangeLog-7.php

Medium (CVSS: 6.4)
NVT: PHP Multiple Information Disclosure Vulnerabilities

Product detection result
cpe:/a:php:php:5.2.4
Detected by PHP Version Detection (Remote) (OID: 1.3.6.1.4.1.25623.1.0.800109)

Summary
This host is running PHP and is prone to multiple information disclosure vulnerabilities.

Vulnerability Detection Result
Installed version: 5.2.4
Fixed version: 5.2.14/5.3.3

Impact
Successful exploitation could allow local attackers to bypass certain security restrictions and to obtain sensitive information.
Impact Level: Network

Solution
Solution type: VendorFix
Upgrade to PHP version 5.2.14/5.3.3 or later For updates refer to http://www.php.net/downloads.php

Affected Software/OS
PHP version 5.2 through 5.2.13 and 5.3 through 5.3.2

Vulnerability Insight

... continues on next page ...

... continued from previous page ...

Multiple flaws are due to: - Error in 'trim()', 'ltrim()','rtrim()' and 'substr_replace()' functions, which causes a userspace interruption of an internal function within the call time pass by reference feature. - Error in 'parse_str()', 'preg_match()', 'unpack()' and 'pack()' functions, 'ZEND_FETCH_RW()', 'ZEND_CONCAT()', and 'ZEND_ASSIGN_CONCAT()' opcodes, and the 'ArrayObject::uasort' method, trigger memory corruption by causing a userspace interruption of an internal function or handler.

Vulnerability Detection Method
Details:PHP Multiple Information Disclosure Vulnerabilities
OID:1.3.6.1.4.1.25623.1.0.801359
Version used: $Revision: 4503 $

Product Detection Result
Product: cpe:/a:php:php:5.2.4
Method: PHP Version Detection (Remote)
OID: 1.3.6.1.4.1.25623.1.0.800109)

References
CVE: CVE-2010-2190, CVE-2010-2191
Other:
URL:http://www.php-security.org/2010/05/30/mops-2010-048-php-substr_replace-in
↪terruption-information-leak-vulnerability/index.html
URL:http://www.php-security.org/2010/05/30/mops-2010-047-php-trimltrimrtrim-i
↪nterruption-information-leak-vulnerability/index.html

Medium (CVSS: 5.0)
NVT: PHP Multiple Security Bypass Vulnerabilities

Product detection result
cpe:/a:php:php:5.2.4
Detected by PHP Version Detection (Remote) (OID: 1.3.6.1.4.1.25623.1.0.800109)

Summary
This host is running PHP and is prone to multiple security bypass vulnerability.

Vulnerability Detection Result
Installed version: 5.2.4
Fixed version: 5.3.4

Impact
Successful exploitation could allow remote attackers to trigger an incomplete output array, and possibly bypass spam detection or have unspecified other impact.
Impact Level: Application/Network

Solution

... continues on next page ...

... continued from previous page ...

Solution type: VendorFix
Upgrade to PHP 5.3.4 or later For updates refer to http://www.php.net/downloads.php

Affected Software/OS
PHP version prior to 5.3.4

Vulnerability Insight
The flaws are caused to: - An error in handling pathname which accepts the '?' character in a pathname. - An error in 'iconv_mime_decode_headers()' function in the 'Iconv' extension. - 'SplFileInfo::getType' function in the Standard PHP Library (SPL) extension, does not properly detect symbolic links in windows. - Integer overflow in the 'mt_rand' function. - Race condition in the 'PCNTL extension', when a user-defined signal handler exists.

Vulnerability Detection Method
Details:`PHP Multiple Security Bypass Vulnerabilities`
OID:1.3.6.1.4.1.25623.1.0.801585
Version used: `$Revision: 4502 $`

Product Detection Result
Product: `cpe:/a:php:php:5.2.4`
Method: `PHP Version Detection (Remote)`
OID: 1.3.6.1.4.1.25623.1.0.800109)

References
`CVE: CVE-2006-7243, CVE-2010-4699, CVE-2011-0754, CVE-2011-0753, CVE-2011-0755`
`Other:`
`URL:http://www.php.net/ChangeLog-5.php`
`URL:http://www.php.net/releases/5_3_4.php`
`URL:http://openwall.com/lists/oss-security/2010/12/09/9`
`URL:http://svn.php.net/viewvc?view=revision&revision=305507`

Medium (CVSS: 6.4)
NVT: PHP Out of Bounds Read Memory Corruption Vulnerability - 01 - Mar16 (Linux)

Product detection result
`cpe:/a:php:php:5.2.4`
`Detected by PHP Version Detection (Remote) (OID: 1.3.6.1.4.1.25623.1.0.800109)`

Summary
This host is installed with PHP and is prone to out-of-bounds read memory corruption vulnerability.

Vulnerability Detection Result
`Installed version: 5.2.4`

... continues on next page ...

... continued from previous page ...

Fixed version: 5.5.31

Impact
Successfully exploiting this issue allow remote attackers to obtain sensitive information or cause a denial-of-service condition.
Impact Level: Application

Solution
Solution type: VendorFix
Upgrade to PHP version 5.5.31, or 5.6.17 or 7.0.2 or later. For updates refer to http://www.php.net

Affected Software/OS
PHP versions before 5.5.31, 5.6.x before 5.6.17, and 7.x before 7.0.2 on Linux

Vulnerability Insight
The flaw is due to memory corruption vulnerability via a large 'bgd_color' argument to the 'imagerotate' function in 'ext/gd/libgd/gd_interpolation.c' script.

Vulnerability Detection Method
Get the installed version with the help of detect NVT and check the version is vulnerable or not.
Details:PHP Out of Bounds Read Memory Corruption Vulnerability - 01 - Mar16 (Linux)
OID:1.3.6.1.4.1.25623.1.0.807504
Version used: $Revision: 5083 $

Product Detection Result
Product: cpe:/a:php:php:5.2.4
Method: PHP Version Detection (Remote)
OID: 1.3.6.1.4.1.25623.1.0.800109)

References
CVE: CVE-2016-1903
BID:79916
Other:
URL:https://bugs.php.net/bug.php?id=70976
URL:http://www.openwall.com/lists/oss-security/2016/01/14/8

Medium (CVSS: 4.3)
NVT: PHP SOAP Parser Multiple Information Disclosure Vulnerabilities

Product detection result
cpe:/a:php:php:5.2.4
Detected by PHP Version Detection (Remote) (OID: 1.3.6.1.4.1.25623.1.0.800109)

... continues on next page ...

... continued from previous page ...

Summary
This host is installed with PHP and is prone to multiple information disclosure vulnerabilities.

Vulnerability Detection Result
`Installed version: 5.2.4`
`Fixed version: 5.3.22/5.4.12`

Impact
Successful exploitation will allow remote attackers to obtain sensitive information.
Impact Level: Application

Solution
Solution type: VendorFix
Upgrade to PHP 5.3.22 or 5.4.12 or later, http://www.php.net/downloads.php

Affected Software/OS
PHP version before 5.3.22 and 5.4.x before 5.4.12

Vulnerability Insight
Flaws are due to the way SOAP parser process certain SOAP objects (due to allowed expansion of XML external entities during SOAP WSDL files parsing).

Vulnerability Detection Method
Get the installed version of PHP with the help of detect NVT and check the version is vulnerable or not.
Details:`PHP SOAP Parser Multiple Information Disclosure Vulnerabilities`
OID:1.3.6.1.4.1.25623.1.0.803764
Version used: `$Revision: 5351 $`

Product Detection Result
Product: `cpe:/a:php:php:5.2.4`
Method: `PHP Version Detection (Remote)`
OID: 1.3.6.1.4.1.25623.1.0.800109)

References
`CVE: CVE-2013-1824`
`BID:62373`
`Other:`
`URL:http://php.net/ChangeLog-5.php`
`URL:http://git.php.net/?p=php-src.git;a=commit;h=afe98b7829d50806559acac9b530`
`↪acb8283c3bf4`

Medium (CVSS: 6.8)
NVT: PHP Version 5.2 < 5.2.15 Multiple Vulnerabilities

... continues on next page ...

... continued from previous page ...

Product detection result
cpe:/a:php:php:5.2.4
Detected by PHP Version Detection (Remote) (OID: 1.3.6.1.4.1.25623.1.0.800109)

Summary
PHP 5.2 < 5.2.15 suffers from multiple vulnerabilities such as a crash in the zip extract method, NULL pointer dereference and stack-based buffer overflow.

Vulnerability Detection Result
Installed version: 5.2.4
Fixed version: 5.2.15

Solution
Solution type: VendorFix
Upgrade to PHP version 5.2.15 or later.

Vulnerability Detection Method
Details:PHP Version 5.2 < 5.2.15 Multiple Vulnerabilities
OID:1.3.6.1.4.1.25623.1.0.110066
Version used: $Revision: 4506 $

Product Detection Result
Product: cpe:/a:php:php:5.2.4
Method: PHP Version Detection (Remote)
OID: 1.3.6.1.4.1.25623.1.0.800109)

References
CVE: CVE-2010-3436, CVE-2010-3709, CVE-2010-4150, CVE-2010-4697, CVE-2010-4698,
↪CVE-2011-0752
BID:44718, 44723, 45335, 45952, 46448

Medium (CVSS: 5.0)
NVT: PHP Version < 5.2.9 Multiple Vulnerabilities

Product detection result
cpe:/a:php:php:5.2.4
Detected by PHP Version Detection (Remote) (OID: 1.3.6.1.4.1.25623.1.0.800109)

Summary
PHP version smaller than 5.2.9 suffers from multiple vulnerabilities.

Vulnerability Detection Result
Installed version: 5.2.4

... continues on next page ...

... continued from previous page ...

Fixed version: 5.2.9

Solution
Solution type: VendorFix
Update PHP to version 5.2.9 or later.

Vulnerability Detection Method
Details:PHP Version < 5.2.9 Multiple Vulnerabilities
OID:1.3.6.1.4.1.25623.1.0.110187
Version used: $Revision: 4506 $

Product Detection Result
Product: cpe:/a:php:php:5.2.4
Method: PHP Version Detection (Remote)
OID: 1.3.6.1.4.1.25623.1.0.800109)

References
CVE: CVE-2008-5498, CVE-2009-1271, CVE-2009-1272
BID:33002, 33927

Medium (CVSS: 6.8)
NVT: PHP Version < 5.3.4 Multiple Vulnerabilities

Product detection result
cpe:/a:php:php:5.2.4
Detected by PHP Version Detection (Remote) (OID: 1.3.6.1.4.1.25623.1.0.800109)

Summary
PHP version smaller than 5.3.4 suffers from multiple vulnerabilities.

Vulnerability Detection Result
Installed version: 5.2.4
Fixed version: 5.3.4

Solution
Solution type: VendorFix
Update PHP to version 5.3.4 or later.

Vulnerability Detection Method
Details:PHP Version < 5.3.4 Multiple Vulnerabilities
OID:1.3.6.1.4.1.25623.1.0.110181
Version used: $Revision: 4506 $

Product Detection Result

... continues on next page ...

... continued from previous page ...

Product: cpe:/a:php:php:5.2.4
Method: PHP Version Detection (Remote)
OID: 1.3.6.1.4.1.25623.1.0.800109)

References
CVE: CVE-2006-7243, CVE-2010-2094, CVE-2010-2950, CVE-2010-3436, CVE-2010-3709, ↪CVE-2010-3710, CVE-2010-3870, CVE-2010-4150, CVE-2010-4156, CVE-2010-4409, CVE ↪-2010-4697, CVE-2010-4698, CVE-2010-4699, CVE-2010-4700, CVE-2011-0753, CVE-20 ↪11-0754, CVE-2011-0755
BID:40173, 43926, 44605, 44718, 44723, 44951, 44980, 45119, 45335, 45338, 45339, ↪ 45952, 45954, 46056, 46168

Medium (CVSS: 6.4)
NVT: PHP Version < 5.3.9 Multiple Vulnerabilities

Product detection result
cpe:/a:php:php:5.2.4
Detected by PHP Version Detection (Remote) (OID: 1.3.6.1.4.1.25623.1.0.800109)

Summary
PHP version < 5.3.9 suffers from multiple vulnerabilities such as DOS by sending crafted requests including hash collision parameter values. Several errors exist in some certain functions as well.

Vulnerability Detection Result
Installed version: 5.2.4
Fixed version: 5.3.9

Solution
Solution type: VendorFix
Upgrade PHP to 5.3.9 or versions after.

Vulnerability Detection Method
Details:PHP Version < 5.3.9 Multiple Vulnerabilities
OID:1.3.6.1.4.1.25623.1.0.110012
Version used: $Revision: 4589 $

Product Detection Result
Product: cpe:/a:php:php:5.2.4
Method: PHP Version Detection (Remote)
OID: 1.3.6.1.4.1.25623.1.0.800109)

References
CVE: CVE-2011-4566, CVE-2011-4885, CVE-2012-0057, CVE-2012-0781, CVE-2012-0788, ↪CVE-2012-0789

... continues on next page ...

... continued from previous page ...

BID:50907, 51193, 51806, 51952, 51992, 52043

Medium (CVSS: 5.0)
NVT: PHP Versions Prior to 5.3.3/5.2.14 Multiple Vulnerabilities

Product detection result
cpe:/a:php:php:5.2.4
Detected by PHP Version Detection (Remote) (OID: 1.3.6.1.4.1.25623.1.0.800109)

Summary
PHP is prone to multiple security vulnerabilities.

Vulnerability Detection Result
Installed version: 5.2.4
Fixed version: 5.2.14

Impact
An attacker can exploit these issues to execute arbitrary code, crash the affected application, gain access to sensitive information and bypass security restrictions. Other attacks are also possible.

Solution
Solution type: VendorFix
Updates are available. Please see the references for more information.

Affected Software/OS
PHP 5.3 (Prior to 5.3.3) PHP 5.2 (Prior to 5.2.14)

Vulnerability Detection Method
Details:PHP Versions Prior to 5.3.3/5.2.14 Multiple Vulnerabilities
OID:1.3.6.1.4.1.25623.1.0.100726
Version used: $Revision: 4503 $

Product Detection Result
Product: cpe:/a:php:php:5.2.4
Method: PHP Version Detection (Remote)
OID: 1.3.6.1.4.1.25623.1.0.800109)

References
CVE: CVE-2010-2531, CVE-2010-2484
BID:41991
Other:
URL:https://www.securityfocus.com/bid/41991
URL:http://www.php.net/ChangeLog-5.php#5.3.3
URL:http://www.php.net/

Medium (CVSS: 6.8)
NVT: PHP XML Entity Expansion And XML External Entity Vulnerabilities (Linux)

Product detection result
cpe:/a:php:php:5.2.4
Detected by PHP Version Detection (Remote) (OID: 1.3.6.1.4.1.25623.1.0.800109)

Summary
This host is installed with PHP and is prone to XML entity expansion and XML external entity vulnerbilities

Vulnerability Detection Result
Installed version: 5.2.4
Fixed version: 5.5.22

Impact
Successfully exploiting this issue allow remote attackers to conduct XML External Entity (XXE) and XML Entity Expansion (XEE) attacks.
Impact Level: Application

Solution
Solution type: VendorFix
Upgrade to PHP version 5.5.22, or 5.6.6, or later. For updates refer to http://www.php.net

Affected Software/OS
PHP versions prior to 5.5.22 and 5.6.x before 5.6.6 on Linux

Vulnerability Insight
The flaw is due to script 'ext/libxml/libxml.c' does not isolate each thread from 'libxml_disable_entity_loader' when PHP-FPM is used.

Vulnerability Detection Method
Get the installed version with the help of detect NVT and check the version is vulnerable or not.
Details:PHP XML Entity Expansion And XML External Entity Vulnerabilities (Linux)
OID:1.3.6.1.4.1.25623.1.0.808615
Version used: $Revision: 5083 $

Product Detection Result
Product: cpe:/a:php:php:5.2.4
Method: PHP Version Detection (Remote)
OID: 1.3.6.1.4.1.25623.1.0.800109)

References
CVE: CVE-2015-8866
BID:87470
Other:

. . . continues on next page . . .

... continued from previous page ...

URL:http://www.php.net/ChangeLog-5.php

Medium (CVSS: 6.8)
NVT: PHP Zend and GD Multiple Denial of Service Vulnerabilities

Product detection result
cpe:/a:php:php:5.2.4
Detected by PHP Version Detection (Remote) (OID: 1.3.6.1.4.1.25623.1.0.800109)

Summary
This host is running PHP and is prone to multiple denial of service vulnerabilities.

Vulnerability Detection Result
Installed version: 5.2.4
Fixed version: 5.2.15/5.3.5

Impact
Successful exploitation could allow local attackers to crash the affected application, denying service to legitimate users.
Impact Level: Application/Network

Solution
Solution type: VendorFix
Upgrade to PHP 5.3.5 or later For updates refer to http://www.php.net/downloads.php

Affected Software/OS
PHP version prior to 5.2.15 and 5.3.x before 5.3.4

Vulnerability Insight
The flaws are due to: - An use-after-free error in the 'Zend' engine, which allows remote attackers to cause a denial of service. - A stack-based buffer overflow in the 'GD' extension, which allows attackers to cause a denial of service.

Vulnerability Detection Method
Details:PHP Zend and GD Multiple Denial of Service Vulnerabilities
OID:1.3.6.1.4.1.25623.1.0.801586
Version used: $Revision: 4502 $

Product Detection Result
Product: cpe:/a:php:php:5.2.4
Method: PHP Version Detection (Remote)
OID: 1.3.6.1.4.1.25623.1.0.800109)

References

... continues on next page ...

... continued from previous page ...

CVE: CVE-2010-4697, CVE-2010-4698
Other:
URL:http://bugs.php.net/52879
URL:http://www.php.net/ChangeLog-5.php

Medium (CVSS: 4.3)
NVT: phpMyAdmin 'error.php' Cross Site Scripting Vulnerability

Product detection result
cpe:/a:phpmyadmin:phpmyadmin:3.1.1
Detected by phpMyAdmin Detection (OID: 1.3.6.1.4.1.25623.1.0.900129)

Summary
The host is running phpMyAdmin and is prone to Cross-Site Scripting Vulnerability.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact
Successful exploitation will allow attackers to inject arbitrary HTML code within the error page and conduct phishing attacks.
Impact Level: Application

Solution
Solution type: WillNotFix
No solution or patch was made available for at least one year since disclosure of this vulnerability. Likely none will be provided anymore. General solution options are to upgrade to a newer release, disable respective features, remove the product or replace the product by another one.

Affected Software/OS
phpMyAdmin version 3.3.8.1 and prior.

Vulnerability Insight
The flaw is caused by input validation errors in the 'error.php' script when processing crafted BBcode tags containing '@' characters, which could allow attackers to inject arbitrary HTML code within the error page and conduct phishing attacks.

Vulnerability Detection Method
Details:phpMyAdmin 'error.php' Cross Site Scripting Vulnerability
OID:1.3.6.1.4.1.25623.1.0.801660
Version used: $Revision: 5323 $

Product Detection Result
Product: cpe:/a:phpmyadmin:phpmyadmin:3.1.1
Method: phpMyAdmin Detection

... continues on next page ...

... continued from previous page ...

OID: 1.3.6.1.4.1.25623.1.0.900129)

References
CVE: CVE-2010-4480
Other:
URL:http://www.exploit-db.com/exploits/15699/
URL:http://www.vupen.com/english/advisories/2010/3133

Medium (CVSS: 6.5)
NVT: phpMyAdmin Bookmark Security Bypass Vulnerability

Product detection result
cpe:/a:phpmyadmin:phpmyadmin:3.1.1
Detected by phpMyAdmin Detection (OID: 1.3.6.1.4.1.25623.1.0.900129)

Summary
phpMyAdmin is prone to a security-bypass vulnerability that affects bookmarks.
Successfully exploiting this issue allows a remote attacker to bypass certain security restrictions and perform unauthorized actions.
Versions prior to phpMyAdmin 3.3.9.2 and 2.11.11.3 are vulnerable.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Solution
Updates are available. Please see the references for details.

Vulnerability Detection Method
Details:phpMyAdmin Bookmark Security Bypass Vulnerability
OID:1.3.6.1.4.1.25623.1.0.103076
Version used: $Revision: 3911 $

Product Detection Result
Product: cpe:/a:phpmyadmin:phpmyadmin:3.1.1
Method: phpMyAdmin Detection
OID: 1.3.6.1.4.1.25623.1.0.900129)

References
CVE: CVE-2011-0987
BID:46359
Other:
URL:https://www.securityfocus.com/bid/46359
URL:http://www.phpmyadmin.net/
URL:http://www.phpmyadmin.net/home_page/security/PMASA-2011-2.php

Medium (CVSS: 4.3)
NVT: phpMyAdmin Database Search Cross Site Scripting Vulnerability

Product detection result
cpe:/a:phpmyadmin:phpmyadmin:3.1.1
Detected by phpMyAdmin Detection (OID: 1.3.6.1.4.1.25623.1.0.900129)

Summary
phpMyAdmin is prone to a cross-site scripting vulnerability because it fails to sufficiently sanitize user-supplied data.
An attacker may leverage this issue to execute arbitrary script code in the browser of an unsuspecting user in the context of the affected site. This may allow the attacker to steal cookie-based authentication credentials and to launch other attacks.
Versions prior to phpMyAdmin 3.3.8.1 and 2.11.11.1 are vulnerable.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Solution
Vendor updates are available. Please see the references for more information.

Vulnerability Detection Method
Details:phpMyAdmin Database Search Cross Site Scripting Vulnerability
OID:1.3.6.1.4.1.25623.1.0.100939
Version used: $Revision: 5323 $

Product Detection Result
Product: cpe:/a:phpmyadmin:phpmyadmin:3.1.1
Method: phpMyAdmin Detection
OID: 1.3.6.1.4.1.25623.1.0.900129)

References
CVE: CVE-2010-4329
BID:45100
Other:
URL:https://www.securityfocus.com/bid/45100
URL:http://www.phpmyadmin.net/
URL:http://www.phpmyadmin.net/home_page/security/PMASA-2010-8.php

Medium (CVSS: 4.3)
NVT: phpMyAdmin Debug Backtrace Cross Site Scripting Vulnerability

Product detection result
cpe:/a:phpmyadmin:phpmyadmin:3.1.1
Detected by phpMyAdmin Detection (OID: 1.3.6.1.4.1.25623.1.0.900129)

... continues on next page ...

... continued from previous page ...

Summary
phpMyAdmin is prone to a cross-site scripting vulnerability because it fails to sufficiently sanitize user-supplied data.
An attacker may leverage this issue to execute arbitrary script code in the browser of an unsuspecting user in the context of the affected site. This may allow the attacker to steal cookie-based authentication credentials and to launch other attacks.
Versions prior to phpMyAdmin 3.3.6 are vulnerable other versions may also be affected.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Solution
Vendor updates are available. Please see the references for more information.

Vulnerability Detection Method
Details:`phpMyAdmin Debug Backtrace Cross Site Scripting Vulnerability`
OID:1.3.6.1.4.1.25623.1.0.100775
Version used: `$Revision: 5323 $`

Product Detection Result
Product: `cpe:/a:phpmyadmin:phpmyadmin:3.1.1`
Method: `phpMyAdmin Detection`
OID: 1.3.6.1.4.1.25623.1.0.900129)

References
`CVE: CVE-2010-2958`
`BID:42874`
`Other:`
`URL:https://www.securityfocus.com/bid/42874`
`URL:http://www.phpmyadmin.net/`
`URL:http://www.phpmyadmin.net/home_page/security/PMASA-2010-6.php`
`URL:http://www.phpmyadmin.git.sourceforge.net/git/gitweb.cgi?p=phpmyadmin/php`
`↪myadmin;a=commitdiff;h=133a77fac7d31a38703db2099a90c1b49de62e37`

Medium (CVSS: 4.3)
NVT: phpMyAdmin Multiple Cross Site Scripting Vulnerabilities

Product detection result
`cpe:/a:phpmyadmin:phpmyadmin:3.1.1`
`Detected by phpMyAdmin Detection (OID: 1.3.6.1.4.1.25623.1.0.900129)`

Summary

... continues on next page ...

... continued from previous page ...

phpMyAdmin is prone to multiple cross-site scripting vulnerabilities because it fails to properly sanitize user-supplied input.
An attacker may leverage these issues to execute arbitrary script code in the browser of an unsuspecting user in the context of the affected site. This can allow the attacker to steal cookie-based authentication credentials and launch other attacks.
The following versions are vulnerable:
phpMyAdmin 2.11.x prior to 2.11.10.1 phpMyAdmin 3.x prior to 3.3.5.1

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Solution
Updates are available. Please see the references for details.

Vulnerability Detection Method
Details:`phpMyAdmin Multiple Cross Site Scripting Vulnerabilities`
OID:1.3.6.1.4.1.25623.1.0.100761
Version used: `$Revision: 5323 $`

Product Detection Result
Product: `cpe:/a:phpmyadmin:phpmyadmin:3.1.1`
Method: `phpMyAdmin Detection`
OID: 1.3.6.1.4.1.25623.1.0.900129)

References
`CVE: CVE-2010-3056`
`BID:42584`
`Other:`
`URL:https://www.securityfocus.com/bid/42584`
`URL:http://www.phpmyadmin.net/`
`URL:http://www.phpmyadmin.net/home_page/security/PMASA-2010-5.php`

Medium (CVSS: 4.3)
NVT: phpMyAdmin Setup Script Request Cross Site Scripting Vulnerability

Product detection result
`cpe:/a:phpmyadmin:phpmyadmin:3.1.1`
`Detected by phpMyAdmin Detection (OID: 1.3.6.1.4.1.25623.1.0.900129)`

Summary
The host is running phpMyAdmin and is prone to Cross-Site Scripting Vulnerability.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

... continues on next page ...

... continued from previous page ...

Impact
Successful exploitation will allow attackers to execute arbitrary web script or HTML in a user's browser session in the context of an affected site. Impact Level: Application

Solution
Upgrade to phpMyAdmin version 3.3.7 or later, For updates refer to http://www.phpmyadmin.net/home_page/downloads.php

Affected Software/OS
phpMyAdmin versions 3.x before 3.3.7

Vulnerability Insight
The flaw is caused by an unspecified input validation error when processing spoofed requests sent to setup script, which could be exploited by attackers to cause arbitrary scripting code to be executed on the user's browser session in the security context of an affected site.

Vulnerability Detection Method
Details:`phpMyAdmin Setup Script Request Cross Site Scripting Vulnerability`
OID:1.3.6.1.4.1.25623.1.0.801286
Version used: `$Revision: 5373 $`

Product Detection Result
Product: `cpe:/a:phpmyadmin:phpmyadmin:3.1.1`
Method: `phpMyAdmin Detection`
OID: 1.3.6.1.4.1.25623.1.0.900129)

References
```
CVE: CVE-2010-3263
Other:
  URL:http://secunia.com/advisories/41210
   URL:http://xforce.iss.net/xforce/xfdb/61675
   URL:http://www.phpmyadmin.net/home_page/security/PMASA-2010-7.php
```

Medium (CVSS: 4.3)
NVT: phpMyAdmin SQL bookmark XSS Vulnerability

Product detection result
```
cpe:/a:phpmyadmin:phpmyadmin:3.1.1
Detected by phpMyAdmin Detection (OID: 1.3.6.1.4.1.25623.1.0.900129)
```

Summary
This host is running phpMyAdmin and is prone to Cross Site Scripting vulnerability.

... continues on next page ...

... continued from previous page ...

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact
Successful exploitation will let the attacker cause XSS attacks and inject malicious web script or HTML code via a crafted SQL bookmarks.

Solution
Apply the respective patches or upgrade to version 3.2.0.1 http://www.phpmyadmin.net/home_page/downloads.php http://phpmyadmin.svn.sourceforge.net/viewvc/phpmy
*** Note: Ignore the warning if above mentioned patches are applied. *****

Affected Software/OS
phpMyAdmin version 3.0.x to 3.2.0.rc1

Vulnerability Insight
This flaw arises because the input passed into SQL bookmarks is not adequately sanitised before using it in dynamically generated content.

Vulnerability Detection Method
Details:`phpMyAdmin SQL bookmark XSS Vulnerability`
OID:1.3.6.1.4.1.25623.1.0.800595
Version used: `$Revision: 4869 $`

Product Detection Result
Product: `cpe:/a:phpmyadmin:phpmyadmin:3.1.1`
Method: `phpMyAdmin Detection`
OID: 1.3.6.1.4.1.25623.1.0.900129)

References
`CVE: CVE-2009-2284`
`BID:35543`
`Other:`
`URL:http://secunia.com/advisories/35649`
`URL:http://www.phpmyadmin.net/home_page/security/PMASA-2009-5.php`

Medium (CVSS: 4.3)
NVT: phpMyAdmin Unspecified SQL Injection and Cross Site Scripting Vulnerabilities

Product detection result
`cpe:/a:phpmyadmin:phpmyadmin:3.1.1`
`Detected by phpMyAdmin Detection (OID: 1.3.6.1.4.1.25623.1.0.900129)`

Summary

... continues on next page ...

... continued from previous page ...

phpMyAdmin is prone to SQL-injection and cross-site scripting vulnerabilities because it fails to sufficiently sanitize user- supplied data.
Exploiting these issues could allow an attacker to steal cookie- based authentication credentials, compromise the application, access or modify data, or exploit latent vulnerabilities in the underlying database.
Versions prior to phpMyAdmin 2.11.9.6 and 3.2.2.1 are affected.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Solution
Vendor updates are available. Please see the references for details.

Vulnerability Detection Method
Details:`phpMyAdmin Unspecified SQL Injection and Cross Site Scripting Vulnerabilities`
OID:1.3.6.1.4.1.25623.1.0.100307
Version used: `$Revision: 5016 $`

Product Detection Result
Product: `cpe:/a:phpmyadmin:phpmyadmin:3.1.1`
Method: `phpMyAdmin Detection`
OID: 1.3.6.1.4.1.25623.1.0.900129)

References
```
CVE: CVE-2009-3696
BID:36658
Other:
  URL:http://www.securityfocus.com/bid/36658
   URL:http://www.phpmyadmin.net/
   URL:http://freshmeat.net/projects/phpmyadmin/releases/306669
   URL:http://freshmeat.net/projects/phpmyadmin/releases/306667
```

Medium (CVSS: 5.0)
NVT: Tiki Wiki CMS Groupware 'fixedURLData' Local File Inclusion Vulnerability

Product detection result
`cpe:/a:tiki:tikiwiki_cms/groupware:1.9.5`
`Detected by Tiki Wiki CMS Groupware Version Detection (OID: 1.3.6.1.4.1.25623.1.`
`↪0.901001)`

Summary
The host is installed with Tiki Wiki CMS Groupware and is prone to a local file inclusion vulnerability.

Vulnerability Detection Result

... continues on next page ...

... continued from previous page ...

```
Installed version: 1.9.5
Fixed version:     12.11
```

Impact
Successful exploitation will allow an user having access to the admin backend to gain access to arbitrary files and to compromise the application.
Impact Level: System/Application

Solution
Solution type: VendorFix
Upgrade to Tiki Wiki CMS Groupware version 12.11 LTS, 15.4 or later. For updates refer to https://tiki.org

Affected Software/OS
Tiki Wiki CMS Groupware versions:
- below 12.11 LTS
- 13.x, 14.x and 15.x below 15.4

Vulnerability Insight
The Flaw is due to improper sanitization of input passed to the 'fixedURLData' parameter of the 'display_banner.php' script.

Vulnerability Detection Method
Get the installed version with the help of the detect NVT and check the version is vulnerable or not.
Details:`Tiki Wiki CMS Groupware 'fixedURLData' Local File Inclusion Vulnerability`
OID:1.3.6.1.4.1.25623.1.0.108064
Version used: `$Revision: 5144 $`

Product Detection Result
Product: `cpe:/a:tiki:tikiwiki_cms/groupware:1.9.5`
Method: `Tiki Wiki CMS Groupware Version Detection`
OID: 1.3.6.1.4.1.25623.1.0.901001)

References
`CVE: CVE-2016-10143`
`Other:`
`URL:http://tiki.org/article445-Security-updates-Tiki-16-2-15-4-and-Tiki-12-11-released`
`URL:https://sourceforge.net/p/tikiwiki/code/60308/`

Medium (CVSS: 5.0)
NVT: Tiki Wiki CMS Groupware Input Sanitation Weakness Vulnerability

Product detection result
`cpe:/a:tiki:tikiwiki_cms/groupware:1.9.5`

... continues on next page ...

... continued from previous page ...

Detected by Tiki Wiki CMS Groupware Version Detection (OID: 1.3.6.1.4.1.25623.1.
↪0.901001)

Summary
The host is installed with Tiki Wiki CMS Groupware and is prone to input sanitation weakness vulnerability.

Vulnerability Detection Result
Installed version: 1.9.5
Fixed version: 2.2

Impact
Successful exploitation could allow arbitrary code execution in the context of an affected site.
Impact Level: Application

Solution
Solution type: VendorFix
Upgrade to version 2.2 or latest http://info.tikiwiki.org/tiki-index.php?page=Get+Tiki&bl

Affected Software/OS
Tiki Wiki CMS Groupware version prior to 2.2 on all running platform

Vulnerability Insight
The vulnerability is due to input validation error in tiki-error.php which fails to sanitise before being returned to the user.

Vulnerability Detection Method
Details:Tiki Wiki CMS Groupware Input Sanitation Weakness Vulnerability
OID:1.3.6.1.4.1.25623.1.0.800315
Version used: $Revision: 5144 $

Product Detection Result
Product: cpe:/a:tiki:tikiwiki_cms/groupware:1.9.5
Method: Tiki Wiki CMS Groupware Version Detection
OID: 1.3.6.1.4.1.25623.1.0.901001)

References
CVE: CVE-2008-5318, CVE-2008-5319
Other:
URL:http://secunia.com/advisories/32341
URL:http://info.tikiwiki.org/tiki-read_article.php?articleId=41

Medium (CVSS: 6.0)
NVT: TWiki Cross-Site Request Forgery Vulnerability

... continues on next page ...

... continued from previous page ...

Product detection result
cpe:/a:twiki:twiki:01.Feb.2003
Detected by TWiki Version Detection (OID: 1.3.6.1.4.1.25623.1.0.800399)

Summary
The host is running TWiki and is prone to Cross-Site Request Forgery Vulnerability.

Vulnerability Detection Result
Installed version: 01.Feb.2003
Fixed version: 4.3.1

Impact
Successful exploitation will allow attacker to gain administrative privileges on the target application and can cause CSRF attack.
Impact Level: Application

Solution
Solution type: VendorFix
Upgrade to version 4.3.1 or later, http://twiki.org/cgi-bin/view/Codev/DownloadTWiki

Affected Software/OS
TWiki version prior to 4.3.1

Vulnerability Insight
Remote authenticated user can create a specially crafted image tag that, when viewed by the target user, will update pages on the target system with the privileges of the target user via HTTP requests.

Vulnerability Detection Method
Details:TWiki Cross-Site Request Forgery Vulnerability
OID:1.3.6.1.4.1.25623.1.0.800400
Version used: $Revision: 4892 $

Product Detection Result
Product: cpe:/a:twiki:twiki:01.Feb.2003
Method: TWiki Version Detection
OID: 1.3.6.1.4.1.25623.1.0.800399)

References
CVE: CVE-2009-1339
Other:
URL:http://secunia.com/advisories/34880
URL:http://bugs.debian.org/cgi-bin/bugreport.cgi?bug=526258
URL:http://twiki.org/p/pub/Codev/SecurityAlert-CVE-2009-1339/TWiki-4.3.0-c-di
↪ff-cve-2009-1339.txt

Medium (CVSS: 6.8)
NVT: TWiki Cross-Site Request Forgery Vulnerability - Sep10

Product detection result
cpe:/a:twiki:twiki:01.Feb.2003
Detected by TWiki Version Detection (OID: 1.3.6.1.4.1.25623.1.0.800399)

Summary
The host is running TWiki and is prone to Cross-Site Request Forgery vulnerability.

Vulnerability Detection Result
Installed version: 01.Feb.2003
Fixed version: 4.3.2

Impact
Successful exploitation will allow attacker to gain administrative privileges on the target application and can cause CSRF attack.
Impact Level: Application

Solution
Solution type: VendorFix
Upgrade to TWiki version 4.3.2 or later, For updates refer to http://twiki.org/cgi-bin/view/Codev/DownloadTWiki

Affected Software/OS
TWiki version prior to 4.3.2

Vulnerability Insight
Attack can be done by tricking an authenticated TWiki user into visiting a static HTML page on another side, where a Javascript enabled browser will send an HTTP POST request to TWiki, which in turn will process the request as the TWiki user.

Vulnerability Detection Method
Details:TWiki Cross-Site Request Forgery Vulnerability - Sep10
OID:1.3.6.1.4.1.25623.1.0.801281
Version used: $Revision: 4293 $

Product Detection Result
Product: cpe:/a:twiki:twiki:01.Feb.2003
Method: TWiki Version Detection
OID: 1.3.6.1.4.1.25623.1.0.800399)

References
CVE: CVE-2009-4898
Other:
URL:http://www.openwall.com/lists/oss-security/2010/08/03/8

... continues on next page ...

... continued from previous page ...

URL:http://www.openwall.com/lists/oss-security/2010/08/02/17
URL:http://twiki.org/cgi-bin/view/Codev/SecurityAuditTokenBasedCsrfFix

[return to 192.168.8.102]

2.1.22 Low 5432/tcp

Low (CVSS: 3.5)
NVT: PostgreSQL Hash Table Integer Overflow Vulnerability

Product detection result
cpe:/a:postgresql:postgresql:8.3.1
Detected by PostgreSQL Detection (OID: 1.3.6.1.4.1.25623.1.0.100151)

Summary
The host is running PostgreSQL and is prone to integer overflow vulnerability.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact
Successful exploitation could allow execution of specially-crafted sql query which once processed would lead to denial of service (postgresql daemon crash). Impact Level: Application

Solution
Apply the patch, http://git.postgresql.org/gitweb?p=postgresql.git a=commitdiff h=64b057e6823655fb6c5d1f24a28f236b94dd6c54
**** NOTE: Please ignore this warning if the patch is applied. ******

Affected Software/OS
PostgreSQL version 8.4.1 and prior and 8.5 through 8.5alpha2

Vulnerability Insight
The flaw is due to an integer overflow error in 'src/backend/executor/nodeHash.c', when used to calculate size for the hashtable for joined relations.

Vulnerability Detection Method
Details:PostgreSQL Hash Table Integer Overflow Vulnerability
OID:1.3.6.1.4.1.25623.1.0.902139
Version used: $Revision: 5401 $

Product Detection Result
Product: cpe:/a:postgresql:postgresql:8.3.1
Method: PostgreSQL Detection

... continues on next page ...

... continued from previous page ...

OID: 1.3.6.1.4.1.25623.1.0.100151)

References

```
CVE: CVE-2010-0733
Other:
  URL:https://bugzilla.redhat.com/show_bug.cgi?id=546621
   URL:http://www.openwall.com/lists/oss-security/2010/03/16/10
   URL:http://archives.postgresql.org/pgsql-bugs/2009-10/msg00310.php
   URL:http://archives.postgresql.org/pgsql-bugs/2009-10/msg00289.php
   URL:http://archives.postgresql.org/pgsql-bugs/2009-10/msg00287.php
   URL:http://archives.postgresql.org/pgsql-bugs/2009-10/msg00277.php
```

Low (CVSS: 2.1)
NVT: PostgreSQL Low Cost Function Information Disclosure Vulnerability

Product detection result

```
cpe:/a:postgresql:postgresql:8.3.1
Detected by PostgreSQL Detection (OID: 1.3.6.1.4.1.25623.1.0.100151)
```

Summary

PostgreSQL is prone to an information-disclosure vulnerability.
Local attackers can exploit this issue to obtain sensitive information that may lead to further attacks.
PostgreSQL 8.3.6 is vulnerable other versions may also be affected.

Vulnerability Detection Result

Vulnerability was detected according to the Vulnerability Detection Method.

Vulnerability Detection Method

Details:`PostgreSQL Low Cost Function Information Disclosure Vulnerability`
OID:1.3.6.1.4.1.25623.1.0.100158
Version used: `$Revision: 5016 $`

Product Detection Result

Product: `cpe:/a:postgresql:postgresql:8.3.1`
Method: `PostgreSQL Detection`
OID: 1.3.6.1.4.1.25623.1.0.100151)

References

```
BID:34069
Other:
  URL:http://www.securityfocus.com/bid/34069
   URL:http://www.postgresql.org/
```

[return to 192.168.8.102]

2.1.23 Low 22/tcp

Low (CVSS: 2.1)
NVT: OpenSSH 'ssh-keysign.c' Local Information Disclosure Vulnerability

Summary
OpenSSH is prone to a local information-disclosure vulnerability.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact
Local attackers can exploit this issue to obtain sensitive information. Information obtained may lead to further attacks.

Solution
Updates are available.

Affected Software/OS
Versions prior to OpenSSH 5.8p2 are vulnerable.

Vulnerability Insight
ssh-keysign.c in ssh-keysign in OpenSSH before 5.8p2 on certain platforms executes ssh-rand-helper with unintended open file descriptors, which allows local users to obtain sensitive key information via the ptrace system call.

Vulnerability Detection Method
Check the version.
Details:`OpenSSH 'ssh-keysign.c' Local Information Disclosure Vulnerability`
OID:1.3.6.1.4.1.25623.1.0.105002
Version used: `$Revision: 4336 $`

References
```
CVE: CVE-2011-4327
BID:65674
Other:
  URL:http://www.securityfocus.com/bid/65674
   URL:http://www.openssh.com
   URL:http://www.openssh.com/txt/portable-keysign-rand-helper.adv
```

Low (CVSS: 3.5)
NVT: OpenSSH 'ssh_gssapi_parse_ename()' Function Denial of Service Vulnerability

Summary

... continues on next page ...

. . . continued from previous page . . .

OpenSSH is prone to a remote denial-of-service vulnerability.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact
Exploiting this issue allows remote attackers to trigger denial-of-service conditions due to excessive memory consumption.

Solution
Updates are available. Please see the references for details.

Affected Software/OS
OpenSSH 5.8 and prior are vulnerable.

Vulnerability Detection Method
Check the version.
Details:`OpenSSH 'ssh_gssapi_parse_ename()' Function Denial of Service Vulnerability`
OID:1.3.6.1.4.1.25623.1.0.103937
Version used: `$Revision: 4336 $`

References
`CVE: CVE-2011-5000`
`BID:54114`
`Other:`
`URL:http://www.securityfocus.com/bid/54114`
`URL:http://www.openssh.com`

Low (CVSS: 2.6)
NVT: OpenSSH CBC Mode Information Disclosure Vulnerability

Summary
The host is installed with OpenSSH and is prone to information disclosure vulnerability.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact
Successful exploits will allow attackers to obtain four bytes of plaintext from an encrypted session.
Impact Level: Application

Solution
Upgrade to higher version http://www.openssh.com/portable.html

Affected Software/OS
Versions prior to OpenSSH 5.2 are vulnerable. Various versions of SSH Tectia are also affected.

. . . continues on next page . . .

... continued from previous page ...

Vulnerability Insight
The flaw is due to the improper handling of errors within an SSH session encrypted with a block cipher algorithm in the Cipher-Block Chaining 'CBC' mode.

Vulnerability Detection Method
Details:`OpenSSH CBC Mode Information Disclosure Vulnerability`
OID:1.3.6.1.4.1.25623.1.0.100153
Version used: `$Revision: 5002 $`

References
`CVE: CVE-2008-5161`
`BID:32319`
`Other:`
`URL:http://www.securityfocus.com/bid/32319`

Low (CVSS: 3.5)
NVT: openssh-server Forced Command Handling Information Disclosure Vulnerability

Summary
The auth_parse_options function in auth-options.c in sshd in OpenSSH before 5.7 provides debug messages containing authorized_keys command options, which allows remote authenticated users to obtain potentially sensitive information by reading these messages, as demonstrated by the shared user account required by Gitolite. NOTE: this can cross privilege boundaries because a user account may intentionally have no shell or filesystem access, and therefore may have no supported way to read an authorized_keys file in its own home directory.

Vulnerability Detection Result
```
According to its banner, the version of OpenSSH installed on the remote
host is older than 5.7:
 SSH-2.0-OpenSSH_4.7p1 Debian-8ubuntu1
```

Solution
Updates are available. Please see the references for more information.

Affected Software/OS
OpenSSH before 5.7

Vulnerability Detection Method
Details:`openssh-server Forced Command Handling Information Disclosure Vulnerability`
OID:1.3.6.1.4.1.25623.1.0.103503
Version used: `$Revision: 5950 $`

References
`CVE: CVE-2012-0814`
`BID:51702`

... continues on next page ...

... continued from previous page ...

```
Other:
  URL:http://www.securityfocus.com/bid/51702
   URL:http://bugs.debian.org/cgi-bin/bugreport.cgi?bug=657445
   URL:http://packages.debian.org/squeeze/openssh-server
   URL:https://downloads.avaya.com/css/P8/documents/100161262
```

Low (CVSS: 2.6)
NVT: SSH Weak MAC Algorithms Supported

Summary
The remote SSH server is configured to allow weak MD5 and/or 96-bit MAC algorithms.

Vulnerability Detection Result

```
The following weak client-to-server MAC algorithms are supported by the remote s
↪ervice:
hmac-md5
hmac-md5-96
hmac-sha1-96
The following weak server-to-client MAC algorithms are supported by the remote s
↪ervice:
hmac-md5
hmac-md5-96
hmac-sha1-96
```

Solution
Solution type: Mitigation
Disable the weak MAC algorithms.

Vulnerability Detection Method
Details:`SSH Weak MAC Algorithms Supported`
OID:1.3.6.1.4.1.25623.1.0.105610
Version used: `$Revision: 4490 $`

[return to 192.168.8.102]

2.1.24 Low general/tcp

Low (CVSS: 2.6)
NVT: TCP timestamps

Summary
The remote host implements TCP timestamps and therefore allows to compute the uptime.

Vulnerability Detection Result

```
It was detected that the host implements RFC1323.
```

... continues on next page ...

... continued from previous page ...

```
The following timestamps were retrieved with a delay of 1 seconds in-between:
Packet 1: 606423
Packet 2: 606526
```

Impact
A side effect of this feature is that the uptime of the remote host can sometimes be computed.

Solution
Solution type: Mitigation
To disable TCP timestamps on linux add the line 'net.ipv4.tcp_timestamps = 0' to /etc/sysctl.conf. Execute 'sysctl -p' to apply the settings at runtime.
To disable TCP timestamps on Windows execute 'netsh int tcp set global timestamps=disabled' Starting with Windows Server 2008 and Vista, the timestamp can not be completely disabled.
The default behavior of the TCP/IP stack on this Systems is to not use the Timestamp options when initiating TCP connections, but use them if the TCP peer that is initiating communication includes them in their synchronize (SYN) segment.
See also: http://www.microsoft.com/en-us/download/details.aspx?id=9152

Affected Software/OS
TCP/IPv4 implementations that implement RFC1323.

Vulnerability Insight
The remote host implements TCP timestamps, as defined by RFC1323.

Vulnerability Detection Method
Special IP packets are forged and sent with a little delay in between to the target IP. The responses are searched for a timestamps. If found, the timestamps are reported.
Details:`TCP timestamps`
OID:1.3.6.1.4.1.25623.1.0.80091
Version used: `$Revision: 5740 $`

References
```
Other:
  URL:http://www.ietf.org/rfc/rfc1323.txt
```

[return to 192.168.8.102]

2.1.25 Low 445/tcp

Low (CVSS: 2.1)
NVT: Samba 'client/mount.cifs.c' Remote Denial of Service Vulnerability

Product detection result
```
cpe:/a:samba:samba:3.0.20
Detected by SMB NativeLanMan (OID: 1.3.6.1.4.1.25623.1.0.102011)
```

... continues on next page ...

... continued from previous page ...

Summary
Samba is prone to a remote denial-of-service vulnerability.

Vulnerability Detection Result
Installed version: 3.0.20
Fixed version: 3.5.11 or later

Impact
A remote attacker can exploit this issue to crash the affected application, denying service to legitimate users.

Solution
Solution type: VendorFix
Upgrade to Samba version 3.5.11 or later.

Affected Software/OS
Samba 3.5.10 and earlier are vulnerable.

Vulnerability Detection Method
Details:Samba 'client/mount.cifs.c' Remote Denial of Service Vulnerability
OID:1.3.6.1.4.1.25623.1.0.100499
Version used: $Revision: 4387 $

Product Detection Result
Product: cpe:/a:samba:samba:3.0.20
Method: SMB NativeLanMan
OID: 1.3.6.1.4.1.25623.1.0.102011)

References
CVE: CVE-2010-0547, CVE-2011-2724
BID:38326
Other:
URL:http://www.securityfocus.com/bid/38326
URL:http://git.samba.org/?p=samba.git;a=commit;h=a065c177dfc8f968775593ba00df
↪fafeebb2e054
URL:http://us1.samba.org/samba/

Low (CVSS: 3.3)
NVT: Samba 'etc/mtab' File Appending Local Denial of Service Vulnerability

Product detection result
cpe:/a:samba:samba:3.0.20
Detected by SMB NativeLanMan (OID: 1.3.6.1.4.1.25623.1.0.102011)

... continues on next page ...

... continued from previous page ...

Summary
Samba is prone to a local denial-of-service vulnerability.

Vulnerability Detection Result
`Installed version: 3.0.20`
`Fixed version: 3.5.9`

Impact
A local attacker can exploit this issue to cause the computer to stop responding, denying service to legitimate users.

Solution
Solution type: VendorFix
Updates are available. Please see the references for more information.

Vulnerability Detection Method
Details:`Samba 'etc/mtab' File Appending Local Denial of Service Vulnerability`
OID:1.3.6.1.4.1.25623.1.0.103298
Version used: `$Revision: 4398 $`

Product Detection Result
Product: `cpe:/a:samba:samba:3.0.20`
Method: `SMB NativeLanMan`
OID: 1.3.6.1.4.1.25623.1.0.102011)

References
`CVE: CVE-2011-1678`
`BID:49939`
`Other:`
`URL:http://www.securityfocus.com/bid/49939`
`URL:https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2011-1678`
`URL:http://us1.samba.org/samba/`

Low (CVSS: 3.5)
NVT: Samba Symlink Directory Traversal Vulnerability

Product detection result
`cpe:/a:samba:samba:3.0.20`
`Detected by SMB NativeLanMan (OID: 1.3.6.1.4.1.25623.1.0.102011)`

Summary
Samba is prone to a directory-traversal vulnerability because the application fails to sufficiently sanitize user-supplied input.

... continues on next page ...

... continued from previous page ...

Vulnerability Detection Result
Installed version: 3.0.20
Fixed version: 3.3.11/3.4.6/3.5.0rc3

Impact
Exploits would allow an attacker to access files outside of the Samba user's root directory to obtain sensitive information and perform other attacks.

Solution
Solution type: VendorFix
The vendor commented on the issue stating that it stems from an insecure default configuration. The Samba team advises administrators to set 'wide links = no' in the '[global]' section of 'smb.conf' and then restart the service to correct misconfigured services.
Please see the references for more information.

Affected Software/OS
Samba versions before 3.3.11, 3.4.x before 3.4.6, and 3.5.x before 3.5.0rc3

Vulnerability Insight
To exploit this issue, attackers require authenticated access to a writable share. Note that this issue may be exploited through a writable share accessible by guest accounts.

Vulnerability Detection Method
Details:Samba Symlink Directory Traversal Vulnerability
OID:1.3.6.1.4.1.25623.1.0.100488
Version used: $Revision: 4392 $

Product Detection Result
Product: cpe:/a:samba:samba:3.0.20
Method: SMB NativeLanMan
OID: 1.3.6.1.4.1.25623.1.0.102011)

References
CVE: CVE-2010-0926
BID:38111
Other:
URL:http://www.securityfocus.com/bid/38111
URL:http://www.samba.org/samba/news/symlink_attack.html
URL:http://archives.neohapsis.com/archives/fulldisclosure/2010-02/0100.html
URL:http://www.samba.org
URL:http://lists.grok.org.uk/pipermail/full-disclosure/2010-February/072927.h
↪tml
URL:https://www.samba.org/samba/security/CVE-2010-0926.html

[return to 192.168.8.102]

2.1.26 Low 53/tcp

Low (CVSS: 2.6)
NVT: ISC BIND 9 DNSSEC Query Response Additional Section Remote Cache Poisoning Vulnerability

Product detection result
cpe:/a:isc:bind:9.4.2
Detected by Determine which version of BIND name daemon is running (OID: 1.3.6.1
↪.4.1.25623.1.0.10028)

Summary
ISC BIND 9 is prone to a remote cache-poisoning vulnerability.

Vulnerability Detection Result
Installed version: 9.4.2
Fixed version: 9.4.3-P4

Impact
An attacker may leverage this issue to manipulate cache data, potentially facilitating man-in-the-middle, site-impersonation, or denial-of- service attacks.

Solution
Solution type: VendorFix
Updates are available. Please see the references for details.

Affected Software/OS
Versions prior to the following are vulnerable:
BIND 9.4.3-P4 BIND 9.5.2-P1 BIND 9.6.1-P2

Vulnerability Detection Method
Details:ISC BIND 9 DNSSEC Query Response Additional Section Remote Cache Poisoning Vuln.
↪..
OID:1.3.6.1.4.1.25623.1.0.100362
Version used: $Revision: 4435 $

Product Detection Result
Product: cpe:/a:isc:bind:9.4.2
Method: Determine which version of BIND name daemon is running
OID: 1.3.6.1.4.1.25623.1.0.10028)

References
CVE: CVE-2009-4022
BID:37118
Other:
URL:http://www.securityfocus.com/bid/37118

... continues on next page ...

... continued from previous page ...

URL:https://www.isc.org/node/504
URL:http://www.isc.org/products/BIND/

[return to 192.168.8.102]

2.1.27 Low 80/tcp

Low (CVSS: 2.6)
NVT: Apache 'mod_proxy_ftp' Module Denial Of Service Vulnerability (Linux)

Summary
The host is running Apache and is prone to Denial of Service vulnerability.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact
Successful exploitation could allow remote attackers to cause a Denial of Service in the context of the affected application. Impact Level: Application

Solution
Upgrade to Apache HTTP Server version 2.2.15 or later For updates refer to http://www.apache.org/

Affected Software/OS
Apache HTTP Server version 2.0.x to 2.0.63 and and 2.2.x to 2.2.13 on Linux.

Vulnerability Insight
The flaw is due to an error in 'ap_proxy_ftp_handler' function in modules/proxy/proxy_ftp.c in the mod_proxy_ftp module while processing responses received from FTP servers. This can be exploited to trigger a NULL-pointer dereference and crash an Apache child process via a malformed EPSV response.

Vulnerability Detection Method
Details:Apache 'mod_proxy_ftp' Module Denial Of Service Vulnerability (Linux)
OID:1.3.6.1.4.1.25623.1.0.900841
Version used: $Revision: 5390 $

References
CVE: CVE-2009-3094
BID:36260
Other:
URL:http://intevydis.com/vd-list.shtml
URL:http://www.intevydis.com/blog/?p=59
URL:http://secunia.com/advisories/36549
URL:http://httpd.apache.org/docs/2.0/mod/mod_proxy_ftp.html

Low (CVSS: 1.2)
NVT: Apache HTTP Server 'ap_pregsub()' Function Local Denial of Service Vulnerability

Summary
Apache HTTP Server is prone to a local denial-of-service vulnerability because of a NULL-pointer dereference error or a memory exhaustion.
Local attackers can exploit this issue to trigger a NULL-pointer dereference or memory exhaustion, and cause a server crash, denying service to legitimate users.
Note: To trigger this issue, 'mod_setenvif' must be enabled and the attacker should be able to place a malicious '.htaccess' file on the affected webserver.
Apache HTTP Server 2.0.x through 2.0.64 and 2.2.x through 2.2.21 are vulnerable. Other versions may also be affected.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Vulnerability Detection Method
Details:`Apache HTTP Server 'ap_pregsub()' Function Local Denial of Service Vulnerability`
OID:1.3.6.1.4.1.25623.1.0.103333
Version used: `$Revision: 5424 $`

References
`CVE: CVE-2011-4415`
`BID:50639`
`Other:`
`URL:http://www.securityfocus.com/bid/50639`
`URL:http://httpd.apache.org/`
`URL:http://www.halfdog.net/Security/2011/ApacheModSetEnvIfIntegerOverflow/`
`URL:http://www.gossamer-threads.com/lists/apache/dev/403775`

Low (CVSS: 2.1)
NVT: PHP 'mbstring.func_overload' DoS Vulnerability

Product detection result
`cpe:/a:php:php:5.2.4`
`Detected by PHP Version Detection (Remote) (OID: 1.3.6.1.4.1.25623.1.0.800109)`

Summary
The host is running PHP and is prone to denial of service vulnerability.

Vulnerability Detection Result
`Installed version: 5.2.4`
`Fixed version: 4.4.5/5.1.7/5.2.6`

Impact
. . . continues on next page . . .

... continued from previous page ...

Successful exploitation will let the local attackers to crash an affected web server. Impact Level: Application

Solution
Solution type: VendorFix
Apply patch from below link, http://php.net

Affected Software/OS
PHP version 4.4.4 and prior PHP 5.1.x to 5.1.6 PHP 5.2.x to 5.2.5

Vulnerability Insight
This bug is due to an error in 'mbstring.func_overload' setting in .htaccess file. It can be exploited via modifying behavior of other sites hosted on the same web server which causes this setting to be applied to other virtual hosts on the same server.

Vulnerability Detection Method
Details:`PHP 'mbstring.func_overload' DoS Vulnerability`
OID:1.3.6.1.4.1.25623.1.0.800373
Version used: `$Revision: 4504 $`

Product Detection Result
Product: `cpe:/a:php:php:5.2.4`
Method: `PHP Version Detection (Remote)`
OID: 1.3.6.1.4.1.25623.1.0.800109)

References
`CVE: CVE-2009-0754`
`BID:33542`
`Other:`
`URL:http://bugs.php.net/bug.php?id=27421`
`URL:https://bugzilla.redhat.com/show_bug.cgi?id=479272`

Low (CVSS: 2.6)
NVT: PHP display_errors Cross-Site Scripting Vulnerability

Product detection result
`cpe:/a:php:php:5.2.4`
`Detected by PHP Version Detection (Remote) (OID: 1.3.6.1.4.1.25623.1.0.800109)`

Summary
The host is running PHP and is prone to Cross-Site Scripting vulnerability.

Vulnerability Detection Result
`Installed version: 5.2.4`

... continues on next page ...

... continued from previous page ...

Fixed version: 5.2.8

Impact
Successful exploitation could allow attackers to inject arbitrary web script or HTML via unspecified vectors and conduct Cross-Site Scripting attacks.
Impact Level: Application

Solution
Solution type: VendorFix
Upgrade to version 5.2.8 or later http://www.php.net/downloads.php

Affected Software/OS
PHP version 5.2.7 and prior on all running platform.

Vulnerability Insight
The flaw is due to improper handling of certain inputs when display_errors settings is enabled.

Vulnerability Detection Method
Details:PHP display_errors Cross-Site Scripting Vulnerability
OID:1.3.6.1.4.1.25623.1.0.800334
Version used: $Revision: 4504 $

Product Detection Result
Product: cpe:/a:php:php:5.2.4
Method: PHP Version Detection (Remote)
OID: 1.3.6.1.4.1.25623.1.0.800109)

References
CVE: CVE-2008-5814
Other:
URL:http://jvn.jp/en/jp/JVN50327700/index.html
URL:http://jvndb.jvn.jp/en/contents/2008/JVNDB-2008-000084.html

[return to 192.168.8.102]

2.1.28 Log 6667/tcp

Log (CVSS: 0.0)
NVT: Identify unknown services with 'HELP'

Summary
This plugin performs service detection.
Description :
This plugin is a complement of find_service.nasl. It sends a HELP request to the remaining unknown services and tries to identify them.

... continues on next page ...

... continued from previous page ...

Vulnerability Detection Result
An IRC server seems to be running on this port

Log Method
Details:Identify unknown services with 'HELP'
OID:1.3.6.1.4.1.25623.1.0.11153
Version used: $Revision: 5284 $

Log (CVSS: 0.0)
NVT: IRC daemon identification

Summary
This script determines the version of the IRC daemon.

Vulnerability Detection Result
The IRC server version is : Unreal3.2.8.1. FhiXOoE [*=2309]

Log Method
Details:IRC daemon identification
OID:1.3.6.1.4.1.25623.1.0.11156
Version used: $Revision: 5433 $

Log (CVSS: 0.0)
NVT: UnrealIRCd Detection

Summary
Detection of UnrealIRCd Deamon. This script sends a request to the server and gets the version from the response.

Vulnerability Detection Result
Detected UnrealIRCd
Version: 3.2.8.1
Location: 6667/tcp
CPE: cpe:/a:unrealircd:unrealircd:3.2.8.1
Concluded from version/product identification result:
Unreal3.2.8.1

Log Method
Details:UnrealIRCd Detection
OID:1.3.6.1.4.1.25623.1.0.809884
Version used: $Revision: 5433 $

[return to 192.168.8.102]

2.1.29 Log general/CPE-T

Log (CVSS: 0.0) NVT: CPE Inventory
Summary This routine uses information collected by other routines about CPE identities (http://cpe.mitre.org/) of operating systems, services and applications detected during the scan.
Vulnerability Detection Result 192.168.8.102|cpe:/a:apache:http_server:2.2.8 192.168.8.102|cpe:/a:beasts:vsftpd:2.3.4 192.168.8.102|cpe:/a:isc:bind:9.4.2 192.168.8.102|cpe:/a:openbsd:openssh:4.7p1 192.168.8.102|cpe:/a:php:php:5.2.4 192.168.8.102|cpe:/a:phpmyadmin:phpmyadmin:3.1.1 192.168.8.102|cpe:/a:postgresql:postgresql:8.3.1 192.168.8.102|cpe:/a:samba:samba:3.0.20 192.168.8.102|cpe:/a:tiki:tikiwiki_cms/groupware:1.9.5 192.168.8.102|cpe:/a:twiki:twiki:01.Feb.2003 192.168.8.102|cpe:/a:unrealircd:unrealircd:3.2.8.1 192.168.8.102|cpe:/a:x.org:x11:11.0 192.168.8.102|cpe:/o:canonical:ubuntu_linux:8.04
Log Method Details:CPE Inventory OID:1.3.6.1.4.1.25623.1.0.810002 Version used: $Revision: 5458 $

[return to 192.168.8.102]

2.1.30 Log 5432/tcp

Log (CVSS: 0.0) NVT: Database Open Access Vulnerability
Summary The host is running a Database server and is prone to information disclosure vulnerability.
Vulnerability Detection Result Postgresql database can be accessed by remote attackers
Impact Successful exploitation could allow an attacker to obtain the sensitive information of the database. Impact Level: Application

. . . continues on next page . . .

... continued from previous page ...

Solution
Solution type: Workaround
Restrict Database access to remote systems.

Affected Software/OS
MySQL IBM DB2 PostgreSQL IBM solidDB Oracle Database Microsoft SQL Server

Vulnerability Insight
Do not restricting direct access of databases to the remote systems.

Log Method
Details:`Database Open Access Vulnerability`
OID:1.3.6.1.4.1.25623.1.0.902799
Version used: `$Revision: 5988 $`

References
```
Other:
  URL:https://www.pcisecuritystandards.org/security_standards/index.php?id=pci_d
↪ss_v1-2.pdf
```

Log (CVSS: 0.0)
NVT: PostgreSQL Detection

Summary
Detection of PostgreSQL, a open source object-relational database system (http://www.postgresql.org).
The script sends a connection request to the server (user:postgres, DB:postgres) and attempts to extract the version number from the reply.

Vulnerability Detection Result
```
Detected PostgreSQL
Version:  8.3.1
Location: 5432/tcp
CPE:      cpe:/a:postgresql:postgresql:8.3.1
Concluded from version/product identification result:
8.3.1
```

Log Method
Details:`PostgreSQL Detection`
OID:1.3.6.1.4.1.25623.1.0.100151
Version used: `$Revision: 4688 $`

... continues on next page ...

... continued from previous page ...

Log (CVSS: 0.0)
NVT: PostgreSQL TLS Detection

Summary
The remote PostgreSQL Server supports TLS.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Log Method
Details:`PostgreSQL TLS Detection`
OID:1.3.6.1.4.1.25623.1.0.105013
Version used: `$Revision: 4682 $`

Log (CVSS: 0.0)
NVT: Services

Summary
This routine attempts to guess which service is running on the remote ports. For instance, it searches for a web server which could listen on another port than 80 or 443 and makes this information available for other check routines.

Vulnerability Detection Result
```
An unknown service is running on this port.
It is usually reserved for Postgres
```

Log Method
Details:`Services`
OID:1.3.6.1.4.1.25623.1.0.10330
Version used: `$Revision: 5180 $`

Log (CVSS: 0.0)
NVT: SSL/TLS: Certificate - Self-Signed Certificate Detection

Summary
The SSL/TLS certificate on this port is self-signed.

Vulnerability Detection Result
```
The certificate of the remote service is self signed.
Certificate details:
subject ...: 1.2.840.113549.1.9.1=#726F6F74407562756E74753830342D626173652E6C6F6
↪3616C646F6D61696E,CN=ubuntu804-base.localdomain,OU=Office for Complication of
↪Otherwise Simple Affairs,O=OCOSA,L=Everywhere,ST=There is no such thing outsid
↪e US,C=XX
```

... continues on next page ...

... continued from previous page ...

```
subject alternative names (SAN):
None
issued by .: 1.2.840.113549.1.9.1=#726F6F74407562756E74753830342D626173652E6C6F6
↪3616C646F6D61696E,CN=ubuntu804-base.localdomain,OU=Office for Complication of
↪Otherwise Simple Affairs,O=OCOSA,L=Everywhere,ST=There is no such thing outsid
↪e US,C=XX
serial ....: 00FAF93A4C7FB6B9CC
valid from : 2010-03-17 14:07:45 UTC
valid until: 2010-04-16 14:07:45 UTC
fingerprint (SHA-1): ED093088706603BFD5DC237399B498DA2D4D31C6
fingerprint (SHA-256): E7A7FA0D63E457C7C4A59B38B70849C6A70BDA6F830C7AF1E32DEE436
↪DE813CC
```

Log Method

Details:SSL/TLS: Certificate - Self-Signed Certificate Detection
OID:1.3.6.1.4.1.25623.1.0.103140
Version used: $Revision: 4765 $

References

```
Other:
  URL:http://en.wikipedia.org/wiki/Self-signed_certificate
```

Log (CVSS: 0.0)
NVT: SSL/TLS: Collect and Report Certificate Details

Summary

This script collects and reports the details of all SSL/TLS certificates.
This data will be used by other tests to verify server certificates.

Vulnerability Detection Result

```
The following certificate details of the remote service were collected.
Certificate details:
subject ...: 1.2.840.113549.1.9.1=#726F6F74407562756E74753830342D626173652E6C6F6
↪3616C646F6D61696E,CN=ubuntu804-base.localdomain,OU=Office for Complication of
↪Otherwise Simple Affairs,O=OCOSA,L=Everywhere,ST=There is no such thing outsid
↪e US,C=XX
subject alternative names (SAN):
None
issued by .: 1.2.840.113549.1.9.1=#726F6F74407562756E74753830342D626173652E6C6F6
↪3616C646F6D61696E,CN=ubuntu804-base.localdomain,OU=Office for Complication of
↪Otherwise Simple Affairs,O=OCOSA,L=Everywhere,ST=There is no such thing outsid
↪e US,C=XX
serial ....: 00FAF93A4C7FB6B9CC
valid from : 2010-03-17 14:07:45 UTC
valid until: 2010-04-16 14:07:45 UTC
fingerprint (SHA-1): ED093088706603BFD5DC237399B498DA2D4D31C6
fingerprint (SHA-256): E7A7FA0D63E457C7C4A59B38B70849C6A70BDA6F830C7AF1E32DEE436
```

... continues on next page ...

... continued from previous page ...

↪DE813CC

Log Method
Details:SSL/TLS: Collect and Report Certificate Details
OID:1.3.6.1.4.1.25623.1.0.103692
Version used: $Revision: 4768 $

Log (CVSS: 0.0)
NVT: SSL/TLS: Report Medium Cipher Suites

Summary
This routine reports all Medium SSL/TLS cipher suites accepted by a service.

Vulnerability Detection Result
'Medium' cipher suites accepted by this service via the SSLv3 protocol:
TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA
TLS_DHE_RSA_WITH_AES_128_CBC_SHA
TLS_RSA_WITH_3DES_EDE_CBC_SHA
TLS_RSA_WITH_AES_128_CBC_SHA
TLS_RSA_WITH_AES_256_CBC_SHA
'Medium' cipher suites accepted by this service via the TLSv1.0 protocol:
TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA
TLS_DHE_RSA_WITH_AES_128_CBC_SHA
TLS_RSA_WITH_3DES_EDE_CBC_SHA
TLS_RSA_WITH_AES_128_CBC_SHA
TLS_RSA_WITH_AES_256_CBC_SHA

Vulnerability Insight
Any cipher suite considered to be secure for only the next 10 years is considered as medium

Log Method
Details:SSL/TLS: Report Medium Cipher Suites
OID:1.3.6.1.4.1.25623.1.0.902816
Version used: $Revision: 4743 $

Log (CVSS: 0.0)
NVT: SSL/TLS: Report Non Weak Cipher Suites

Summary
This routine reports all Non Weak SSL/TLS cipher suites accepted by a service.

Vulnerability Detection Result
'Non Weak' cipher suites accepted by this service via the SSLv3 protocol:
TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA
TLS_DHE_RSA_WITH_AES_128_CBC_SHA

... continues on next page ...

... continued from previous page ...

```
TLS_DHE_RSA_WITH_AES_256_CBC_SHA
TLS_RSA_WITH_3DES_EDE_CBC_SHA
TLS_RSA_WITH_AES_128_CBC_SHA
TLS_RSA_WITH_AES_256_CBC_SHA
'Non Weak' cipher suites accepted by this service via the TLSv1.0 protocol:
TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA
TLS_DHE_RSA_WITH_AES_128_CBC_SHA
TLS_DHE_RSA_WITH_AES_256_CBC_SHA
TLS_RSA_WITH_3DES_EDE_CBC_SHA
TLS_RSA_WITH_AES_128_CBC_SHA
TLS_RSA_WITH_AES_256_CBC_SHA
```

Log Method
Details:SSL/TLS: Report Non Weak Cipher Suites
OID:1.3.6.1.4.1.25623.1.0.103441
Version used: $Revision: 4736 $

Log (CVSS: 0.0)
NVT: SSL/TLS: Report Perfect Forward Secrecy (PFS) Cipher Suites

Summary
This routine reports all SSL/TLS cipher suites accepted by a service which are supporting Perfect Forward Secrecy (PFS).

Vulnerability Detection Result

```
Cipher suites supporting Perfect Forward Secrecy (PFS) are accepted by this serv
↪ice via the SSLv3 protocol:
TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA
TLS_DHE_RSA_WITH_AES_128_CBC_SHA
TLS_DHE_RSA_WITH_AES_256_CBC_SHA
Cipher suites supporting Perfect Forward Secrecy (PFS) are accepted by this serv
↪ice via the TLSv1.0 protocol:
TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA
TLS_DHE_RSA_WITH_AES_128_CBC_SHA
TLS_DHE_RSA_WITH_AES_256_CBC_SHA
```

Log Method
Details:SSL/TLS: Report Perfect Forward Secrecy (PFS) Cipher Suites
OID:1.3.6.1.4.1.25623.1.0.105018
Version used: $Revision: 4771 $

Log (CVSS: 0.0)
NVT: SSL/TLS: Report Supported Cipher Suites

Summary

... continues on next page ...

... continued from previous page ...

This routine reports all SSL/TLS cipher suites accepted by a service.
As the NVT 'SSL/TLS: Check Supported Cipher Suites' (OID: 1.3.6.1.4.1.25623.1.0.900234) might run into a timeout the actual reporting of all accepted cipher suites takes place in this NVT instead. The script preference 'Report timeout' allows you to configure if such an timeout is reported.

Vulnerability Detection Result

```
'Strong' cipher suites accepted by this service via the SSLv3 protocol:
TLS_DHE_RSA_WITH_AES_256_CBC_SHA
'Medium' cipher suites accepted by this service via the SSLv3 protocol:
TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA
TLS_DHE_RSA_WITH_AES_128_CBC_SHA
TLS_RSA_WITH_3DES_EDE_CBC_SHA
TLS_RSA_WITH_AES_128_CBC_SHA
TLS_RSA_WITH_AES_256_CBC_SHA
'Weak' cipher suites accepted by this service via the SSLv3 protocol:
TLS_RSA_WITH_RC4_128_SHA
No 'Null' cipher suites accepted by this service via the SSLv3 protocol.
No 'Anonymous' cipher suites accepted by this service via the SSLv3 protocol.
'Strong' cipher suites accepted by this service via the TLSv1.0 protocol:
TLS_DHE_RSA_WITH_AES_256_CBC_SHA
'Medium' cipher suites accepted by this service via the TLSv1.0 protocol:
TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA
TLS_DHE_RSA_WITH_AES_128_CBC_SHA
TLS_RSA_WITH_3DES_EDE_CBC_SHA
TLS_RSA_WITH_AES_128_CBC_SHA
TLS_RSA_WITH_AES_256_CBC_SHA
'Weak' cipher suites accepted by this service via the TLSv1.0 protocol:
TLS_RSA_WITH_RC4_128_SHA
No 'Null' cipher suites accepted by this service via the TLSv1.0 protocol.
No 'Anonymous' cipher suites accepted by this service via the TLSv1.0 protocol.
```

Log Method

Details:SSL/TLS: Report Supported Cipher Suites
OID:1.3.6.1.4.1.25623.1.0.802067
Version used: $Revision: 5987 $

[return to 192.168.8.102]

2.1.31 Log 2121/tcp

Log (CVSS: 0.0)
NVT: Identify Unknown Services with nmap

Summary

... continues on next page ...

... continued from previous page ...

This plugin performs service detection by launching nmap's service probe (nmap -sV) against ports that are running unidentified services.

Vulnerability Detection Result

```
Nmap service detection result for this port: ccproxy-ftp
This is a guess. A confident identification of the service was not possible.
```

Log Method

Details:`Identify Unknown Services with nmap`
OID:1.3.6.1.4.1.25623.1.0.66286
Version used: `$Revision: 5296 $`

[return to 192.168.8.102]

2.1.32 Log 22/tcp

Log (CVSS: 0.0)
NVT: Services

Summary

This routine attempts to guess which service is running on the remote ports. For instance, it searches for a web server which could listen on another port than 80 or 443 and makes this information available for other check routines.

Vulnerability Detection Result

```
An ssh server is running on this port
```

Log Method

Details:`Services`
OID:1.3.6.1.4.1.25623.1.0.10330
Version used: `$Revision: 5180 $`

Log (CVSS: 0.0)
NVT: SSH Protocol Algorithms Supported

Summary

This script detects which algorithms and languages are supported by the remote SSH Service

Vulnerability Detection Result

```
The following options are supported by the remote ssh service:
kex_algorithms:
diffie-hellman-group-exchange-sha256,diffie-hellman-group-exchange-sha1,diffie-h
↪ellman-group14-sha1,diffie-hellman-group1-sha1
server_host_key_algorithms:
ssh-rsa,ssh-dss
```

... continues on next page ...

... continued from previous page ...

```
encryption_algorithms_client_to_server:
aes128-cbc,3des-cbc,blowfish-cbc,cast128-cbc,arcfour128,arcfour256,arcfour,aes19
↪2-cbc,aes256-cbc,rijndael-cbc@lysator.liu.se,aes128-ctr,aes192-ctr,aes256-ctr
encryption_algorithms_server_to_client:
aes128-cbc,3des-cbc,blowfish-cbc,cast128-cbc,arcfour128,arcfour256,arcfour,aes19
↪2-cbc,aes256-cbc,rijndael-cbc@lysator.liu.se,aes128-ctr,aes192-ctr,aes256-ctr
mac_algorithms_client_to_server:
hmac-md5,hmac-sha1,umac-64@openssh.com,hmac-ripemd160,hmac-ripemd160@openssh.com
↪,hmac-sha1-96,hmac-md5-96
mac_algorithms_server_to_client:
hmac-md5,hmac-sha1,umac-64@openssh.com,hmac-ripemd160,hmac-ripemd160@openssh.com
↪,hmac-sha1-96,hmac-md5-96
compression_algorithms_client_to_server:
none,zlib@openssh.com
compression_algorithms_server_to_client:
none,zlib@openssh.com
```

Log Method
Details:SSH Protocol Algorithms Supported
OID:1.3.6.1.4.1.25623.1.0.105565
Version used: $Revision: 2828 $

Log (CVSS: 0.0)
NVT: SSH Protocol Versions Supported

Summary
Identification of SSH protocol versions supported by the remote SSH Server. Also reads the corresponding fingerprints from the service.
The following versions are tried: 1.33, 1.5, 1.99 and 2.0

Vulnerability Detection Result

```
The remote SSH Server supports the following SSH Protocol Versions:
1.99
2.0
SSHv2 Fingerprint:
ssh-dss: 60:0f:cf:e1:c0:5f:6a:74:d6:90:24:fa:c4:d5:6c:cd
ssh-rsa: 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3
```

Log Method
Details:SSH Protocol Versions Supported
OID:1.3.6.1.4.1.25623.1.0.100259
Version used: $Revision: 4484 $

... continues on next page ...

... continued from previous page ...

Log (CVSS: 0.0)
NVT: SSH Server type and version

Summary
This detects the SSH Server's type and version by connecting to the server and processing the buffer received.
This information gives potential attackers additional information about the system they are attacking. Versions and Types should be omitted where possible.

Vulnerability Detection Result
```
Detected SSH server version: SSH-2.0-OpenSSH_4.7p1 Debian-8ubuntu1
Remote SSH supported authentication: none,password,publickey,hostbased,keyboard-
↪interactive
Remote SSH banner:
(not available)
CPE: cpe:/a:openbsd:openssh:4.7p1
Concluded from remote connection attempt with credentials:
  Login: VulnScan
  Password: VulnScan
```

Log Method
Details:`SSH Server type and version`
OID:1.3.6.1.4.1.25623.1.0.10267
Version used: `$Revision: 4947 $`

[return to 192.168.8.102]

2.1.33 Log 512/tcp

Log (CVSS: 0.0)
NVT: Identify Unknown Services with nmap

Summary
This plugin performs service detection by launching nmap's service probe (nmap -sV) against ports that are running unidentified services.

Vulnerability Detection Result
```
Nmap service detection result for this port: exec
This is a guess. A confident identification of the service was not possible.
```

Log Method
Details:`Identify Unknown Services with nmap`
OID:1.3.6.1.4.1.25623.1.0.66286
Version used: `$Revision: 5296 $`

[return to 192.168.8.102]

2.1.34 Log 8787/tcp

Log (CVSS: 0.0)
NVT: Identify unknown services with 'GET'

Summary
This plugin performs service detection.
This plugin is a complement of find_service.nasl. It sends a GET request to the remaining unknown services and tries to identify them.

Vulnerability Detection Result
`A Distributed Ruby (dRuby/DRb) service seems to be running on this port.`

Log Method
Details:`Identify unknown services with 'GET'`
OID:1.3.6.1.4.1.25623.1.0.17975
Version used: `$Revision: 5482 $`

[return to 192.168.8.102]

2.1.35 Log 8009/tcp

Log (CVSS: 0.0)
NVT: Apache JServ Protocol v1.3 Detection

Summary
The script detects a service running the Apache JServ Protocol version 1.3.

Vulnerability Detection Result
`A service supporting the Apache JServ Protocol v1.3 seems to be running on this ↪port.`

Log Method
Details:`Apache JServ Protocol v1.3 Detection`
OID:1.3.6.1.4.1.25623.1.0.108082
Version used: `$Revision: 5264 $`

[return to 192.168.8.102]

2.1.36 Log 3306/tcp

Log (CVSS: 0.0)
NVT: Identify Unknown Services with nmap

Summary
This plugin performs service detection by launching nmap's service probe (nmap -sV) against ports that are running unidentified services.

Vulnerability Detection Result
`Nmap service detection result for this port: mysql`
`This is a guess. A confident identification of the service was not possible.`

Log Method
Details:`Identify Unknown Services with nmap`
OID:1.3.6.1.4.1.25623.1.0.66286
Version used: `$Revision: 5296 $`

Log (CVSS: 0.0)
NVT: Services

Summary
This routine attempts to guess which service is running on the remote ports. For instance, it searches for a web server which could listen on another port than 80 or 443 and makes this information available for other check routines.

Vulnerability Detection Result
`An unknown service is running on this port.`
`It is usually reserved for MySQL`

Log Method
Details:`Services`
OID:1.3.6.1.4.1.25623.1.0.10330
Version used: `$Revision: 5180 $`

[return to 192.168.8.102]

2.1.37 Log 5900/tcp

Log (CVSS: 0.0)
NVT: VNC security types

Summary
This script checks the remote VNC protocol version and the available 'security types'.

Vulnerability Detection Result
`The remote VNC server chose security type #2 (VNC authentication)`

... continues on next page ...

... continued from previous page ...

Log Method
Details:`VNC security types`
OID:1.3.6.1.4.1.25623.1.0.19288
Version used: `$Revision: 4469 $`

Log (CVSS: 0.0)
NVT: VNC Server and Protocol Version Detection

Summary
The remote host is running a remote display software (VNC) which permits a console to be displayed remotely.
This allows authenticated users of the remote host to take its control remotely.

Vulnerability Detection Result
```
A VNC server seems to be running on this port.
The version of the VNC protocol is : RFB 003.003
```

Solution
Make sure the use of this software is done in accordance with your corporate security policy, filter incoming traffic to this port.

Log Method
Details:`VNC Server and Protocol Version Detection`
OID:1.3.6.1.4.1.25623.1.0.10342
Version used: `$Revision: 4944 $`

[return to 192.168.8.102]

2.1.38 Log 6000/tcp

Log (CVSS: 0.0)
NVT: Identify Unknown Services with nmap

Summary
This plugin performs service detection by launching nmap's service probe (nmap -sV) against ports that are running unidentified services.

Vulnerability Detection Result
```
Nmap service detection result for this port: X11
```

Log Method
Details:`Identify Unknown Services with nmap`
OID:1.3.6.1.4.1.25623.1.0.66286
Version used: `$Revision: 5296 $`

[return to 192.168.8.102]

2.1.39 Log 23/tcp

Log (CVSS: 0.0)
NVT: Services

Summary
This routine attempts to guess which service is running on the remote ports. For instance, it searches for a web server which could listen on another port than 80 or 443 and makes this information available for other check routines.

Vulnerability Detection Result
```
An unknown service is running on this port.
It is usually reserved for Telnet
```

Log Method
Details:`Services`
OID:1.3.6.1.4.1.25623.1.0.10330
Version used: `$Revision: 5180 $`

[return to 192.168.8.102]

2.1.40 Log 513/tcp

Log (CVSS: 0.0)
NVT: Identify Unknown Services with nmap

Summary
This plugin performs service detection by launching nmap's service probe (nmap -sV) against ports that are running unidentified services.

Vulnerability Detection Result
```
Nmap service detection result for this port: login
This is a guess. A confident identification of the service was not possible.
```

Log Method
Details:`Identify Unknown Services with nmap`
OID:1.3.6.1.4.1.25623.1.0.66286
Version used: `$Revision: 5296 $`

[return to 192.168.8.102]

2.1.41 Log general/tcp

Log (CVSS: 0.0)
NVT: OS Detection Consolidation and Reporting

Summary
This script consolidates the OS information detected by several NVTs and tries to find the best matching OS.
Furthermore it reports all previously collected information leading to this best matching OS. It also reports possible additional informations which might help to improve the OS detection.
If any of this information is wrong or could be improved please consider to report these to openvas-plugins@wald.intevation.org.

Vulnerability Detection Result

```
Best matching OS:
OS: Ubuntu 8.04
Version: 8.04
CPE: cpe:/o:canonical:ubuntu_linux:8.04
Found by NVT: 1.3.6.1.4.1.25623.1.0.105586 (SSH OS Identification)
Concluded from SSH banner on port 22/tcp: SSH-2.0-OpenSSH_4.7p1 Debian-8ubuntu1
Setting key "Host/runs_unixoide" based on this information
Other OS detections (in order of reliability):
OS: Linux
CPE: cpe:/o:linux:kernel
Found by NVT: 1.3.6.1.4.1.25623.1.0.105355 (FTP OS Identification)
Concluded from FTP banner on port 21/tcp: 220 (vsFTPd 2.3.4)
OS: Debian GNU/Linux
CPE: cpe:/o:debian:debian_linux
Found by NVT: 1.3.6.1.4.1.25623.1.0.102011 (SMB NativeLanMan)
Concluded from SMB/Samba banner on port 445/tcp: OS String: Debian GNU/Linux; SM
↪B String: Samba 3.0.20-Debian
OS: Ubuntu
CPE: cpe:/o:canonical:ubuntu_linux
Found by NVT: 1.3.6.1.4.1.25623.1.0.111067 (HTTP OS Identification)
Concluded from HTTP Server banner on port 80/tcp: Server: Apache/2.2.8 (Ubuntu)
↪DAV/2
OS: Linux 2.6.9 - 2.6.33
CPE: cpe:/o:linux:linux_kernel:2.6
Found by NVT: 1.3.6.1.4.1.25623.1.0.108021 (Nmap OS Identification (NASL wrapper
↪))
Concluded from Nmap TCP/IP fingerprinting:
OS details: Linux 2.6.9 - 2.6.33
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS: Linux Kernel
CPE: cpe:/o:linux:kernel
Found by NVT: 1.3.6.1.4.1.25623.1.0.102002 (ICMP based OS Fingerprinting)
Concluded from ICMP based OS fingerprint:
(100% confidence)
Linux Kernel
```

. . . continues on next page . . .

. . . continued from previous page . . .

Log Method
Details:OS Detection Consolidation and Reporting
OID:1.3.6.1.4.1.25623.1.0.105937
Version used: $Revision: 5435 $

Log (CVSS: 0.0)
NVT: SSL/TLS: Hostname discovery from server certificate

Summary
It was possible to discover an additional hostname of this server from its certificate Common or Subject Alt Name.

Vulnerability Detection Result
The following additional but not resolvable hostnames were detected:
ubuntu804-base.localdomain

Log Method
Details:SSL/TLS: Hostname discovery from server certificate
OID:1.3.6.1.4.1.25623.1.0.111010
Version used: $Revision: 5180 $

Log (CVSS: 0.0)
NVT: Traceroute

Summary
A traceroute from the scanning server to the target system was conducted. This traceroute is provided primarily for informational value only. In the vast majority of cases, it does not represent a vulnerability. However, if the displayed traceroute contains any private addresses that should not have been publicly visible, then you have an issue you need to correct.

Vulnerability Detection Result
Here is the route from 192.168.8.101 to 192.168.8.102:
192.168.8.101
192.168.8.102

Solution
Block unwanted packets from escaping your network.

Log Method
Details:Traceroute
OID:1.3.6.1.4.1.25623.1.0.51662
Version used: $Revision: 5390 $

Log (CVSS: 10.0)
NVT: X Server

Summary
This plugin detects X Window servers.
X11 is a client - server protocol. Basically, the server is in charge of the screen, and the clients connect to it and send several requests like drawing a window or a menu, and the server sends events back to the clients, such as mouse clicks, key strokes, and so on...
An improperly configured X server will accept connections from clients from anywhere. This allows an attacker to make a client connect to the X server to record the keystrokes of the user, which may contain sensitive information, such as account passwords. This can be prevented by using xauth, MIT cookies, or preventing the X server from listening on TCP (a Unix sock is used for local connections)

Vulnerability Detection Result
```
Detected X Windows Server
Version:  11.0
Location: undefined
CPE:      cpe:/a:x.org:x11:11.0
Concluded from version/product identification result:
11.0
```

Vulnerability Detection Method
Details:`X Server`
OID:1.3.6.1.4.1.25623.1.0.10407
Version used: `$Revision: 5943 $`

References
`CVE: CVE-1999-0526`

[return to 192.168.8.102]

2.1.42 Log 111/tcp

Log (CVSS: 0.0)
NVT: Obtain list of all port mapper registered programs via RPC

Summary
This script calls the DUMP RPC on the port mapper, to obtain the list of all registered programs.

Vulnerability Detection Result
```
These are the registered RPC programs:
RPC program #100000 version 2 'portmapper' (portmap sunrpc rpcbind) on port 111/
↪TCP
RPC program #100003 version 2 'nfs' (nfsprog) on port 2049/TCP
RPC program #100003 version 3 'nfs' (nfsprog) on port 2049/TCP
RPC program #100003 version 4 'nfs' (nfsprog) on port 2049/TCP
```

... continues on next page ...

... continued from previous page ...

```
RPC program #100005 version 1 'mountd' (mount showmount) on port 41000/TCP
RPC program #100005 version 2 'mountd' (mount showmount) on port 41000/TCP
RPC program #100005 version 3 'mountd' (mount showmount) on port 41000/TCP
RPC program #100021 version 1 'nlockmgr' on port 46525/TCP
RPC program #100021 version 3 'nlockmgr' on port 46525/TCP
RPC program #100021 version 4 'nlockmgr' on port 46525/TCP
RPC program #100024 version 1 'status' on port 49412/TCP
RPC program #100000 version 2 'portmapper' (portmap sunrpc rpcbind) on port 111/
↪UDP
RPC program #100003 version 2 'nfs' (nfsprog) on port 2049/UDP
RPC program #100003 version 3 'nfs' (nfsprog) on port 2049/UDP
RPC program #100003 version 4 'nfs' (nfsprog) on port 2049/UDP
RPC program #100005 version 1 'mountd' (mount showmount) on port 48749/UDP
RPC program #100005 version 2 'mountd' (mount showmount) on port 48749/UDP
RPC program #100005 version 3 'mountd' (mount showmount) on port 48749/UDP
RPC program #100024 version 1 'status' on port 54573/UDP
RPC program #100021 version 1 'nlockmgr' on port 58344/UDP
RPC program #100021 version 3 'nlockmgr' on port 58344/UDP
RPC program #100021 version 4 'nlockmgr' on port 58344/UDP
```

Log Method
Details:`Obtain list of all port mapper registered programs via RPC`
OID:1.3.6.1.4.1.25623.1.0.11111
Version used: `$Revision: 4827 $`

Log (CVSS: 0.0)
NVT: RPC portmapper (TCP)

Summary
This script performs detection of RPC portmapper on TCP.

Vulnerability Detection Result
`RPC portmapper is running on this port`

Log Method
Details:`RPC portmapper (TCP)`
OID:1.3.6.1.4.1.25623.1.0.108090
Version used: `$Revision: 5487 $`

[return to 192.168.8.102]

2.1.43 Log 445/tcp

Log (CVSS: 0.0)
NVT: Microsoft SMB Signing Disabled

Summary
Checking for SMB signing is disabled.
The script logs in via smb, checks the SMB Negotiate Protocol response to confirm SMB signing is disabled.

Vulnerability Detection Result
`SMB signing is disabled on this host`

Log Method
Details:`Microsoft SMB Signing Disabled`
OID:1.3.6.1.4.1.25623.1.0.802726
Version used: `$Revision: 5958 $`

Log (CVSS: 0.0)
NVT: Microsoft Windows SMB Accessible Shares

Summary
The script detects the Windows SMB Accessible Shares and sets the result into KB.

Vulnerability Detection Result
`The following shares were found`
`IPC$`

Log Method
Details:`Microsoft Windows SMB Accessible Shares`
OID:1.3.6.1.4.1.25623.1.0.902425
Version used: `$Revision: 5336 $`

Log (CVSS: 0.0)
NVT: SMB log in

Summary
This script attempts to logon into the remote host using login/password credentials.

Vulnerability Detection Result
`It was possible to log into the remote host using the SMB protocol.`

Log Method
Details:`SMB log in`
OID:1.3.6.1.4.1.25623.1.0.10394
Version used: `$Revision: 5336 $`

Log (CVSS: 0.0)
NVT: SMB NativeLanMan

Summary
It is possible to extract OS, domain and SMB server information from the Session Setup AndX Response packet which is generated during NTLM authentication.

Vulnerability Detection Result
```
Detected Samba
Version:  3.0.20
Location: 445/tcp
CPE:      cpe:/a:samba:samba:3.0.20
Concluded from version/product identification result:
Samba 3.0.20-Debian
Detected SMB workgroup: WORKGROUP
Detected SMB server: Samba 3.0.20-Debian
```

Log Method
Details:`SMB NativeLanMan`
OID:1.3.6.1.4.1.25623.1.0.102011
Version used: `$Revision: 5924 $`

Log (CVSS: 0.0)
NVT: SMB NativeLanMan

Summary
It is possible to extract OS, domain and SMB server information from the Session Setup AndX Response packet which is generated during NTLM authentication.

Vulnerability Detection Result
```
Detected SMB workgroup: WORKGROUP
Detected SMB server: Samba 3.0.20-Debian
Detected OS: Debian GNU/Linux
```

Log Method
Details:`SMB NativeLanMan`
OID:1.3.6.1.4.1.25623.1.0.102011
Version used: `$Revision: 5924 $`

Log (CVSS: 0.0)
NVT: SMB Remote Version Detection

Summary
Detection of Server Message Block(SMB).
This script sends SMB Negotiation request and try to get the version from the response.

. . . continues on next page . . .

... continued from previous page ...

Vulnerability Detection Result
`Only SMBv1 is enabled on remote target`

Log Method
Details:`SMB Remote Version Detection`
OID:1.3.6.1.4.1.25623.1.0.807830
Version used: `$Revision: 5438 $`

Log (CVSS: 0.0)
NVT: SMB Test with 'smbclient'

Summary
This script tests the remote host SMB Functions with the 'smbclient' tool.

Vulnerability Detection Result
```
OS Version = UNIX
Domain = WORKGROUP
SMB Serverversion = SAMBA 3.0.20-DEBIAN
```

Log Method
Details:`SMB Test with 'smbclient'`
OID:1.3.6.1.4.1.25623.1.0.90011
Version used: `$Revision: 5260 $`

Log (CVSS: 0.0)
NVT: SMB/CIFS Server Detection

Summary
This script detects wether port 445 and 139 are open and if they are running a CIFS/SMB server.

Vulnerability Detection Result
`A CIFS server is running on this port`

Log Method
Details:`SMB/CIFS Server Detection`
OID:1.3.6.1.4.1.25623.1.0.11011
Version used: `$Revision: 4261 $`

[return to 192.168.8.102]

2.1.44 Log 1524/tcp

Log (CVSS: 0.0)
NVT: Check for Telnet Server

Summary
A telnet Server is running at this host.
Experts in computer security, such as SANS Institute, and the members of the comp.os.linux.security newsgroup recommend that the use of Telnet for remote logins should be discontinued under all normal circumstances, for the following reasons:
Telnet, by default, does not encrypt any data sent over the connection (including passwords), and so it is often practical to eavesdrop on the communications and use the password later for malicious purposes anybody who has access to a router, switch, hub or gateway located on the network between the two hosts where Telnet is being used can intercept the packets passing by and obtain login and password information (and whatever else is typed) with any of several common utilities like tcpdump and Wireshark.
Most implementations of Telnet have no authentication that would ensure communication is carried out between the two desired hosts and not intercepted in the middle.
Commonly used Telnet daemons have several vulnerabilities discovered over the years.

Vulnerability Detection Result
`A telnet server seems to be running on this port`

Log Method
Details:`Check for Telnet Server`
OID:1.3.6.1.4.1.25623.1.0.100074
Version used: `$Revision: 5273 $`

Log (CVSS: 0.0)
NVT: Report Telnet Banner

Summary
This scripts reports the received banner of a Telnet Server.

Vulnerability Detection Result
```
Remote telnet banner :
root@metasploitable:/#
```

Impact
This information gives potential attackers additional information about the system they are attacking. Versions and Types should be omitted where possible.

Solution
Change the login banner to something generic.

Log Method
Details:`Report Telnet Banner`
OID:1.3.6.1.4.1.25623.1.0.10281
Version used: `$Revision: 4771 $`

[return to 192.168.8.102]

2.1.45 Log 21/tcp

Log (CVSS: 0.0)
NVT: FTP Banner Detection

Summary
This Plugin detects the FTP Server Banner and the Banner of the 'HELP' command.

Vulnerability Detection Result
```
Remote FTP server banner :
220 (vsFTPd 2.3.4)
```

Log Method
Details:`FTP Banner Detection`
OID:1.3.6.1.4.1.25623.1.0.10092
Version used: `$Revision: 4780 $`

Log (CVSS: 0.0)
NVT: Services

Summary
This routine attempts to guess which service is running on the remote ports. For instance, it searches for a web server which could listen on another port than 80 or 443 and makes this information available for other check routines.

Vulnerability Detection Result
```
An FTP server is running on this port.
Here is its banner :
220 (vsFTPd 2.3.4)
```

Log Method
Details:`Services`
OID:1.3.6.1.4.1.25623.1.0.10330
Version used: `$Revision: 5180 $`

Log (CVSS: 0.0)
NVT: vsFTPd FTP Server Detection

Summary
The script is grabbing the banner of a FTP server and attempts to identify a vsFTPd FTP Server and its version from the reply.

Vulnerability Detection Result

. . . continues on next page . . .

... continued from previous page ...

```
Detected vsFTPd
Version:  2.3.4
Location: 21/tcp
CPE:      cpe:/a:beasts:vsftpd:2.3.4
Concluded from version/product identification result:
220 (vsFTPd 2.3.4)
```

Log Method
Details:`vsFTPd FTP Server Detection`
OID:1.3.6.1.4.1.25623.1.0.111050
Version used: `$Revision: 4777 $`

[return to 192.168.8.102]

2.1.46 Log 53/tcp

Log (CVSS: 0.0)
NVT: Determine which version of BIND name daemon is running

Summary
BIND 'NAMED' is an open-source DNS server from ISC.org. Many proprietary DNS servers are based on BIND source code.

Vulnerability Detection Result

```
Detected Bind
Version:  9.4.2
Location: 53/tcp
CPE:      cpe:/a:isc:bind:9.4.2
Concluded from version/product identification result:
9.4.2
```

Solution
Using the 'version' directive in the 'options' section will block the 'version.bind' query, but it will not log such attempts.

Vulnerability Insight
The BIND based NAMED servers (or DNS servers) allow remote users to query for version and type information. The query of the CHAOS TXT record 'version.bind', will typically prompt the server to send the information back to the querying source.

Log Method
Details:`Determine which version of BIND name daemon is running`
OID:1.3.6.1.4.1.25623.1.0.10028
Version used: `$Revision: 5445 $`

Log (CVSS: 0.0)
NVT: DNS Server Detection (TCP)

Summary
A DNS Server is running at this Host. A Name Server translates domain names into IP addresses. This makes it possible for a user to access a website by typing in the domain name instead of the website's actual IP address.

Vulnerability Detection Result
`The remote DNS server banner is:`
`9.4.2`

Log Method
Details:`DNS Server Detection (TCP)`
OID:1.3.6.1.4.1.25623.1.0.108018
Version used: `$Revision: 4944 $`

[return to 192.168.8.102]

2.1.47 Log 514/tcp

Log (CVSS: 0.0)
NVT: Identify Unknown Services with nmap

Summary
This plugin performs service detection by launching nmap's service probe (nmap -sV) against ports that are running unidentified services.

Vulnerability Detection Result
`Nmap service detection result for this port: shell`
`This is a guess. A confident identification of the service was not possible.`

Log Method
Details:`Identify Unknown Services with nmap`
OID:1.3.6.1.4.1.25623.1.0.66286
Version used: `$Revision: 5296 $`

[return to 192.168.8.102]

2.1.48 Log 80/tcp

Log (CVSS: 0.0)
NVT: Apache Web Server Version Detection

Summary

. . . continues on next page . . .

... continued from previous page ...

Detection of installed version of Apache Web Server
The script detects the version of Apache HTTP Server on remote host and sets the KB.

Vulnerability Detection Result

```
Detected Apache
Version:  2.2.8
Location: 80/tcp
CPE:      cpe:/a:apache:http_server:2.2.8
Concluded from version/product identification result:
Server: Apache/2.2.8
```

Log Method

Details:`Apache Web Server Version Detection`
OID:1.3.6.1.4.1.25623.1.0.900498
Version used: `$Revision: 4249 $`

Log (CVSS: 0.0)
NVT: CGI Scanning Consolidation

Summary

The script consolidates various information for CGI scanning.
This information is based on the following scripts / settings:
- Web mirroring / webmirror.nasl (OID: 1.3.6.1.4.1.25623.1.0.10662)
- Directory Scanner / DDI_Directory_Scanner.nasl (OID: 1.3.6.1.4.1.25623.1.0.11032)
- The configured 'cgi_path' within the 'Scanner Preferences' of the scan config in use

Vulnerability Detection Result

```
The host seems to be able to host PHP scripts.
The host seems to be NOT able to host ASP scripts.
The following directories were used for CGI scanning:
http://192.168.8.102/
http://192.168.8.102/cgi-bin
http://192.168.8.102/dav
http://192.168.8.102/doc
http://192.168.8.102/dvwa
http://192.168.8.102/mutillidae
http://192.168.8.102/mutillidae/documentation
http://192.168.8.102/oops/TWiki
http://192.168.8.102/phpMyAdmin
http://192.168.8.102/rdiff/TWiki
http://192.168.8.102/scripts
http://192.168.8.102/test
http://192.168.8.102/test/testoutput
http://192.168.8.102/twiki
http://192.168.8.102/twiki/pub
http://192.168.8.102/twiki/pub/TWiki/FileAttachment
http://192.168.8.102/twiki/pub/TWiki/TWikiDocGraphics
```

... continues on next page ...

... continued from previous page ...

```
http://192.168.8.102/twiki/pub/TWiki/TWikiLogos
http://192.168.8.102/twiki/pub/TWiki/TWikiPreferences
http://192.168.8.102/twiki/pub/TWiki/TWikiTemplates
http://192.168.8.102/twiki/pub/icn
http://192.168.8.102/view/TWiki
While this is not, in and of itself, a bug, you should manually inspect these di
↪rectories to ensure that they are in compliance with company security standard
↪s
The following directories were excluded from CGI scanning because of the "Regex
↪pattern to exclude directories from CGI scanning" setting of the NVT "Global v
↪ariable settings" (OID: 1.3.6.1.4.1.25623.1.0.12288):
http://192.168.8.102/icons
http://192.168.8.102/mutillidae/images
http://192.168.8.102/mutillidae/javascript
http://192.168.8.102/mutillidae/javascript/ddsmoothmenu
http://192.168.8.102/mutillidae/styles
http://192.168.8.102/mutillidae/styles/ddsmoothmenu
http://192.168.8.102/phpMyAdmin/themes/original/img
Directory index found at:
http://192.168.8.102/dav/
http://192.168.8.102/mutillidae/documentation/
http://192.168.8.102/test/
http://192.168.8.102/test/testoutput/
http://192.168.8.102/twiki/TWikiDocumentation.html
http://192.168.8.102/twiki/bin/view/TWiki/TWikiDocumentation
http://192.168.8.102/twiki/bin/view/TWiki/TWikiInstallationGuide
The following CGIs were discovered:
Syntax : cginame (arguments [default value])
http://192.168.8.102/dav/ (C=S;O [A] C=N;O [D] C=M;O [A] C=D;O [A] )
http://192.168.8.102/mutillidae/ (page [add-to-your-blog.php] )
http://192.168.8.102/mutillidae/documentation/ (C=S;O [A] C=N;O [D] C=M;O [A] C=
↪D;O [A] )
http://192.168.8.102/mutillidae/index.php (username [anonymous] do [toggle-hints
↪] page [home.php] )
http://192.168.8.102/oops/TWiki/TWikiHistory (template [oopsrev] param1 [1.10] )
http://192.168.8.102/phpMyAdmin/index.php (pma_password [] token [17b2377f1c781d
↪a1c450c058b85dfaa5] pma_username [] convcharset [utf-8] table [] lang [] serve
↪r [1] db [] phpMyAdmin [0887cb09b0e02e597cbf176968151f38ed9ce431] )
http://192.168.8.102/phpMyAdmin/phpmyadmin.css.php (token [17b2377f1c781da1c450c
↪058b85dfaa5] convcharset [utf-8] js_frame [right] lang [en-utf-8] nocache [245
↪7687151] )
http://192.168.8.102/rdiff/TWiki/TWikiHistory (rev1 [1.10] rev2 [1.9] )
http://192.168.8.102/test/ (C=S;O [A] C=N;O [D] C=M;O [A] C=D;O [A] )
http://192.168.8.102/test/testoutput/ (C=S;O [A] C=N;O [D] C=M;O [A] C=D;O [A] )
http://192.168.8.102/twiki/bin/attach/TWiki/FileAttachment (filename [Sample.txt
↪] revInfo [1] )
http://192.168.8.102/twiki/bin/edit/Know/ReadmeFirst (t [1494445996] )
```

... continues on next page ...

... continued from previous page ...

```
http://192.168.8.102/twiki/bin/edit/Know/WebChanges (t [1494445826] )
http://192.168.8.102/twiki/bin/edit/Know/WebHome (t [1494445787] )
http://192.168.8.102/twiki/bin/edit/Know/WebIndex (t [1494445997] )
http://192.168.8.102/twiki/bin/edit/Know/WebNotify (t [1494445999] )
http://192.168.8.102/twiki/bin/edit/Know/WebPreferences (t [1494445833] )
http://192.168.8.102/twiki/bin/edit/Know/WebSearch (t [1494445832] )
http://192.168.8.102/twiki/bin/edit/Know/WebStatistics (t [1494446000] )
http://192.168.8.102/twiki/bin/edit/Know/WebTopicList (t [1494445998] )
http://192.168.8.102/twiki/bin/edit/Main/BillClinton (topicparent [Main.TWikiUse
↪rs] )
http://192.168.8.102/twiki/bin/edit/Main/CharleytheHorse (t [1494446013] )
http://192.168.8.102/twiki/bin/edit/Main/ChristopheVermeulen (topicparent [Main.
↪TWikiUsers] )
http://192.168.8.102/twiki/bin/edit/Main/DavidWarman (topicparent [Main.TWikiUse
↪rs] )
http://192.168.8.102/twiki/bin/edit/Main/EngineeringGroup (topicparent [Main.TWi
↪kiGroups] )
http://192.168.8.102/twiki/bin/edit/Main/GoodStyle (topicparent [Main.WebHome] )
http://192.168.8.102/twiki/bin/edit/Main/JohnAltstadt (topicparent [Main.TWikiUs
↪ers] )
http://192.168.8.102/twiki/bin/edit/Main/JohnTalintyre (t [1494446013] )
http://192.168.8.102/twiki/bin/edit/Main/LondonOffice (t [1494446023] )
http://192.168.8.102/twiki/bin/edit/Main/MartinRaabe (topicparent [TWiki.TWikiUp
↪gradeGuide] )
http://192.168.8.102/twiki/bin/edit/Main/NicholasLee (t [1494446014] )
http://192.168.8.102/twiki/bin/edit/Main/OfficeLocations (t [1494445797] )
http://192.168.8.102/twiki/bin/edit/Main/PeterFokkinga (topicparent [Main.TWikiU
↪sers] )
http://192.168.8.102/twiki/bin/edit/Main/PeterThoeny (t [1494445899] )
http://192.168.8.102/twiki/bin/edit/Main/SanJoseOffice (t [1494446022] )
http://192.168.8.102/twiki/bin/edit/Main/SupportGroup (topicparent [Main.TWikiGr
↪oups] )
http://192.168.8.102/twiki/bin/edit/Main/TWikiAdminGroup (t [1494446019] )
http://192.168.8.102/twiki/bin/edit/Main/TWikiDocumentation (topicparent [Main.W
↪ebStatistics] )
http://192.168.8.102/twiki/bin/edit/Main/TWikiGroups (t [1494445795] )
http://192.168.8.102/twiki/bin/edit/Main/TWikiGuest (t [1494446015] )
http://192.168.8.102/twiki/bin/edit/Main/TWikiPreferences (topicparent [Main.Web
↪Home] )
http://192.168.8.102/twiki/bin/edit/Main/TWikiRegistration (topicparent [Main.TW
↪ikiUsers] )
http://192.168.8.102/twiki/bin/edit/Main/TWikiUsers (t [1494445793] )
http://192.168.8.102/twiki/bin/edit/Main/TWikiWeb (topicparent [Main.WebHome] )
http://192.168.8.102/twiki/bin/edit/Main/TestArea (topicparent [Main.WebHome] )
http://192.168.8.102/twiki/bin/edit/Main/TextFormattingFAQ (topicparent [Main.We
↪bHome] )
http://192.168.8.102/twiki/bin/edit/Main/TextFormattingRules (topicparent [Main.
```

... continues on next page ...

... continued from previous page ...

```
↪WebHome] )
http://192.168.8.102/twiki/bin/edit/Main/TokyoOffice (t [1494446023] )
http://192.168.8.102/twiki/bin/edit/Main/WebChanges (t [1494445798] )
http://192.168.8.102/twiki/bin/edit/Main/WebHome (t [1494445775] )
http://192.168.8.102/twiki/bin/edit/Main/WebIndex (t [1494445803] )
http://192.168.8.102/twiki/bin/edit/Main/WebNotify (t [1494445838] )
http://192.168.8.102/twiki/bin/edit/Main/WebPreferences (t [1494445807] )
http://192.168.8.102/twiki/bin/edit/Main/WebRss (t [1494446025] )
http://192.168.8.102/twiki/bin/edit/Main/WebSearch (t [1494445805] )
http://192.168.8.102/twiki/bin/edit/Main/WebStatistics (t [1494445839] )
http://192.168.8.102/twiki/bin/edit/Main/WebTopicEditTemplate (topicparent [Main
↪.WebPreferences] )
http://192.168.8.102/twiki/bin/edit/Main/WebTopicList (t [1494445838] )
http://192.168.8.102/twiki/bin/edit/Main/WelcomeGuest (topicparent [Main.WebHome
↪] )
http://192.168.8.102/twiki/bin/edit/Main/WikiName (topicparent [Main.TWikiUsers]
↪ )
http://192.168.8.102/twiki/bin/edit/Main/WikiNotation (topicparent [Main.TWikiUs
↪ers] )
http://192.168.8.102/twiki/bin/edit/Sandbox/TestTopic1 (topicparent [Sandbox.Web
↪Home] )
http://192.168.8.102/twiki/bin/edit/Sandbox/TestTopic2 (topicparent [Sandbox.Web
↪Home] )
http://192.168.8.102/twiki/bin/edit/Sandbox/TestTopic3 (topicparent [Sandbox.Web
↪Home] )
http://192.168.8.102/twiki/bin/edit/Sandbox/TestTopic4 (topicparent [Sandbox.Web
↪Home] )
http://192.168.8.102/twiki/bin/edit/Sandbox/TestTopic5 (topicparent [Sandbox.Web
↪Home] )
http://192.168.8.102/twiki/bin/edit/Sandbox/TestTopic6 (topicparent [Sandbox.Web
↪Home] )
http://192.168.8.102/twiki/bin/edit/Sandbox/TestTopic7 (topicparent [Sandbox.Web
↪Home] )
http://192.168.8.102/twiki/bin/edit/Sandbox/TestTopic8 (topicparent [Sandbox.Web
↪Home] )
http://192.168.8.102/twiki/bin/edit/Sandbox/WebChanges (t [1494445834] )
http://192.168.8.102/twiki/bin/edit/Sandbox/WebHome (t [1494445789] )
http://192.168.8.102/twiki/bin/edit/Sandbox/WebIndex (t [1494446003] )
http://192.168.8.102/twiki/bin/edit/Sandbox/WebNotify (t [1494446009] )
http://192.168.8.102/twiki/bin/edit/Sandbox/WebPreferences (t [1494445837] )
http://192.168.8.102/twiki/bin/edit/Sandbox/WebSearch (t [1494445835] )
http://192.168.8.102/twiki/bin/edit/Sandbox/WebStatistics (t [1494446010] )
http://192.168.8.102/twiki/bin/edit/Sandbox/WebTopicEditTemplate (topicparent [S
↪andbox.WebPreferences] )
http://192.168.8.102/twiki/bin/edit/Sandbox/WebTopicList (t [1494446008] )
http://192.168.8.102/twiki/bin/edit/TWiki/ (templatetopic [TWikiFaqTemplate] top
↪ic [] topicparent [TWikiFAQ] onlywikiname [on] )
```

... continues on next page ...

... continued from previous page ...

```
http://192.168.8.102/twiki/bin/edit/TWiki/AppendixFileSystem (t [1494445982] )
http://192.168.8.102/twiki/bin/edit/TWiki/DefaultPlugin (t [1494445928] )
http://192.168.8.102/twiki/bin/edit/TWiki/FileAttachment (t [1494445922] )
http://192.168.8.102/twiki/bin/edit/TWiki/FormattedSearch (t [1494445960] )
http://192.168.8.102/twiki/bin/edit/TWiki/GnuGeneralPublicLicense (t [1494445990
↪] )
http://192.168.8.102/twiki/bin/edit/TWiki/GoodStyle (t [1494445888] )
http://192.168.8.102/twiki/bin/edit/TWiki/InstalledPlugins (t [1494445987] )
http://192.168.8.102/twiki/bin/edit/TWiki/InstantEnhancements (t [1494445935] )
http://192.168.8.102/twiki/bin/edit/TWiki/InterWikis (t [1494445931] )
http://192.168.8.102/twiki/bin/edit/TWiki/InterwikiPlugin (t [1494445929] )
http://192.168.8.102/twiki/bin/edit/TWiki/ManagingTopics (t [1494445978] )
http://192.168.8.102/twiki/bin/edit/TWiki/ManagingWebs (t [1494445980] )
http://192.168.8.102/twiki/bin/edit/TWiki/MeaningfulTitle (topicparent [TWiki.Te
↪xtFormattingFAQ] )
http://192.168.8.102/twiki/bin/edit/TWiki/NewTopic (topicparent [TWiki.TWikiShor
↪thand] )
http://192.168.8.102/twiki/bin/edit/TWiki/NotExistingYet (topicparent [TWiki.Tex
↪tFormattingRules] )
http://192.168.8.102/twiki/bin/edit/TWiki/PeterThoeny (t [1494445989] )
http://192.168.8.102/twiki/bin/edit/TWiki/SiteMap (t [1494445988] )
http://192.168.8.102/twiki/bin/edit/TWiki/StartingPoints (t [1494445810] )
http://192.168.8.102/twiki/bin/edit/TWiki/TWikiAccessControl (t [1494445951] )
http://192.168.8.102/twiki/bin/edit/TWiki/TWikiAdminCookBook (t [1494445932] )
http://192.168.8.102/twiki/bin/edit/TWiki/TWikiCourseOutlineExample (topicparent
↪ [TWiki.WebHome] )
http://192.168.8.102/twiki/bin/edit/TWiki/TWikiFAQ (t [1494445844] )
http://192.168.8.102/twiki/bin/edit/TWiki/TWikiFormTemplate (topicparent [Main.W
↪ebPreferences] )
http://192.168.8.102/twiki/bin/edit/TWiki/TWikiForms (t [1494445822] )
http://192.168.8.102/twiki/bin/edit/TWiki/TWikiFuncModule (t [1494445968] )
http://192.168.8.102/twiki/bin/edit/TWiki/TWikiGlossary (t [1494445927] )
http://192.168.8.102/twiki/bin/edit/TWiki/TWikiHistory (t [1494445882] )
http://192.168.8.102/twiki/bin/edit/TWiki/TWikiImplementationNotes (topicparent
↪[TWiki.WebHome] )
http://192.168.8.102/twiki/bin/edit/TWiki/TWikiInstallationGuide (t [1494445939]
↪ )
http://192.168.8.102/twiki/bin/edit/TWiki/TWikiMetaData (t [1494445961] )
http://192.168.8.102/twiki/bin/edit/TWiki/TWikiPages (topicparent [TWiki.WebHome
↪] )
http://192.168.8.102/twiki/bin/edit/TWiki/TWikiPlugins (t [1494445964] )
http://192.168.8.102/twiki/bin/edit/TWiki/TWikiPreferences (t [1494445840] )
http://192.168.8.102/twiki/bin/edit/TWiki/TWikiRegistration (t [1494445809] )
http://192.168.8.102/twiki/bin/edit/TWiki/TWikiShorthand (t [1494445919] )
http://192.168.8.102/twiki/bin/edit/TWiki/TWikiSite (t [1494445843] )
http://192.168.8.102/twiki/bin/edit/TWiki/TWikiSiteTools (t [1494445976] )
http://192.168.8.102/twiki/bin/edit/TWiki/TWikiSkins (t [1494445958] )
```

... continues on next page ...

... continued from previous page ...

```
http://192.168.8.102/twiki/bin/edit/TWiki/TWikiSystemRequirements (t [1494445937
↪] )
http://192.168.8.102/twiki/bin/edit/TWiki/TWikiTemplates (t [1494445954] )
http://192.168.8.102/twiki/bin/edit/TWiki/TWikiTopic (topicparent [TWiki.TWikiTo
↪pics] )
http://192.168.8.102/twiki/bin/edit/TWiki/TWikiTopics (t [1494445916] )
http://192.168.8.102/twiki/bin/edit/TWiki/TWikiTutorial (t [1494445914] )
http://192.168.8.102/twiki/bin/edit/TWiki/TWikiUpgradeGuide (t [1494445947] )
http://192.168.8.102/twiki/bin/edit/TWiki/TWikiUserAuthentication (t [1494445949
↪] )
http://192.168.8.102/twiki/bin/edit/TWiki/TWikiVariables (t [1494445920] )
http://192.168.8.102/twiki/bin/edit/TWiki/TWikiVariablesExamples (topicparent [T
↪Wiki.WebHome] )
http://192.168.8.102/twiki/bin/edit/TWiki/TWikiWeb (topicparent [Main.WebHome] )
http://192.168.8.102/twiki/bin/edit/TWiki/TextFormattingFAQ (t [1494445892] )
http://192.168.8.102/twiki/bin/edit/TWiki/TextFormattingRules (t [1494445889] )
http://192.168.8.102/twiki/bin/edit/TWiki/WebChanges (t [1494445811] )
http://192.168.8.102/twiki/bin/edit/TWiki/WebChangesAlert (t [1494445926] )
http://192.168.8.102/twiki/bin/edit/TWiki/WebHome (t [1494445781] )
http://192.168.8.102/twiki/bin/edit/TWiki/WebIndex (t [1494445904] )
http://192.168.8.102/twiki/bin/edit/TWiki/WebNotify (t [1494445986] )
http://192.168.8.102/twiki/bin/edit/TWiki/WebPreferences (t [1494445821] )
http://192.168.8.102/twiki/bin/edit/TWiki/WebSearch (t [1494445820] )
http://192.168.8.102/twiki/bin/edit/TWiki/WebStatistics (t [1494445986] )
http://192.168.8.102/twiki/bin/edit/TWiki/WebTopicList (t [1494445900] )
http://192.168.8.102/twiki/bin/edit/TWiki/WelcomeGuest (t [1494445806] )
http://192.168.8.102/twiki/bin/edit/TWiki/WikiCulture (t [1494446020] )
http://192.168.8.102/twiki/bin/edit/TWiki/WikiName (t [1494446004] )
http://192.168.8.102/twiki/bin/edit/TWiki/WikiOrg (topicparent [TWiki.TWikiAdmin
↪CookBook] )
http://192.168.8.102/twiki/bin/edit/TWiki/WikiStyleWord (topicparent [TWiki.Text
↪FormattingFAQ] )
http://192.168.8.102/twiki/bin/edit/TWiki/WindowsInstallCookbook (t [1494445942]
↪ )
http://192.168.8.102/twiki/bin/manage/TWiki/ManagingWebs (newweb [] baseweb [] w
↪ebbgcolor [#D0D0D0] sitemapwhat [] sitemapuseto [...collaborate on] nosearchal
↪l [] nosearchall [on] newtopic [] action [createweb] )
http://192.168.8.102/twiki/bin/oops/Know/ReadmeFirst (template [oopsmore] param1
↪ [1.6] param2 [1.6] )
http://192.168.8.102/twiki/bin/oops/Know/WebChanges (template [oopsmore] param1
↪[1.2] param2 [1.2] )
http://192.168.8.102/twiki/bin/oops/Know/WebHome (param1 [1.10] param2 [1.10] te
↪mplate [oopsmore] )
http://192.168.8.102/twiki/bin/oops/Know/WebIndex (template [oopsmore] param1 [1
↪.2] param2 [1.2] )
http://192.168.8.102/twiki/bin/oops/Know/WebNotify (template [oopsmore] param1 [
↪1.7] param2 [1.7] )
```

... continues on next page ...

... continued from previous page ...

```
http://192.168.8.102/twiki/bin/oops/Know/WebPreferences (template [oopsmore] par
↪am1 [1.11] param2 [1.11] )
http://192.168.8.102/twiki/bin/oops/Know/WebSearch (template [oopsmore] param1 [
↪1.9] param2 [1.9] )
http://192.168.8.102/twiki/bin/oops/Know/WebStatistics (template [oopsmore] para
↪m1 [1.4] param2 [1.4] )
http://192.168.8.102/twiki/bin/oops/Know/WebTopicList (template [oopsmore] param
↪1 [1.1] param2 [1.1] )
http://192.168.8.102/twiki/bin/oops/Main/CharleytheHorse (param1 [1.1] param2 [1
↪.1] template [oopsmore] )
http://192.168.8.102/twiki/bin/oops/Main/JohnTalintyre (template [oopsmore] para
↪m1 [1.3] param2 [1.3] )
http://192.168.8.102/twiki/bin/oops/Main/LondonOffice (template [oopsmore] param
↪1 [1.3] param2 [1.3] )
http://192.168.8.102/twiki/bin/oops/Main/NicholasLee (template [oopsmore] param1
↪ [1.2] param2 [1.2] )
http://192.168.8.102/twiki/bin/oops/Main/OfficeLocations (param1 [1.4] param2 [1
↪.4] template [oopsmore] )
http://192.168.8.102/twiki/bin/oops/Main/PeterThoeny (template [oopsmore] param1
↪ [1.8] param2 [1.8] )
http://192.168.8.102/twiki/bin/oops/Main/SanJoseOffice (template [oopsmore] para
↪m1 [1.3] param2 [1.3] )
http://192.168.8.102/twiki/bin/oops/Main/TWikiAdminGroup (template [oopsmore] pa
↪ram1 [1.7] param2 [1.7] )
http://192.168.8.102/twiki/bin/oops/Main/TWikiGroups (param1 [1.3] param2 [1.3]
↪template [oopsmore] )
http://192.168.8.102/twiki/bin/oops/Main/TWikiGuest (template [oopsmore] param1
↪[1.5] param2 [1.5] )
http://192.168.8.102/twiki/bin/oops/Main/TWikiUsers (param1 [1.16] param2 [1.16]
↪ template [oopsmore] )
http://192.168.8.102/twiki/bin/oops/Main/TokyoOffice (template [oopsmore] param1
↪ [1.3] param2 [1.3] )
http://192.168.8.102/twiki/bin/oops/Main/WebChanges (template [oopsmore] param1
↪[1.2] param2 [1.2] )
http://192.168.8.102/twiki/bin/oops/Main/WebHome (param1 [1.20] param2 [1.20] te
↪mplate [oopsmore] )
http://192.168.8.102/twiki/bin/oops/Main/WebIndex (template [oopsmore] param1 [1
↪.2] param2 [1.2] )
http://192.168.8.102/twiki/bin/oops/Main/WebNotify (param1 [1.7] param2 [1.7] te
↪mplate [oopsmore] )
http://192.168.8.102/twiki/bin/oops/Main/WebPreferences (param1 [1.13] param2 [1
↪.13] template [oopsmore] )
http://192.168.8.102/twiki/bin/oops/Main/WebRss (param1 [1.1] param2 [1.1] templ
↪ate [oopsmore] )
http://192.168.8.102/twiki/bin/oops/Main/WebSearch (template [oopsmore] param1 [
↪1.8] param2 [1.8] )
http://192.168.8.102/twiki/bin/oops/Main/WebStatistics (param1 [1.4] param2 [1.4
```

... continues on next page ...

... continued from previous page ...

```
↪] template [oopsmore] )
http://192.168.8.102/twiki/bin/oops/Main/WebTopicList (template [oopsmore] param
↪1 [1.1] param2 [1.1] )
http://192.168.8.102/twiki/bin/oops/Sandbox/WebChanges (template [oopsmore] para
↪m1 [1.2] param2 [1.2] )
http://192.168.8.102/twiki/bin/oops/Sandbox/WebHome (param1 [1.7] param2 [1.7] t
↪emplate [oopsmore] )
http://192.168.8.102/twiki/bin/oops/Sandbox/WebIndex (template [oopsmore] param1
↪ [1.2] param2 [1.2] )
http://192.168.8.102/twiki/bin/oops/Sandbox/WebNotify (template [oopsmore] param
↪1 [1.5] param2 [1.5] )
http://192.168.8.102/twiki/bin/oops/Sandbox/WebPreferences (template [oopsmore]
↪param1 [1.10] param2 [1.10] )
http://192.168.8.102/twiki/bin/oops/Sandbox/WebSearch (template [oopsmore] param
↪1 [1.6] param2 [1.6] )
http://192.168.8.102/twiki/bin/oops/Sandbox/WebStatistics (template [oopsmore] p
↪aram1 [1.3] param2 [1.3] )
http://192.168.8.102/twiki/bin/oops/Sandbox/WebTopicList (template [oopsmore] pa
↪ram1 [1.1] param2 [1.1] )
http://192.168.8.102/twiki/bin/oops/TWiki/AppendixFileSystem (template [oopsmore
↪] param1 [1.12] param2 [1.12] )
http://192.168.8.102/twiki/bin/oops/TWiki/DefaultPlugin (template [oopsmore] par
↪am1 [1.5] param2 [1.5] )
http://192.168.8.102/twiki/bin/oops/TWiki/FileAttachment (template [oopsmore] pa
↪ram1 [1.10] param2 [1.10] )
http://192.168.8.102/twiki/bin/oops/TWiki/FormattedSearch (template [oopsmore] p
↪aram1 [1.9] param2 [1.9] )
http://192.168.8.102/twiki/bin/oops/TWiki/GnuGeneralPublicLicense (template [oop
↪smore] param1 [1.2] param2 [1.2] )
http://192.168.8.102/twiki/bin/oops/TWiki/GoodStyle (template [oopsmore] param1
↪[1.6] param2 [1.6] )
http://192.168.8.102/twiki/bin/oops/TWiki/InstalledPlugins (template [oopsmore]
↪param1 [1.1] param2 [1.1] )
http://192.168.8.102/twiki/bin/oops/TWiki/InstantEnhancements (template [oopsmor
↪e] param1 [1.1] param2 [1.1] )
http://192.168.8.102/twiki/bin/oops/TWiki/InterWikis (template [oopsmore] param1
↪ [1.3] param2 [1.3] )
http://192.168.8.102/twiki/bin/oops/TWiki/InterwikiPlugin (template [oopsmore] p
↪aram1 [1.6] param2 [1.6] )
http://192.168.8.102/twiki/bin/oops/TWiki/ManagingTopics (template [oopsmore] pa
↪ram1 [1.17] param2 [1.17] )
http://192.168.8.102/twiki/bin/oops/TWiki/ManagingWebs (template [oopsmore] para
↪m1 [1.23] param2 [1.23] )
http://192.168.8.102/twiki/bin/oops/TWiki/PeterThoeny (template [oopsmore] param
↪1 [1.4] param2 [1.4] )
http://192.168.8.102/twiki/bin/oops/TWiki/SiteMap (template [oopsmore] param1 [1
↪.2] param2 [1.2] )
```

... continues on next page ...

... continued from previous page ...

```
http://192.168.8.102/twiki/bin/oops/TWiki/StartingPoints (template [oopsmore] pa
↪ram1 [1.3] param2 [1.3] )
http://192.168.8.102/twiki/bin/oops/TWiki/TWikiAccessControl (template [oopsmore
↪] param1 [1.27] param2 [1.27] )
http://192.168.8.102/twiki/bin/oops/TWiki/TWikiAdminCookBook (template [oopsmore
↪] param1 [1.2] param2 [1.2] )
http://192.168.8.102/twiki/bin/oops/TWiki/TWikiFAQ (template [oopsmore] param1 [
↪1.12] param2 [1.12] )
http://192.168.8.102/twiki/bin/oops/TWiki/TWikiForms (template [oopsmore] param1
↪ [1.16] param2 [1.16] )
http://192.168.8.102/twiki/bin/oops/TWiki/TWikiFuncModule (template [oopsmore] p
↪aram1 [1.3] param2 [1.3] )
http://192.168.8.102/twiki/bin/oops/TWiki/TWikiGlossary (template [oopsmore] par
↪am1 [1.2] param2 [1.2] )
http://192.168.8.102/twiki/bin/oops/TWiki/TWikiHistory (param1 [1.10] param2 [1.
↪61] template [oopsrev] )
http://192.168.8.102/twiki/bin/oops/TWiki/TWikiInstallationGuide (template [oops
↪more] param1 [1.53] param2 [1.53] )
http://192.168.8.102/twiki/bin/oops/TWiki/TWikiMetaData (template [oopsmore] par
↪am1 [1.11] param2 [1.11] )
http://192.168.8.102/twiki/bin/oops/TWiki/TWikiPlugins (template [oopsmore] para
↪m1 [1.21] param2 [1.21] )
http://192.168.8.102/twiki/bin/oops/TWiki/TWikiPreferences (template [oopsmore]
↪param1 [1.47] param2 [1.47] )
http://192.168.8.102/twiki/bin/oops/TWiki/TWikiRegistration (template [oopsmore]
↪ param1 [1.8] param2 [1.8] )
http://192.168.8.102/twiki/bin/oops/TWiki/TWikiShorthand (template [oopsmore] pa
↪ram1 [1.1] param2 [1.1] )
http://192.168.8.102/twiki/bin/oops/TWiki/TWikiSite (template [oopsmore] param1
↪[1.21] param2 [1.21] )
http://192.168.8.102/twiki/bin/oops/TWiki/TWikiSiteTools (template [oopsmore] pa
↪ram1 [1.7] param2 [1.7] )
http://192.168.8.102/twiki/bin/oops/TWiki/TWikiSkins (template [oopsmore] param1
↪ [1.11] param2 [1.11] )
http://192.168.8.102/twiki/bin/oops/TWiki/TWikiSystemRequirements (template [oop
↪smore] param1 [1.28] param2 [1.28] )
http://192.168.8.102/twiki/bin/oops/TWiki/TWikiTemplates (template [oopsmore] pa
↪ram1 [1.18] param2 [1.18] )
http://192.168.8.102/twiki/bin/oops/TWiki/TWikiTopics (template [oopsmore] param
↪1 [1.12] param2 [1.12] )
http://192.168.8.102/twiki/bin/oops/TWiki/TWikiTutorial (template [oopsmore] par
↪am1 [1.12] param2 [1.12] )
http://192.168.8.102/twiki/bin/oops/TWiki/TWikiUpgradeGuide (template [oopsmore]
↪ param1 [1.3] param2 [1.3] )
http://192.168.8.102/twiki/bin/oops/TWiki/TWikiUserAuthentication (template [oop
↪smore] param1 [1.15] param2 [1.15] )
http://192.168.8.102/twiki/bin/oops/TWiki/TWikiVariables (template [oopsmore] pa
```

... continues on next page ...

... continued from previous page ...

```
↪ram1 [1.62] param2 [1.62] )
http://192.168.8.102/twiki/bin/oops/TWiki/TextFormattingFAQ (template [oopsmore]
↪ param1 [1.14] param2 [1.14] )
http://192.168.8.102/twiki/bin/oops/TWiki/TextFormattingRules (template [oopsmor
↪e] param1 [1.37] param2 [1.37] )
http://192.168.8.102/twiki/bin/oops/TWiki/WebChanges (template [oopsmore] param1
↪ [1.3] param2 [1.3] )
http://192.168.8.102/twiki/bin/oops/TWiki/WebChangesAlert (template [oopsmore] p
↪aram1 [1.13] param2 [1.13] )
http://192.168.8.102/twiki/bin/oops/TWiki/WebHome (param1 [1.78] param2 [1.78] t
↪emplate [oopsmore] )
http://192.168.8.102/twiki/bin/oops/TWiki/WebIndex (template [oopsmore] param1 [
↪1.2] param2 [1.2] )
http://192.168.8.102/twiki/bin/oops/TWiki/WebNotify (template [oopsmore] param1
↪[1.5] param2 [1.5] )
http://192.168.8.102/twiki/bin/oops/TWiki/WebPreferences (template [oopsmore] pa
↪ram1 [1.17] param2 [1.17] )
http://192.168.8.102/twiki/bin/oops/TWiki/WebSearch (template [oopsmore] param1
↪[1.12] param2 [1.12] )
http://192.168.8.102/twiki/bin/oops/TWiki/WebStatistics (template [oopsmore] par
↪am1 [1.3] param2 [1.3] )
http://192.168.8.102/twiki/bin/oops/TWiki/WebTopicList (template [oopsmore] para
↪m1 [1.1] param2 [1.1] )
http://192.168.8.102/twiki/bin/oops/TWiki/WelcomeGuest (template [oopsmore] para
↪m1 [1.20] param2 [1.20] )
http://192.168.8.102/twiki/bin/oops/TWiki/WikiCulture (template [oopsmore] param
↪1 [1.8] param2 [1.8] )
http://192.168.8.102/twiki/bin/oops/TWiki/WikiName (template [oopsmore] param1 [
↪1.3] param2 [1.3] )
http://192.168.8.102/twiki/bin/oops/TWiki/WindowsInstallCookbook (template [oops
↪more] param1 [1.3] param2 [1.3] )
http://192.168.8.102/twiki/bin/passwd/Main/WebHome (username [] password [] pass
↪wordA [] TopicName [ResetPassword] )
http://192.168.8.102/twiki/bin/passwd/TWiki/WebHome (username [] oldpassword []
↪password [] passwordA [] TopicName [ChangePassword] change [on] )
http://192.168.8.102/twiki/bin/preview/Know/WebHome (formtemplate [] topicparent
↪ [] cmd [] submitChangeForm [   Add form   ] )
http://192.168.8.102/twiki/bin/preview/Main/EngineeringGroup (formtemplate [] to
↪picparent [] cmd [] )
http://192.168.8.102/twiki/bin/preview/Main/OfficeLocations (formtemplate [] top
↪icparent [] cmd [] )
http://192.168.8.102/twiki/bin/preview/Main/SupportGroup (formtemplate [] topicp
↪arent [] cmd [] )
http://192.168.8.102/twiki/bin/preview/Main/TWikiGroups (formtemplate [] topicpa
↪rent [] cmd [] )
http://192.168.8.102/twiki/bin/preview/Main/TWikiUsers (formtemplate [] topicpar
↪ent [] cmd [] )
```

... continues on next page ...

... continued from previous page ...

```
http://192.168.8.102/twiki/bin/preview/Main/WebHome (formtemplate [] topicparent
↪ [] cmd [] )
http://192.168.8.102/twiki/bin/preview/Sandbox/TestTopic1 (formtemplate [] topic
↪parent [] cmd [] )
http://192.168.8.102/twiki/bin/preview/Sandbox/TestTopic2 (formtemplate [] topic
↪parent [] cmd [] )
http://192.168.8.102/twiki/bin/preview/Sandbox/TestTopic3 (formtemplate [] topic
↪parent [] cmd [] )
http://192.168.8.102/twiki/bin/preview/Sandbox/TestTopic4 (formtemplate [] topic
↪parent [] cmd [] )
http://192.168.8.102/twiki/bin/preview/Sandbox/TestTopic5 (formtemplate [] topic
↪parent [] cmd [] )
http://192.168.8.102/twiki/bin/preview/Sandbox/TestTopic6 (formtemplate [] topic
↪parent [] cmd [] )
http://192.168.8.102/twiki/bin/preview/Sandbox/TestTopic7 (formtemplate [] topic
↪parent [] cmd [] )
http://192.168.8.102/twiki/bin/preview/Sandbox/TestTopic8 (formtemplate [] topic
↪parent [] cmd [] )
http://192.168.8.102/twiki/bin/preview/Sandbox/WebHome (formtemplate [] topicpar
↪ent [] cmd [] )
http://192.168.8.102/twiki/bin/preview/TWiki/WebHome (formtemplate [] topicparen
↪t [] cmd [] )
http://192.168.8.102/twiki/bin/rdiff/Know/ReadmeFirst (rev1 [1.6] rev2 [1.5] )
http://192.168.8.102/twiki/bin/rdiff/Know/WebChanges (rev1 [1.2] rev2 [1.1] )
http://192.168.8.102/twiki/bin/rdiff/Know/WebHome (rev1 [1.10] rev2 [1.9] )
http://192.168.8.102/twiki/bin/rdiff/Know/WebIndex (rev1 [1.2] rev2 [1.1] )
http://192.168.8.102/twiki/bin/rdiff/Know/WebNotify (rev1 [1.7] rev2 [1.6] )
http://192.168.8.102/twiki/bin/rdiff/Know/WebPreferences (rev1 [1.11] rev2 [1.10
↪] )
http://192.168.8.102/twiki/bin/rdiff/Know/WebSearch (rev1 [1.9] rev2 [1.8] )
http://192.168.8.102/twiki/bin/rdiff/Know/WebStatistics (rev1 [1.4] rev2 [1.3] )
http://192.168.8.102/twiki/bin/rdiff/Main/JohnTalintyre (rev1 [1.3] rev2 [1.2] )
http://192.168.8.102/twiki/bin/rdiff/Main/LondonOffice (rev1 [1.3] rev2 [1.2] )
http://192.168.8.102/twiki/bin/rdiff/Main/NicholasLee (rev1 [1.2] rev2 [1.1] )
http://192.168.8.102/twiki/bin/rdiff/Main/OfficeLocations (rev1 [1.4] rev2 [1.3]
↪ )
http://192.168.8.102/twiki/bin/rdiff/Main/PeterThoeny (rev1 [1.8] rev2 [1.7] )
http://192.168.8.102/twiki/bin/rdiff/Main/SanJoseOffice (rev1 [1.3] rev2 [1.2] )
http://192.168.8.102/twiki/bin/rdiff/Main/TWikiAdminGroup (rev1 [1.7] rev2 [1.6]
↪ )
http://192.168.8.102/twiki/bin/rdiff/Main/TWikiGroups (rev1 [1.3] rev2 [1.2] )
http://192.168.8.102/twiki/bin/rdiff/Main/TWikiGuest (rev1 [1.5] rev2 [1.4] )
http://192.168.8.102/twiki/bin/rdiff/Main/TWikiUsers (rev1 [1.16] rev2 [1.15] )
http://192.168.8.102/twiki/bin/rdiff/Main/TokyoOffice (rev1 [1.3] rev2 [1.2] )
http://192.168.8.102/twiki/bin/rdiff/Main/WebChanges (rev1 [1.2] rev2 [1.1] )
http://192.168.8.102/twiki/bin/rdiff/Main/WebHome (rev1 [1.20] rev2 [1.19] )
http://192.168.8.102/twiki/bin/rdiff/Main/WebIndex (rev1 [1.2] rev2 [1.1] )
```

... continues on next page ...

... continued from previous page ...

```
http://192.168.8.102/twiki/bin/rdiff/Main/WebNotify (rev1 [1.7] rev2 [1.6] )
http://192.168.8.102/twiki/bin/rdiff/Main/WebPreferences (rev1 [1.13] rev2 [1.12
↪] )
http://192.168.8.102/twiki/bin/rdiff/Main/WebSearch (rev1 [1.8] rev2 [1.7] )
http://192.168.8.102/twiki/bin/rdiff/Main/WebStatistics (rev1 [1.4] rev2 [1.3] )
http://192.168.8.102/twiki/bin/rdiff/Sandbox/WebChanges (rev1 [1.2] rev2 [1.1] )
http://192.168.8.102/twiki/bin/rdiff/Sandbox/WebHome (rev1 [1.7] rev2 [1.6] )
http://192.168.8.102/twiki/bin/rdiff/Sandbox/WebIndex (rev1 [1.2] rev2 [1.1] )
http://192.168.8.102/twiki/bin/rdiff/Sandbox/WebNotify (rev1 [1.5] rev2 [1.4] )
http://192.168.8.102/twiki/bin/rdiff/Sandbox/WebPreferences (rev1 [1.10] rev2 [1
↪.9] )
http://192.168.8.102/twiki/bin/rdiff/Sandbox/WebSearch (rev1 [1.6] rev2 [1.5] )
http://192.168.8.102/twiki/bin/rdiff/Sandbox/WebStatistics (rev1 [1.3] rev2 [1.2
↪] )
http://192.168.8.102/twiki/bin/rdiff/TWiki/AppendixFileSystem (rev1 [1.12] rev2
↪[1.11] )
http://192.168.8.102/twiki/bin/rdiff/TWiki/DefaultPlugin (rev1 [1.5] rev2 [1.4]
↪)
http://192.168.8.102/twiki/bin/rdiff/TWiki/FileAttachment (rev1 [1.10] rev2 [1.9
↪] )
http://192.168.8.102/twiki/bin/rdiff/TWiki/FormattedSearch (rev1 [1.9] rev2 [1.8
↪] )
http://192.168.8.102/twiki/bin/rdiff/TWiki/GnuGeneralPublicLicense (rev1 [1.2] r
↪ev2 [1.1] )
http://192.168.8.102/twiki/bin/rdiff/TWiki/GoodStyle (rev1 [1.6] rev2 [1.5] )
http://192.168.8.102/twiki/bin/rdiff/TWiki/InterWikis (rev1 [1.3] rev2 [1.2] )
http://192.168.8.102/twiki/bin/rdiff/TWiki/InterwikiPlugin (rev1 [1.6] rev2 [1.5
↪] )
http://192.168.8.102/twiki/bin/rdiff/TWiki/ManagingTopics (rev1 [1.17] rev2 [1.1
↪6] )
http://192.168.8.102/twiki/bin/rdiff/TWiki/ManagingWebs (rev1 [1.23] rev2 [1.22]
↪ )
http://192.168.8.102/twiki/bin/rdiff/TWiki/PeterThoeny (rev1 [1.4] rev2 [1.3] )
http://192.168.8.102/twiki/bin/rdiff/TWiki/SiteMap (rev1 [1.2] rev2 [1.1] )
http://192.168.8.102/twiki/bin/rdiff/TWiki/StartingPoints (rev1 [1.3] rev2 [1.2]
↪ )
http://192.168.8.102/twiki/bin/rdiff/TWiki/TWikiAccessControl (rev1 [1.27] rev2
↪[1.26] )
http://192.168.8.102/twiki/bin/rdiff/TWiki/TWikiAdminCookBook (rev1 [1.2] rev2 [
↪1.1] )
http://192.168.8.102/twiki/bin/rdiff/TWiki/TWikiFAQ (rev1 [1.12] rev2 [1.11] )
http://192.168.8.102/twiki/bin/rdiff/TWiki/TWikiForms (rev1 [1.16] rev2 [1.15] )
http://192.168.8.102/twiki/bin/rdiff/TWiki/TWikiFuncModule (rev1 [1.3] rev2 [1.2
↪] )
http://192.168.8.102/twiki/bin/rdiff/TWiki/TWikiGlossary (rev1 [1.2] rev2 [1.1]
↪)
http://192.168.8.102/twiki/bin/rdiff/TWiki/TWikiHistory (rev1 [1.10] rev2 [1.9]
```

... continues on next page ...

... continued from previous page ...

```
↪)
http://192.168.8.102/twiki/bin/rdiff/TWiki/TWikiInstallationGuide (rev1 [1.53] r
↪ev2 [1.52] )
http://192.168.8.102/twiki/bin/rdiff/TWiki/TWikiMetaData (rev1 [1.11] rev2 [1.10
↪] )
http://192.168.8.102/twiki/bin/rdiff/TWiki/TWikiPlugins (rev1 [1.21] rev2 [1.20]
↪ )
http://192.168.8.102/twiki/bin/rdiff/TWiki/TWikiPreferences (rev1 [1.47] rev2 [1
↪.46] )
http://192.168.8.102/twiki/bin/rdiff/TWiki/TWikiRegistration (rev1 [1.8] rev2 [1
↪.7] )
http://192.168.8.102/twiki/bin/rdiff/TWiki/TWikiSite (rev1 [1.21] rev2 [1.20] )
http://192.168.8.102/twiki/bin/rdiff/TWiki/TWikiSiteTools (rev1 [1.7] rev2 [1.6]
↪ )
http://192.168.8.102/twiki/bin/rdiff/TWiki/TWikiSkins (rev1 [1.11] rev2 [1.10] )
http://192.168.8.102/twiki/bin/rdiff/TWiki/TWikiSystemRequirements (rev1 [1.28]
↪rev2 [1.27] )
http://192.168.8.102/twiki/bin/rdiff/TWiki/TWikiTemplates (rev1 [1.18] rev2 [1.1
↪7] )
http://192.168.8.102/twiki/bin/rdiff/TWiki/TWikiTopics (rev1 [1.12] rev2 [1.11]
↪)
http://192.168.8.102/twiki/bin/rdiff/TWiki/TWikiTutorial (rev1 [1.12] rev2 [1.11
↪] )
http://192.168.8.102/twiki/bin/rdiff/TWiki/TWikiUpgradeGuide (rev1 [1.3] rev2 [1
↪.2] )
http://192.168.8.102/twiki/bin/rdiff/TWiki/TWikiUserAuthentication (rev1 [1.15]
↪rev2 [1.14] )
http://192.168.8.102/twiki/bin/rdiff/TWiki/TWikiVariables (rev1 [1.62] rev2 [1.6
↪1] )
http://192.168.8.102/twiki/bin/rdiff/TWiki/TextFormattingFAQ (rev1 [1.14] rev2 [
↪1.13] )
http://192.168.8.102/twiki/bin/rdiff/TWiki/TextFormattingRules (rev1 [1.37] rev2
↪ [1.36] )
http://192.168.8.102/twiki/bin/rdiff/TWiki/WebChanges (rev1 [1.3] rev2 [1.2] )
http://192.168.8.102/twiki/bin/rdiff/TWiki/WebChangesAlert (rev1 [1.13] rev2 [1.
↪12] )
http://192.168.8.102/twiki/bin/rdiff/TWiki/WebHome (rev1 [1.78] rev2 [1.77] )
http://192.168.8.102/twiki/bin/rdiff/TWiki/WebIndex (rev1 [1.2] rev2 [1.1] )
http://192.168.8.102/twiki/bin/rdiff/TWiki/WebNotify (rev1 [1.5] rev2 [1.4] )
http://192.168.8.102/twiki/bin/rdiff/TWiki/WebPreferences (rev1 [1.17] rev2 [1.1
↪6] )
http://192.168.8.102/twiki/bin/rdiff/TWiki/WebSearch (rev1 [1.12] rev2 [1.11] )
http://192.168.8.102/twiki/bin/rdiff/TWiki/WebStatistics (rev1 [1.3] rev2 [1.2]
↪)
http://192.168.8.102/twiki/bin/rdiff/TWiki/WelcomeGuest (rev1 [1.20] rev2 [1.19]
↪ )
http://192.168.8.102/twiki/bin/rdiff/TWiki/WikiCulture (rev1 [1.8] rev2 [1.7] )
```

... continues on next page ...

... continued from previous page ...

```
http://192.168.8.102/twiki/bin/rdiff/TWiki/WikiName (rev1 [1.3] rev2 [1.2] )
http://192.168.8.102/twiki/bin/rdiff/TWiki/WindowsInstallCookbook (rev1 [1.3] re
↪v2 [1.2] )
http://192.168.8.102/twiki/bin/register/Main/WebHome (Twk1Name [] Twk1WikiName [
↪] Twk1LoginName [] Twk1Email [] Twk0Phone [] Twk0Department [] Twk1Location []
↪ TopicName [TWikiRegistration] )
http://192.168.8.102/twiki/bin/rename/TWiki/AppendixFileSystem (newweb [TWiki] n
↪ewtopic [DocsATWikiFileSystem] confirm [on] )
http://192.168.8.102/twiki/bin/rename/TWiki/FileAttachment (attachment [Sample.t
↪xt] )
http://192.168.8.102/twiki/bin/rename/TWiki/ManagingTopics (newweb [TWiki] newto
↪pic [RenameTopic] confirm [on] )
http://192.168.8.102/twiki/bin/rename/TWiki/TWikiForms (newweb [TWiki] newtopic
↪[TWikiFormTemplate] confirm [on] )
http://192.168.8.102/twiki/bin/rename/TWiki/TWikiInstallationGuide (newweb [TWik
↪i] newtopic [TWikiInstallationNotes] confirm [on] )
http://192.168.8.102/twiki/bin/rename/TWiki/TWikiSystemRequirements (newweb [TWi
↪ki] newtopic [TWikiImplementationNotes] confirm [on] )
http://192.168.8.102/twiki/bin/rename/TWiki/TWikiTemplates (newweb [TWiki] newto
↪pic [TWikiTemplateSystem] confirm [on] )
http://192.168.8.102/twiki/bin/rename/TWiki/TWikiTopics (newweb [TWiki] newtopic
↪ [TWikiPages] confirm [on] )
http://192.168.8.102/twiki/bin/rename/TWiki/TWikiUserAuthentication (newweb [TWi
↪ki] newtopic [TWikiAuthentication] confirm [on] )
http://192.168.8.102/twiki/bin/rename/TWiki/WebChangesAlert (newweb [TWiki] newt
↪opic [WebChangesNotify] confirm [on] )
http://192.168.8.102/twiki/bin/search/Know/ (showlock [] search [%5C.*] web [] n
↪osearch [on] scope [topic] reverse [on] casesensitive [] regex [on] limit [100
↪] order [modified] nototal [] bookview [] nosummary [] ignorecase [on] )
http://192.168.8.102/twiki/bin/search/Know/SearchResult (search [] scope [text]
↪nosearch [on] reverse [on] regex [on] order [modified] )
http://192.168.8.102/twiki/bin/search/Main/ (showlock [] search [%5C.*] web [] s
↪cope [topic] nosearch [on] reverse [on] casesensitive [] regex [on] order [mod
↪ified] limit [100] nototal [] bookview [] nosummary [] ignorecase [on] )
http://192.168.8.102/twiki/bin/search/Main/SearchResult (search [] nosearch [on]
↪ scope [text] reverse [on] regex [on] order [modified] )
http://192.168.8.102/twiki/bin/search/Sandbox/ (showlock [] search [%5C.*] web [
↪] nosearch [on] scope [topic] casesensitive [] reverse [on] regex [on] nototal
↪ [] limit [100] order [modified] nosummary [] bookview [] )
http://192.168.8.102/twiki/bin/search/Sandbox/SearchResult (search [] nosearch [
↪on] scope [text] reverse [on] regex [on] order [modified] )
http://192.168.8.102/twiki/bin/search/TWiki/ (showlock [] search [] web [] scope
↪ [topic] nosearch [on] casesensitive [] reverse [on] regex [on] nototal [] ord
↪er [modified] limit [100] nosummary [] bookview [] )
http://192.168.8.102/twiki/bin/search/TWiki/SearchResult (search [] nosearch [on
↪] scope [text] reverse [on] regex [on] order [modified] )
http://192.168.8.102/twiki/bin/upload/Know/WebHome (filename [] filepath [] file
```

... continues on next page ...

... continued from previous page ...

```
↪comment [] createlink [] hidefile [] )
http://192.168.8.102/twiki/bin/upload/Main/OfficeLocations (filename [] filepath
↪ [] filecomment [] createlink [] hidefile [] )
http://192.168.8.102/twiki/bin/upload/Main/TWikiGroups (filename [] filepath []
↪filecomment [] createlink [] hidefile [] )
http://192.168.8.102/twiki/bin/upload/Main/TWikiUsers (filename [] filepath [] f
↪ilecomment [] createlink [] hidefile [] )
http://192.168.8.102/twiki/bin/upload/Main/WebHome (filename [] filepath [] file
↪comment [] createlink [] hidefile [] )
http://192.168.8.102/twiki/bin/upload/Sandbox/WebHome (filename [] filepath [] f
↪ilecomment [] createlink [] hidefile [] )
http://192.168.8.102/twiki/bin/upload/TWiki/WebHome (filename [] filepath [] fil
↪ecomment [] createlink [] hidefile [] )
http://192.168.8.102/twiki/bin/view/Know/ReadmeFirst (topic [] skin [print] rev
↪[1.5] )
http://192.168.8.102/twiki/bin/view/Know/WebChanges (topic [] skin [print] rev [
↪1.1] )
http://192.168.8.102/twiki/bin/view/Know/WebHome (topic [] skin [print] rev [1.9
↪] unlock [on] )
http://192.168.8.102/twiki/bin/view/Know/WebIndex (topic [] skin [print] rev [1.
↪1] )
http://192.168.8.102/twiki/bin/view/Know/WebNotify (topic [] skin [print] rev [1
↪.6] )
http://192.168.8.102/twiki/bin/view/Know/WebPreferences (topic [] skin [print] r
↪ev [1.10] )
http://192.168.8.102/twiki/bin/view/Know/WebSearch (topic [] skin [print] rev [1
↪.8] )
http://192.168.8.102/twiki/bin/view/Know/WebStatistics (topic [] skin [print] re
↪v [1.3] )
http://192.168.8.102/twiki/bin/view/Know/WebTopicList (topic [] skin [print] )
http://192.168.8.102/twiki/bin/view/Main/CharleytheHorse (topic [] skin [print]
↪rev [r1.1] )
http://192.168.8.102/twiki/bin/view/Main/EngineeringGroup (unlock [on] )
http://192.168.8.102/twiki/bin/view/Main/JohnTalintyre (topic [] skin [print] re
↪v [1.2] )
http://192.168.8.102/twiki/bin/view/Main/LondonOffice (topic [] skin [print] rev
↪ [1.2] )
http://192.168.8.102/twiki/bin/view/Main/NicholasLee (topic [] skin [print] rev
↪[1.1] )
http://192.168.8.102/twiki/bin/view/Main/OfficeLocations (topic [] skin [print]
↪rev [1.3] unlock [on] )
http://192.168.8.102/twiki/bin/view/Main/PeterThoeny (topic [] skin [print] rev
↪[1.7] )
http://192.168.8.102/twiki/bin/view/Main/SanJoseOffice (topic [] skin [print] re
↪v [1.2] )
http://192.168.8.102/twiki/bin/view/Main/SupportGroup (unlock [on] )
http://192.168.8.102/twiki/bin/view/Main/TWikiAdminGroup (topic [] skin [print]
```

... continues on next page ...

... continued from previous page ...

```
↪rev [1.6] )
http://192.168.8.102/twiki/bin/view/Main/TWikiGroups (topic [] skin [print] rev
↪[1.2] unlock [on] )
http://192.168.8.102/twiki/bin/view/Main/TWikiGuest (topic [] skin [print] rev [
↪1.4] )
http://192.168.8.102/twiki/bin/view/Main/TWikiUsers (topic [] skin [print] rev [
↪1.15] unlock [on] )
http://192.168.8.102/twiki/bin/view/Main/TokyoOffice (topic [] skin [print] rev
↪[1.2] )
http://192.168.8.102/twiki/bin/view/Main/WebChanges (topic [] skin [print] rev [
↪1.1] )
http://192.168.8.102/twiki/bin/view/Main/WebHome (topic [] skin [print] rev [1.1
↪9] unlock [on] )
http://192.168.8.102/twiki/bin/view/Main/WebIndex (topic [] skin [print] rev [1.
↪1] )
http://192.168.8.102/twiki/bin/view/Main/WebNotify (topic [] skin [print] rev [1
↪.6] )
http://192.168.8.102/twiki/bin/view/Main/WebPreferences (topic [] skin [print] r
↪ev [1.12] )
http://192.168.8.102/twiki/bin/view/Main/WebRss (topic [] skin [print] rev [r1.1
↪] )
http://192.168.8.102/twiki/bin/view/Main/WebSearch (topic [] skin [print] rev [1
↪.7] )
http://192.168.8.102/twiki/bin/view/Main/WebStatistics (topic [] skin [print] re
↪v [1.3] )
http://192.168.8.102/twiki/bin/view/Main/WebTopicList (topic [] skin [print] )
http://192.168.8.102/twiki/bin/view/Sandbox/TestTopic1 (unlock [on] )
http://192.168.8.102/twiki/bin/view/Sandbox/TestTopic2 (unlock [on] )
http://192.168.8.102/twiki/bin/view/Sandbox/TestTopic3 (unlock [on] )
http://192.168.8.102/twiki/bin/view/Sandbox/TestTopic4 (unlock [on] )
http://192.168.8.102/twiki/bin/view/Sandbox/TestTopic5 (unlock [on] )
http://192.168.8.102/twiki/bin/view/Sandbox/TestTopic6 (unlock [on] )
http://192.168.8.102/twiki/bin/view/Sandbox/TestTopic7 (unlock [on] )
http://192.168.8.102/twiki/bin/view/Sandbox/TestTopic8 (unlock [on] )
http://192.168.8.102/twiki/bin/view/Sandbox/WebChanges (topic [] skin [print] re
↪v [1.1] )
http://192.168.8.102/twiki/bin/view/Sandbox/WebHome (topic [] skin [print] rev [
↪1.6] unlock [on] )
http://192.168.8.102/twiki/bin/view/Sandbox/WebIndex (topic [] skin [print] rev
↪[1.1] )
http://192.168.8.102/twiki/bin/view/Sandbox/WebNotify (topic [] skin [print] rev
↪ [1.4] )
http://192.168.8.102/twiki/bin/view/Sandbox/WebPreferences (topic [] skin [print
↪] rev [1.9] )
http://192.168.8.102/twiki/bin/view/Sandbox/WebSearch (topic [] skin [print] rev
↪ [1.5] )
http://192.168.8.102/twiki/bin/view/Sandbox/WebStatistics (topic [] skin [print]
```

... continues on next page ...

... continued from previous page ...

```
↪ rev [1.2] )
http://192.168.8.102/twiki/bin/view/Sandbox/WebTopicList (topic [] skin [print]
↪)
http://192.168.8.102/twiki/bin/view/TWiki/AppendixFileSystem (topic [] skin [pri
↪nt] rev [1.11] )
http://192.168.8.102/twiki/bin/view/TWiki/DefaultPlugin (topic [] skin [print] r
↪ev [1.4] )
http://192.168.8.102/twiki/bin/view/TWiki/FileAttachment (topic [] skin [print]
↪rev [1.9] )
http://192.168.8.102/twiki/bin/view/TWiki/FormattedSearch (topic [] skin [print]
↪ rev [1.8] )
http://192.168.8.102/twiki/bin/view/TWiki/GnuGeneralPublicLicense (topic [] skin
↪ [print] rev [1.1] )
http://192.168.8.102/twiki/bin/view/TWiki/GoodStyle (topic [] skin [print] rev [
↪1.5] )
http://192.168.8.102/twiki/bin/view/TWiki/InstalledPlugins (topic [] skin [print
↪] )
http://192.168.8.102/twiki/bin/view/TWiki/InstantEnhancements (topic [] skin [pr
↪int] )
http://192.168.8.102/twiki/bin/view/TWiki/InterWikis (topic [] skin [print] rev
↪[1.2] )
http://192.168.8.102/twiki/bin/view/TWiki/InterwikiPlugin (topic [] skin [print]
↪ rev [1.5] )
http://192.168.8.102/twiki/bin/view/TWiki/ManagingTopics (topic [] skin [print]
↪rev [1.16] )
http://192.168.8.102/twiki/bin/view/TWiki/ManagingWebs (topic [] skin [print] re
↪v [1.22] )
http://192.168.8.102/twiki/bin/view/TWiki/PeterThoeny (topic [] skin [print] rev
↪ [1.3] )
http://192.168.8.102/twiki/bin/view/TWiki/SiteMap (topic [] skin [print] rev [1.
↪1] )
http://192.168.8.102/twiki/bin/view/TWiki/StartingPoints (topic [] skin [print]
↪rev [1.2] )
http://192.168.8.102/twiki/bin/view/TWiki/TWikiAccessControl (topic [] skin [pri
↪nt] rev [1.26] )
http://192.168.8.102/twiki/bin/view/TWiki/TWikiAdminCookBook (topic [] skin [pri
↪nt] rev [1.1] )
http://192.168.8.102/twiki/bin/view/TWiki/TWikiDocumentation (topic [] )
http://192.168.8.102/twiki/bin/view/TWiki/TWikiFAQ (topic [] skin [print] rev [1
↪.11] )
http://192.168.8.102/twiki/bin/view/TWiki/TWikiForms (topic [] skin [print] rev
↪[1.15] )
http://192.168.8.102/twiki/bin/view/TWiki/TWikiFuncModule (topic [] skin [print]
↪ rev [1.2] )
http://192.168.8.102/twiki/bin/view/TWiki/TWikiGlossary (topic [] skin [print] r
↪ev [1.1] )
http://192.168.8.102/twiki/bin/view/TWiki/TWikiHistory (topic [] skin [print] re
```

... continues on next page ...

... continued from previous page ...

```
↪v [1.9] )
http://192.168.8.102/twiki/bin/view/TWiki/TWikiInstallationGuide (topic [] skin
↪[print] rev [1.52] )
http://192.168.8.102/twiki/bin/view/TWiki/TWikiMetaData (topic [] skin [print] r
↪ev [1.10] raw [debug] )
http://192.168.8.102/twiki/bin/view/TWiki/TWikiPlugins (topic [] skin [print] re
↪v [1.20] )
http://192.168.8.102/twiki/bin/view/TWiki/TWikiPreferences (topic [] skin [print
↪] rev [1.46] )
http://192.168.8.102/twiki/bin/view/TWiki/TWikiRegistration (topic [] skin [prin
↪t] rev [1.7] )
http://192.168.8.102/twiki/bin/view/TWiki/TWikiShorthand (topic [] skin [print]
↪)
http://192.168.8.102/twiki/bin/view/TWiki/TWikiSite (topic [] skin [print] rev [
↪1.20] )
http://192.168.8.102/twiki/bin/view/TWiki/TWikiSiteTools (topic [] skin [print]
↪rev [1.6] )
http://192.168.8.102/twiki/bin/view/TWiki/TWikiSkins (topic [] skin [print] rev
↪[1.10] sel [] )
http://192.168.8.102/twiki/bin/view/TWiki/TWikiSystemRequirements (topic [] skin
↪ [print] rev [1.27] )
http://192.168.8.102/twiki/bin/view/TWiki/TWikiTemplates (topic [] skin [print]
↪rev [1.17] )
http://192.168.8.102/twiki/bin/view/TWiki/TWikiTopics (topic [] skin [print] rev
↪ [1.11] )
http://192.168.8.102/twiki/bin/view/TWiki/TWikiTutorial (topic [] skin [print] r
↪ev [1.11] )
http://192.168.8.102/twiki/bin/view/TWiki/TWikiUpgradeGuide (topic [] skin [prin
↪t] rev [1.2] )
http://192.168.8.102/twiki/bin/view/TWiki/TWikiUserAuthentication (topic [] skin
↪ [print] rev [1.14] )
http://192.168.8.102/twiki/bin/view/TWiki/TWikiVariables (topic [] skin [print]
↪rev [1.61] )
http://192.168.8.102/twiki/bin/view/TWiki/TextFormattingFAQ (topic [] skin [prin
↪t] rev [1.13] )
http://192.168.8.102/twiki/bin/view/TWiki/TextFormattingRules (topic [] skin [pr
↪int] rev [1.36] )
http://192.168.8.102/twiki/bin/view/TWiki/WebChanges (topic [] skin [print] rev
↪[1.2] )
http://192.168.8.102/twiki/bin/view/TWiki/WebChangesAlert (topic [] skin [print]
↪ rev [1.12] )
http://192.168.8.102/twiki/bin/view/TWiki/WebHome (topic [] skin [print] rev [1.
↪77] unlock [on] )
http://192.168.8.102/twiki/bin/view/TWiki/WebIndex (topic [] skin [print] rev [1
↪.1] )
http://192.168.8.102/twiki/bin/view/TWiki/WebNotify (topic [] skin [print] rev [
↪1.4] )
```

... continues on next page ...

... continued from previous page ...

```
http://192.168.8.102/twiki/bin/view/TWiki/WebPreferences (topic [] skin [print]
↪rev [1.16] )
http://192.168.8.102/twiki/bin/view/TWiki/WebSearch (topic [] skin [print] rev [
↪1.11] )
http://192.168.8.102/twiki/bin/view/TWiki/WebStatistics (topic [] skin [print] r
↪ev [1.2] )
http://192.168.8.102/twiki/bin/view/TWiki/WebTopicList (topic [] skin [print] )
http://192.168.8.102/twiki/bin/view/TWiki/WelcomeGuest (topic [] skin [print] re
↪v [1.19] )
http://192.168.8.102/twiki/bin/view/TWiki/WikiCulture (topic [] skin [print] rev
↪ [1.7] )
http://192.168.8.102/twiki/bin/view/TWiki/WikiName (topic [] skin [print] rev [1
↪.2] )
http://192.168.8.102/twiki/bin/view/TWiki/WindowsInstallCookbook (topic [] skin
↪[print] rev [1.2] )
http://192.168.8.102/twiki/bin/viewfile/TWiki/FileAttachment (filename [Sample.t
↪xt] rev [] )
http://192.168.8.102/twiki/bin/viewfile/TWiki/TWiki/FileAttachment (rev [] filen
↪ame [Sample.txt] )
http://192.168.8.102/view/TWiki/TWikiHistory (rev [1.9] )
```

Log Method
Details:CGI Scanning Consolidation
OID:1.3.6.1.4.1.25623.1.0.111038
Version used: $Revision: 5907 $

Log (CVSS: 0.0)
NVT: DIRB (NASL wrapper)

Summary
This script uses DIRB to find directories and files on web applications via brute forcing. See the preferences section for configuration options.

Vulnerability Detection Result

```
This are the directories/files found with brute force:
http://192.168.8.102:80/
```

Log Method
Details:DIRB (NASL wrapper)
OID:1.3.6.1.4.1.25623.1.0.103079
Version used: $Revision: 4685 $

Log (CVSS: 0.0)
NVT: Fingerprint web server with favicon.ico

... continues on next page ...

... continued from previous page ...

Summary
The remote web server contains a graphic image that is prone to information disclosure.

Vulnerability Detection Result
```
The following apps/services were identified:
"phpmyadmin (2.11.8.1)" fingerprinted by the file: "http://192.168.8.102/phpMyAd
↪min/favicon.ico"
```

Impact
The 'favicon.ico' file found on the remote web server belongs to a popular webserver/application. This may be used to fingerprint the webserver/application.

Solution
Solution type: Mitigation
Remove the 'favicon.ico' file or create a custom one for your site.

Log Method
Details:`Fingerprint web server with favicon.ico`
OID:1.3.6.1.4.1.25623.1.0.20108
Version used: `$Revision: 4988 $`

Log (CVSS: 0.0)
NVT: HTTP Server type and version

Summary
This detects the HTTP Server's type and version.

Vulnerability Detection Result
```
The remote web server type is :
Apache/2.2.8 (Ubuntu) DAV/2
Solution : You can set the directive "ServerTokens Prod" to limit
the information emanating from the server in its response headers.
```

Solution
Configure your server to use an alternate name like 'Wintendo httpD w/Dotmatrix display' Be sure to remove common logos like apache_pb.gif. With Apache, you can set the directive 'ServerTokens Prod' to limit the information emanating from the server in its response headers.

Log Method
Details:`HTTP Server type and version`
OID:1.3.6.1.4.1.25623.1.0.10107
Version used: `$Revision: 5943 $`

... continues on next page ...

... continued from previous page ...

Log (CVSS: 0.0)
NVT: Nikto (NASL wrapper)

Summary
This plugin uses nikto(1) to find weak CGI scripts and other known issues regarding web server security. See the preferences section for configuration options.

Vulnerability Detection Result

```
Here is the Nikto report:
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          192.168.8.102
+ Target Hostname:    192.168.8.102
+ Target Port:        80
+ Start Time:         2017-05-11 01:27:31 (GMT0)
---------------------------------------------------------------------------
+ Server: Apache/2.2.8 (Ubuntu) DAV/2
+ Retrieved x-powered-by header: PHP/5.2.4-2ubuntu5.10
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user a
↪gent to protect against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent
↪to render the content of the site in a different fashion to the MIME type
+ Apache/2.2.8 appears to be outdated (current is at least Apache/2.4.12). Apach
↪e 2.0.65 (final release) and 2.2.29 are also current.
+ Uncommon header 'tcn' found, with contents: list
+ Apache mod_negotiation is enabled with MultiViews, which allows attackers to e
↪asily brute force file names. See http://www.wisec.it/sectou.php?id=4698ebdc59
↪d15. The following alternatives for 'index' were found: index.php
+ Web Server returns a valid response with junk HTTP methods, this may cause fal
↪se positives.
+ OSVDB-877: HTTP TRACE method is active, suggesting the host is vulnerable to X
↪ST
+ /phpinfo.php?VARIABLE=<script>alert('Vulnerable')</script>: Output from the ph
↪pinfo() function was found.
+ OSVDB-3268: /doc/: Directory indexing found.
+ OSVDB-48: /doc/: The /doc/ directory is browsable. This may be /usr/doc.
+ OSVDB-12184: /?=PHPB8B5F2A0-3C92-11d3-A3A9-4C7B08C10000: PHP reveals potential
↪ly sensitive information via certain HTTP requests that contain specific QUERY
↪ strings.
+ OSVDB-12184: /?=PHPE9568F36-D428-11d2-A769-00AA001ACF42: PHP reveals potential
↪ly sensitive information via certain HTTP requests that contain specific QUERY
↪ strings.
+ OSVDB-12184: /?=PHPE9568F34-D428-11d2-A769-00AA001ACF42: PHP reveals potential
↪ly sensitive information via certain HTTP requests that contain specific QUERY
↪ strings.
+ OSVDB-12184: /?=PHPE9568F35-D428-11d2-A769-00AA001ACF42: PHP reveals potential
```

... continues on next page ...

... continued from previous page ...

```
↪ly sensitive information via certain HTTP requests that contain specific QUERY
↪ strings.
+ OSVDB-3092: /phpMyAdmin/changelog.php: phpMyAdmin is for managing MySQL databa
↪ses, and should be protected or limited to authorized hosts.
+ Server leaks inodes via ETags, header found with file /phpMyAdmin/ChangeLog, i
↪node: 92462, size: 40540, mtime: Tue Dec  9 17:24:00 2008
+ OSVDB-3092: /phpMyAdmin/ChangeLog: phpMyAdmin is for managing MySQL databases,
↪ and should be protected or limited to authorized hosts.
+ OSVDB-3268: /test/: Directory indexing found.
+ OSVDB-3092: /test/: This might be interesting...
+ /phpinfo.php: Output from the phpinfo() function was found.
+ OSVDB-3233: /phpinfo.php: PHP is installed, and a test script which runs phpin
↪fo() was found. This gives a lot of system information.
+ OSVDB-3268: /icons/: Directory indexing found.
+ /phpinfo.php?GLOBALS[test]=<script>alert(document.cookie);</script>: Output fr
↪om the phpinfo() function was found.
+ /phpinfo.php?cx[]=QVCQUmpwxZtxd7ZFonakwnQceNfdQ8NIR4PwWrxy9IEHO5Xk3PuTDFyKCNVf
↪gbBZqmw6ofrGYs0ALJwKlBboeIKySv5rXv4cR6MzwLWnDuRY6lBKro0TReUuKe6Hm2RxofZj6dyb0y
↪Yt5gx3ZfJlrJC3JHpNqzWhCGTgxp7l1RYq4wBYa7tl3YRRbOA3Sd1kI0yw1x85BGDuOg67n1bx28fb
↪PcsKiFQbtf8C4QIzt2nUW9sExl74zlb6k6yCq0NB62FoT0pCWRtxJvWCUZFNtMY082IhejiJ5Dupbj
↪mMBivC8yoLyzXiFeLBsN3ImzuMAyL1RxyxayD86etpnnXMJkA2Ci2v9CK8TYF18FmDWRVb8g3QBwhY
↪8W6VoGUo8lsdzEzRrc2zBPEEcE2MaJwvArvdLkep6PEExSZyWtImEaB6KzllgokB3e9YE2OnENR9WD
↪y0Dpcc2EjTbEo2RhS8YUeeabI0k5ONNXxb9mjExmspsuBkvoe1XOjrG4Fi8iuXAzHCim4CktVM4Ovd
↪VC60PeTavcyDKwSEBtvLUxoMgZdubKUn3rjF7WJspLh63j4A57BIRNA0kaBt8FxdKwNYWphfG0Jytz
↪ctmiTJaIl0QZof9fNH2epWblRz4U8OqPCgBDF9cTL4S55vo95YV83VeWXRfDwKKsVtB2o8daA7lUDz
↪9G5DRrHWZndUcmxpe5evbrEMMyuIilzssnH3JjPDe6DZ4Um126h2ICy4z0PpWqfRSnZbnhBkDnoFZD
↪07gpUm7qr56Od6RAVAAEEpTkxHKvTGhdKmq69X3S5fQSzJ111ZImz0dfZvSnpHKGSL2uPNFQ3JgA7T
↪LD9TZFUtCEUWRN3Tmjyqa4R2jwDS9GMUNYiqzQizu8E5GWcyOR8B4LNr2rXJYBuJ9MWpmZrkTaYV6K
↪mxGwqtHbj21mBLzNUlZCcEbKXxBe0w3mqCtjy9p5SEAHvyECd0w1MHKRDlSwvJ1voP4cCnAXgEpJhF
↪Vf5WKMfJpDNouV32c2uzjv4tkHnzbsNDOVLShGXCzaaUMKy1K9HPMiTZ4pSTtciVQrA7Yvai2KRqTq
↪BPK6P3NUnAmn2K3KDbKYdrGj5kWFTtRbgl7pLfEoPFwbyJmtcj1WAlL4TDErFP6IFqrpsCZcOcvSsL
↪BNP2qqAlQILAcsbODAZHKH4wvMicth1TOFr8Lx9B8dT5OO46KUhsXzKVFpqDMAOdFqI3EkstantdMN
↪oBpwDfBrD8QT9NCMDU8FqzHCmp1zJGzumM2FksYou9xxp5WwKOZyTtsxQVV2OWd1Da5ZbuEyz9NYhq
↪eTVBaVYnTKTPtoR31RIf22S8vB6IRjDZrsFHS5hHJvhm5wRktRMv6hAsTd25a2OtNirwFiVC6tIUaC
↪GznlJWooxMxCicdiCNLl3laVohcc7otQT7uQFCMbOjvVqS2XBrTEQTRk4Sfs1i9ZNG31qMcKcSPNIy
↪v3xVP1flqkO9tico5DgH17GYKjd9kKHjfV1aft7GgCfziOv5NAFE8AdL6d360N6uiNCVO9mOpu26yH
↪GvJDGTGoumMJ20CP9ur6R2b6iWLCPz9CL13zio5mtWJPHsVetdm9OV5osSJioyqc7QQCwZedYRKUoa
↪ZecHezCFe66nZue25S8MS5mACIZwhtFGfzKlq9zqvN2xStpuXrN4DsyVbsAbWKaMBRGrvr2BWJcfNk
↪WB9szC3Bu9YIXkud7Xggt8hB28UxGzjSjH5bn4qwTXy2O7w4txFQ9NfhJy5MmoaDBEZzSk5gMLgT4n
↪FKKO2dTR2ymgNPOL13JldII0ff6f0WUrlbeQ9YAVkQgAXF5EeXmXVhefvKFTbtVRbe6jHjdvF7jVr4
↪Tm95OyOyZwHXI22sUPVNV1KvjULTmM4FtoETDy6kRJh6UR0GAj1cVr1taMNwbS1kSQ0BowqsZi53RP
↪GCWbJ8KU4e8P5pp3Vxbp8hTQbh4GC6YcGlyUKUXQkDJdNoTqc0QQbeEIJCLLJg9Tb4CcDkWD8GM412
↪acgiQYkzSYZOnySEunkQPgyONEwihFYfiHQJ3l50IlY6u5CmW5bUV6N5lG4HwQqFMejfzcOFVpCi5m
↪Qx6EQ8jeJhdKs6KXfnS20AdfBkP4DAvudTIQU37Fyucc7a75ps11wlPFuGIMEGV6dnvcYar7hGw9xG
↪fRQOzJbvZY3Vw5jhGGBmJrOG1zKdlsM4ZrQTK2kHqaak35Jz5okUOwmw34LBkHvYPdnDRYOZJymgde
↪Te5EQA0vnWwQeTpOkNzBUhGtlqUXhc5Wmuqj5oZ53czJuluVBpvu7wb421iJA4TzXEJBzesP80nJCH
↪vAxz0U7nozKD5W6BHfPAUzhpKd8Rh9THkjRIykBwyPGdnuv9c4oLHkNKmi0i8Dhh1uCk66riudOQQm
```

... continues on next page ...

... continued from previous page ...

```
↪0o75ClnQ0MzdL33W6Y2DHM3zk7knuiRNHvHFlFAz7pXfQYquEUG3qGqpJHcISofE0gQJQNvspOZ0eY
↪bHZctHOKFtUwt2ELxxCAmlmAXU1HtVgFucJOTzXcIUnd0WrpPqD5M53KZaGObIsbyE6I1eavE1gaNw
↪yN3J9VnOMlhCrTfhHsUwNOnZ3WB1e3HBtH7Y1JEhir6ohKKCGRVxdRS2sgdKeyCrHt71dU76n322JU
↪8YGcB0vhVlneskOZDS9bAKaUzvkmkuphKdp7GPU0utBrXCkfEZ4aUnOUuAi6Z1EsdCrT6m39xczHBH
↪Et7cApzdAr4abjpuMZ0GxAE3qNf3DUJcOb5QyhL49wogbiSFNlJmFx3TMrIwNwFx44jk7jF04D7cYM
↪wRwNIjQkexQJqqMjF7ZeWuG6aU8etcBrcpb4gBE3YnSM5HsWjoY82LvlheL4BHSwLIvLbmEXMftOqw
↪NJoNHWIxF2VG19edFVk77H6Zuyd2pkdP375J5GacIJs3ArTNrlS9I1TdLXfYuDg1yzGhaEfvE1zVt8
↪c0XOSLhOZKIPhQAVGgy2C0pE2tF3VAGPPJ4jeT7ZOMEn4LLCaVTM8w2EOK9e7OB7xfGVh25J1857j2
↪jrqsHT23N9axq1qTi8OfRU39wVX9RCfw6xFAJ9iOEStIQXVqzCI84nDskhPhG2OWPsjWSxBuXkmSxA
↪isTLccCOQKRAarMCOWwdGPl2RoBBJjzPZgbED73jPvWuY67UGWT6YFXhBIz7M1HafFpyWn4BbwFc9Z
↪t9lI1C6n2eivvvnGzeiSVHPT5LShfOFFcbuPUdWxAVBPHuAszhtLQZyFtRFVOJSHUxZPj4owU7yu4W
↪A5Z0zS380Cq0t3bCIEHcTgtIRgB1I0xQBAViXOaH9ooB6Uvm0Jpqql6Jz5039eqwjdzk9cbHOpoTVs
↪ZMB9pdvCcedhPrq4fHib2w09f2USEI12sbIkkXpcmruwA3sVzRSxKWjtSpS39CcD0C0DsBQZE12bV3
↪nh9x3Rhv7Xk9HoFXqTrcR2Y6hs4DbpOFbWeFQ3OBwPCy22yGfKQTthRmztD45bHQyp94FZ0z14u4Zc
↪1UEFXw81KmTD0GG5v7e0WY9fsFkQ33WMh7GJGcgrlS1FJs7YyaL2qz1JFEY4wgZX6mK5iUGMItLoYj
↪TyiIHIeIqiu79Lq2F4gUymUBCroTWy12uH8cc9izbmcjoH1d1iiXNsEqVX9Ips6tOITx88gvEuSHzV
↪eEWOlLtmYs8yzJyo7kZlpQqVrNvSC6BoEuaE9UM8JuAzv9ZMzf3LMg7OAH0XVoFyd7f3aYX4tvsm4Q
↪H8ryXdMDwNihgOU2X7NPeuWdr4p1YjFhdTpauNVn4UcDZFO0SGz5qdmL34xef7xwsSJaxKD5rMJPhj
↪bv5wjDNxsSzKGYzgjVsCIGdR1wdHNeMyncJnnaqwTDafqufG6SOCMmkzXaM1WEXtWeyeFJEs1Bpg14
↪NKBk5Z0ZM0FcUaoKOZ2CediOiMK871mlPqH8Jos0cNq6yEFjyUQCCsdbtILxwIII7w9vakPWDN5Cb2
↪3OKw6lb1xixmOPzQE9AvF2luZNnzwptMzPzAtkjRNzGDaqzTGii4bVkIIoQUUVvWVJrPcwTM08xs6s
↪BZ5VlqvIwWrBKT29iSUbCUt3JAztzRNUGOsDWl0jRFeF38huQND2qS6pbX<script>alert(foo)</
↪script>: Output from the phpinfo() function was found.
+ OSVDB-3233: /icons/README: Apache default file found.
+ /phpMyAdmin/: phpMyAdmin directory found
+ OSVDB-3092: /phpMyAdmin/Documentation.html: phpMyAdmin is for managing MySQL d
↪atabases, and should be protected or limited to authorized hosts.
+ 8349 requests: 2 error(s) and 29 item(s) reported on remote host
+ End Time:           2017-05-11 01:28:38 (GMT0) (67 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

Log Method
Details:Nikto (NASL wrapper)
OID:1.3.6.1.4.1.25623.1.0.14260
Version used: $Revision: 4685 $

Log (CVSS: 0.0)
NVT: PHP Version Detection (Remote)

Summary
Detection of installed version of PHP. This script sends HTTP GET request and try to get the version from the response, and sets the result in KB.

Vulnerability Detection Result
Detected PHP
Version: 5.2.4

... continues on next page ...

... continued from previous page ...

```
Location: tcp/80
CPE:      cpe:/a:php:php:5.2.4
Concluded from version/product identification result:
X-Powered-By: PHP/5.2.4-2ubuntu5.10
```

Log Method
Details:`PHP Version Detection (Remote)`
OID:1.3.6.1.4.1.25623.1.0.800109
Version used: `$Revision: 4724 $`

Log (CVSS: 0.0)
NVT: phpMyAdmin Detection

Summary
Detection of phpMyAdmin.
The script sends a connection request to the server and attempts to extract the version number from the reply.

Vulnerability Detection Result

```
Detected phpMyAdmin
Version:  3.1.1
Location: /phpMyAdmin
CPE:      cpe:/a:phpmyadmin:phpmyadmin:3.1.1
Concluded from version/product identification result:
Version 3.1.1
```

Log Method
Details:`phpMyAdmin Detection`
OID:1.3.6.1.4.1.25623.1.0.900129
Version used: `$Revision: 3669 $`

Log (CVSS: 0.0)
NVT: Services

Summary
This routine attempts to guess which service is running on the remote ports. For instance, it searches for a web server which could listen on another port than 80 or 443 and makes this information available for other check routines.

Vulnerability Detection Result

```
A web server is running on this port
```

Log Method
Details:`Services`
OID:1.3.6.1.4.1.25623.1.0.10330

... continues on next page ...

... continued from previous page ...

Version used: $Revision: 5180 $

Log (CVSS: 0.0)
NVT: Tiki Wiki CMS Groupware Version Detection

Summary
Detection of Tiki Wiki CMS Groupware, a open source web application is a wiki-based CMS.
The script sends a connection request to the web server and attempts to extract the version number from the reply.

Vulnerability Detection Result
```
Detected Tiki Wiki CMS Groupware
Version:  1.9.5
Location: /tikiwiki
CPE:      cpe:/a:tiki:tikiwiki_cms/groupware:1.9.5
Concluded from version/product identification result:
version 1.9.5
Concluded from version/product identification location:
http://192.168.8.102/tikiwiki/README
```

Log Method
Details:Tiki Wiki CMS Groupware Version Detection
OID:1.3.6.1.4.1.25623.1.0.901001
Version used: $Revision: 5144 $

References
```
Other:
  URL:http://tiki.org/
```

Log (CVSS: 0.0)
NVT: TWiki Version Detection

Summary
Detection of installed version of TWiki.
This script sends HTTP GET request and try to get the version from the response, and sets the result in KB.

Vulnerability Detection Result
```
Detected TWiki
Version:  01.Feb.2003
Location: /twiki/bin
CPE:      cpe:/a:twiki:twiki:01.Feb.2003
Concluded from version/product identification result:
This site is running TWiki version <strong>01 Feb 2003</strong>
```

... continues on next page ...

. . . continued from previous page . . .

Log Method
Details:`TWiki Version Detection`
OID:1.3.6.1.4.1.25623.1.0.800399
Version used: `$Revision: 4427 $`

[return to 192.168.8.102]

2.1.49 Log 1099/tcp

Log (CVSS: 0.0)
NVT: RMI-Registry Detection

Summary
This Script detects the RMI-Registry Service

Vulnerability Detection Result
`The RMI-Registry Service is running at this port`

Log Method
Details:`RMI-Registry Detection`
OID:1.3.6.1.4.1.25623.1.0.105839
Version used: `$Revision: 4034 $`

[return to 192.168.8.102]

2.1.50 Log general/icmp

Log (CVSS: 0.0)
NVT: ICMP Timestamp Detection

Summary
The remote host responded to an ICMP timestamp request. The Timestamp Reply is an ICMP message which replies to a Timestamp message. It consists of the originating timestamp sent by the sender of the Timestamp as well as a receive timestamp and a transmit timestamp. This information could theoretically be used to exploit weak time-based random number generators in other services.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Log Method
Details:`ICMP Timestamp Detection`
OID:1.3.6.1.4.1.25623.1.0.103190
Version used: `$Revision: 5309 $`

. . . continues on next page . . .

... continued from previous page ...

References
CVE: CVE-1999-0524
Other:
URL:http://www.ietf.org/rfc/rfc0792.txt

[return to 192.168.8.102]

2.1.51 Log 139/tcp

Log (CVSS: 0.0)
NVT: SMB/CIFS Server Detection

Summary
This script detects wether port 445 and 139 are open and if they are running a CIFS/SMB server.

Vulnerability Detection Result
A SMB server is running on this port

Log Method
Details:SMB/CIFS Server Detection
OID:1.3.6.1.4.1.25623.1.0.11011
Version used: $Revision: 4261 $

[return to 192.168.8.102]

2.1.52 Log 25/tcp

Log (CVSS: 0.0)
NVT: Identify Unknown Services with nmap

Summary
This plugin performs service detection by launching nmap's service probe (nmap -sV) against ports that are running unidentified services.

Vulnerability Detection Result
Nmap service detection result for this port: smtp
This is a guess. A confident identification of the service was not possible.

Log Method
Details:Identify Unknown Services with nmap
OID:1.3.6.1.4.1.25623.1.0.66286
Version used: $Revision: 5296 $

Log (CVSS: 0.0)
NVT: Services

Summary
This routine attempts to guess which service is running on the remote ports. For instance, it searches for a web server which could listen on another port than 80 or 443 and makes this information available for other check routines.

Vulnerability Detection Result
`An unknown service is running on this port.`
`It is usually reserved for SMTP`

Log Method
Details:`Services`
OID:1.3.6.1.4.1.25623.1.0.10330
Version used: `$Revision: 5180 $`

[return to 192.168.8.102]