Security Scan Report

Generated on: 2025-05-11 16:52:16

Nmap Scan Results:

```
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-05-11 16:51 EDT
Nmap scan report for 10.0.2.5
Host is up (0.00061s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
53/tcp   open  domain      ISC BIND 9.4.2
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp  open  rpcbind     2 (RPC #100000)
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp  open  exec        netkit-rsh rexecd
513/tcp  open  login       OpenBSD or Solaris rlogind
514/tcp  open  tcpwrapped
1099/tcp open  java-rmi    GNU Classpath grmiregistry
1524/tcp open  bindshell   Metasploitable root shell
2049/tcp open  nfs         2-4 (RPC #100003)
2121/tcp open  ftp         ProFTPD 1.3.1
3306/tcp open  mysql       MySQL 5.0.51a-3ubuntu5
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp open  vnc         VNC (protocol 3.3)
6000/tcp open  X11         (access denied)
6667/tcp open  irc         UnrealIRCd
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 08:00:27:B6:96:A5 (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
Network Distance: 1 hop
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN;
OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

OS and Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 13.46 seconds
```

Security Scan Report

Generated on: 2025-05-11 16:52:16

AI Vulnerability Analysis:

The NMAP scan results show the services running on the host, the software versions and other relative network information. Here are some potential vulnerabilities uncovered by the scan:

1. The FTP service is running vsftpd 2.3.4. This version has a known vulnerability (CVE-2011-0762) related to overly verbose error messages which may reveal sensitive information that could assist an attacker.

2. The SSH service is running OpenSSH 4.7p1. Multiple vulnerabilities (CVE-2008-1483, CVE-2008-1657 and CVE-2008-3259) tied to this version have been reported.

3. Apache HTTPD 2.2.8 in use has multiple vulnerabilities including CVE-2008-2939, CVE-2008-2364 and CVE-2008-3257.

4. The version ISC BIND 9.4.2 of Domain Name Server service could be exploitable due to a deficiency in record parsing (CVE-2008-1447).

5. The SMB service uses Samba versions between 3 to 4. There is a known vulnerability called 'Eternal Blue' (CVE-2017-0144) related to these versions.

6. GNU Classpath's rmiregistry has several reported vulnerabilities such as CVE-2008-3214.

7. Netkit-rsh’s rexecd, OpenBSD or Solaris rlogind, and bindshell running on port 1524 are all known to be insecure and have multiple vulnerabilities, some of which allow arbitrary remote code execution.

8. MySQL version 5.0.51a-3ubuntu5 has multiple vulnerabilities, including but not filled CVE-2008-2079, CVE-2008-3963, and CVE-2008-4456.

9. ProFTPD 1.3.1 is known to have critical vulnerabilities such as CVE-2010-4221, which allows an unauthenticated attacker to cause a denial of service.

Overall, this host seems to be poorly maintained with many outdated versions of services running which have known exploitable vulnerabilities. Updating the software regularly and disabling unnecessary services can significantly improve the security posture of the system.

Security Scan Report

Generated on: 2025-05-11 16:52:16

CVE Details:

=== CVE-2011-0762 ===
Title: CVE-2011-0762
Description: The vsf_filename_passes_filter function in ls.c in vsftpd before 2.3.3 allows remote authenticated users to cause a denial of service (CPU consumption and process slot exhaustion) via crafted glob expressions in STAT commands in multiple FTP sessions, a different vulnerability than CVE-2010-2632.
CVSS v3 Score: 4.0 (MEDIUM)
Vector: AV:N/AC:L/Au:S/C:N/I:N/A:P
Published: 2011-03-02T20:00:01
References:
- http://www.debian.org/security/2011/dsa-2305
- http://www.exploit-db.com/exploits/16270
- http://www.vupen.com/english/advisories/2011/0639
- http://www.vupen.com/english/advisories/2011/0668
- https://exchange.xforce.ibmcloud.com/vulnerabilities/65873
- http://lists.opensuse.org/opensuse-security-announce/2011-05/msg00005.html
- ftp://vsftpd.beasts.org/users/cevans/untar/vsftpd-2.3.4/Changelog
- http://securityreason.com/securityalert/8109
- http://www.securityfocus.com/bid/46617
- http://securityreason.com/achievement_securityalert/95
- http://www.securityfocus.com/archive/1/516748/100/0/threaded
- http://cxib.net/stuff/vspoc232.c
- http://marc.info/?l=bugtraq&m=133226187115472&w=2
- http://lists.fedoraproject.org/pipermail/package-announce/2011-March/055881.html
- http://lists.fedoraproject.org/pipermail/package-announce/2011-March/055957.html
- http://lists.fedoraproject.org/pipermail/package-announce/2011-March/055882.html
- http://bugs.debian.org/cgi-bin/bugreport.cgi?bug=622741
- http://www.vupen.com/english/advisories/2011/0713
- http://www.mandriva.com/security/advisories?name=MDVSA-2011:049
- http://www.redhat.com/support/errata/RHSA-2011-0337.html
- http://www.vupen.com/english/advisories/2011/0547
- http://jvn.jp/en/jp/JVN37417423/index.html
- http://www.ubuntu.com/usn/USN-1098-1
- http://www.kb.cert.org/vuls/id/590604
- http://www.securitytracker.com/id?1025186

=== CVE-2017-0144 ===
Title: CVE-2017-0144
Description: The SMBv1 server in Microsoft Windows Vista SP2; Windows Server 2008 SP2 and R2 SP1; Windows 7 SP1; Windows 8.1; Windows Server 2012 Gold and R2; Windows RT 8.1; and Windows 10

Gold, 1511, and 1607; and Windows Server 2016 allows remote attackers to execute arbitrary code via crafted packets, aka "Windows SMB Remote Code Execution Vulnerability." This vulnerability is different from those described in CVE-2017-0143, CVE-2017-0145, CVE-2017-0146, and CVE-2017-0148.
CVSS v3 Score: 8.8 (HIGH)
Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
Published: 2017-03-17T00:59:04
References:
- http://packetstormsecurity.com/files/156196/SMB-DOUBLEPULSAR-Remote-Code-Execution.html
- https://cert-portal.siemens.com/productcert/pdf/ssa-701903.pdf
- https://www.exploit-db.com/exploits/41891/
- http://www.securitytracker.com/id/1037991
- https://ics-cert.us-cert.gov/advisories/ICSMA-18-058-02
- http://packetstormsecurity.com/files/154690/DOUBLEPULSAR-Payload-Execution-Neutralization.html
- https://www.exploit-db.com/exploits/42031/
- https://cert-portal.siemens.com/productcert/pdf/ssa-966341.pdf
- http://www.securityfocus.com/bid/96704
- https://www.exploit-db.com/exploits/42030/
- https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-0144
- https://www.exploit-db.com/exploits/41987/

=== CVE-2008-1447 ===
Title: CVE-2008-1447
Description: The DNS protocol, as implemented in (1) BIND 8 and 9 before 9.5.0-P1, 9.4.2-P1, and 9.3.5-P1; (2) Microsoft DNS in Windows 2000 SP4, XP SP2 and SP3, and Server 2003 SP1 and SP2; and other implementations allow remote attackers to spoof DNS traffic via a birthday attack that uses in-bailiwick referrals to conduct cache poisoning against recursive resolvers, related to insufficient randomness of DNS transaction IDs and source ports, aka "DNS Insufficient Socket Entropy Vulnerability" or "the Kaminsky bug."
CVSS v3 Score: 6.8 (MEDIUM)
Vector: CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:C/C:N/I:H/A:N
Published: 2008-07-08T23:41:00
References:
- http://secunia.com/advisories/30989
- https://exchange.xforce.ibmcloud.com/vulnerabilities/43637
- http://secunia.com/advisories/31236
- http://secunia.com/advisories/30979
- http://support.citrix.com/article/CTX118183
- http://www.securitytracker.com/id?1020578
- http://rhn.redhat.com/errata/RHSA-2008-0533.html
- http://www.securitytracker.com/id?1020702
- http://www.vupen.com/english/advisories/2008/2123/references
- http://www.novell.com/support/viewContent.do?externalId=7000912

Security Scan Report

Generated on: 2025-05-11 16:52:18

- http://support.nortel.com/go/main.jsp?cscat=BLTNDETAIL&id=762152
- http://www.kb.cert.org/vuls/id/800113
- http://secunia.com/advisories/31900
- http://secunia.com/advisories/30977
- http://wiki.rpath.com/wiki/Advisories:rPSA-2008-0231
- http://secunia.com/advisories/31019
- http://www.vupen.com/english/advisories/2008/2383
- http://secunia.com/advisories/31204
- http://secunia.com/advisories/31422
- https://docs.microsoft.com/en-us/security-updates/securitybulletins/2008/ms08-037
- http://www.securitytracker.com/id?1020449
- http://www.doxpara.com/DMK_BO2K8.ppt
- http://security.freebsd.org/advisories/FreeBSD-SA-08:06.bind.asc
- http://secunia.com/advisories/31237
- http://www.securitytracker.com/id?1020576
- http://www.securitytracker.com/id?1020804
- http://www.ibm.com/support/docview.wss?uid=isg1IZ26667
- http://www.bluecoat.com/support/security-advisories/dns_cache_poisoning
- http://secunia.com/advisories/31031
- http://security.gentoo.org/glsa/glsa-200812-17.xml
- http://secunia.com/advisories/31213
- http://secunia.com/advisories/31254
- http://secunia.com/advisories/31022
- http://www.vupen.com/english/advisories/2008/2050/references
- http://secunia.com/advisories/31354
- http://sunsolve.sun.com/search/document.do?assetkey=1-26-239392-1
- http://www.caughq.org/exploits/CAU-EX-2008-0003.txt
- http://www.us-cert.gov/cas/techalerts/TA08-260A.html
- http://slackware.com/security/viewer.php?l=slackware-security&y=2008&m=slackware-security.452680
- http://www.securitytracker.com/id?1020448
- http://www.securityfocus.com/archive/1/495869/100/0/threaded
- http://www.vupen.com/english/advisories/2009/0297
- http://www.securitytracker.com/id?1020558
- http://www.debian.org/security/2008/dsa-1619
- http://secunia.com/advisories/30980
- https://oval.cisecurity.org/repository/search/definition/oval%3Aorg.mitre.oval%3Adef%3A5917
- http://www.ibm.com/support/docview.wss?uid=isg1IZ26671
- http://www.vupen.com/english/advisories/2008/2051/references
- http://www.vupen.com/english/advisories/2008/2334
- http://up2date.astaro.com/2008/08/up2date_7202_released.html
- http://www.vupen.com/english/advisories/2008/2196/references
- http://www.ibm.com/support/docview.wss?uid=isg1IZ26672
- http://www.rtpro.yamaha.co.jp/RT/FAQ/Security/VU800113.html

- http://www.securitytracker.com/id?1020440
- http://www.vupen.com/english/advisories/2008/2023/references
- http://www.vupen.com/english/advisories/2008/2113/references
- http://secunia.com/advisories/30925
- http://support.apple.com/kb/HT3026
- http://secunia.com/advisories/31207
- http://secunia.com/advisories/31011
- http://wiki.rpath.com/wiki/Advisories:rPSA-2010-0018
- http://secunia.com/advisories/31151
- http://secunia.com/advisories/31093
- http://secunia.com/advisories/31052
- http://www.nominum.com/asset_upload_file741_2661.pdf
- http://www.isc.org/index.pl?/sw/bind/bind-security.php
- http://www.vupen.com/english/advisories/2008/2195/references
- http://www.us-cert.gov/cas/techalerts/TA08-190B.html
- https://www.exploit-db.com/exploits/6130
- http://www.kb.cert.org/vuls/id/MIMG-7DWR4J
- http://www.debian.org/security/2008/dsa-1603
- http://www.caughq.org/exploits/CAU-EX-2008-0002.txt
- http://www.doxpara.com/?p=1176
- http://www.unixwiz.net/techtips/iguide-kaminsky-dns-vuln.html
- http://www.securitytracker.com/id?1020560
- http://www.securitytracker.com/id?1020561
- http://www.vupen.com/english/advisories/2008/2114/references
- http://www.vmware.com/security/advisories/VMSA-2008-0014.html
- http://www.vupen.com/english/advisories/2008/2466
- http://www.ibm.com/support/docview.wss?uid=isg1IZ26670
- http://www.ruby-lang.org/en/news/2008/08/08/multiple-vulnerabilities-in-ruby/
- ftp://ftp.netbsd.org/pub/NetBSD/security/advisories/NetBSD-SA2008-009.txt.asc
- http://www.vupen.com/english/advisories/2008/2582
- http://secunia.com/advisories/31030
- https://www.exploit-db.com/exploits/6123
- http://secunia.com/advisories/31212
- http://secunia.com/advisories/33714
- http://www.ubuntu.com/usn/usn-622-1
- http://www.debian.org/security/2008/dsa-1604
- http://www.kb.cert.org/vuls/id/MIMG-7ECL8Q
- https://oval.cisecurity.org/repository/search/definition/oval%3Aorg.mitre.oval%3Adef%3A5761
- http://www.debian.org/security/2008/dsa-1623
- http://secunia.com/advisories/31137
- http://secunia.com/advisories/31495
- http://www.securitytracker.com/id?1020575
- http://secunia.com/advisories/30988

Security Scan Report

Generated on: 2025-05-11 16:52:18

- http://www.securitytracker.com/id?1020548
- http://www.vupen.com/english/advisories/2008/2377
- http://slackware.com/security/viewer.php?l=slackware-security&y=2008&m=slackware-security.539239
- http://lists.apple.com/archives/security-announce//2008/Sep/msg00004.html
- https://exchange.xforce.ibmcloud.com/vulnerabilities/43334
- https://oval.cisecurity.org/repository/search/definition/oval%3Aorg.mitre.oval%3Adef%3A9627
- http://secunia.com/advisories/33786
- http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=c01523520
- http://sunsolve.sun.com/search/document.do?assetkey=1-26-240048-1
- http://www.vupen.com/english/advisories/2008/2092/references
- http://www.securitytracker.com/id?1020651
- http://lists.apple.com/archives/security-announce//2008/Jul/msg00003.html
- http://secunia.com/advisories/31882
- http://www.vupen.com/english/advisories/2008/2025/references
- http://www.securitytracker.com/id?1020653
- http://www.cisco.com/en/US/products/products_security_advisory09186a00809c2168.shtml
- http://secunia.com/advisories/31033
- http://secunia.com/advisories/31823
- http://www.mandriva.com/security/advisories?name=MDVSA-2008:139
- https://oval.cisecurity.org/repository/search/definition/oval%3Aorg.mitre.oval%3Adef%3A5725
- http://marc.info/?l=bugtraq&m=123324863916385&w=2
- http://www.debian.org/security/2008/dsa-1605
- http://lists.apple.com/archives/security-announce//2008/Sep/msg00003.html
- http://www.vupen.com/english/advisories/2008/2268
- http://secunia.com/advisories/31221
- http://www.vupen.com/english/advisories/2008/2525
- http://secunia.com/advisories/33178
- http://lists.opensuse.org/opensuse-security-announce/2008-07/msg00003.html
- http://secunia.com/advisories/30998
- http://security.gentoo.org/glsa/glsa-201209-25.xml
- http://www.securitytracker.com/id?1020438
- http://secunia.com/advisories/31152
- http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=c01662368
- http://secunia.com/advisories/31482
- http://marc.info/?l=bugtraq&m=121866517322103&w=2
- http://www.securitytracker.com/id?1020577
- http://secunia.com/advisories/31014
- http://secunia.com/advisories/31451
- http://www.vupen.com/english/advisories/2008/2166/references
- http://www.securityfocus.com/bid/30131
- http://secunia.com/advisories/31326
- http://www.vupen.com/english/advisories/2008/2291
- http://lists.apple.com/archives/security-announce//2008/Sep/msg00005.html

Security Scan Report

Generated on: 2025-05-11 16:52:18

- http://www.securitytracker.com/id?1020802
- http://www.securitytracker.com/id?1020437
- http://secunia.com/advisories/31065
- http://www.vupen.com/english/advisories/2008/2029/references
- https://www.exploit-db.com/exploits/6122
- http://www.vupen.com/english/advisories/2008/2342
- http://lists.opensuse.org/opensuse-security-announce/2008-08/msg00006.html
- http://secunia.com/advisories/30973
- http://secunia.com/advisories/31143
- http://www.ipcop.org/index.php?name=News&file=article&sid=40
- http://www.vupen.com/english/advisories/2008/2549
- http://www.openbsd.org/errata42.html#013_bind
- http://www.us-cert.gov/cas/techalerts/TA08-190A.html
- http://www.vupen.com/english/advisories/2008/2055/references
- http://support.apple.com/kb/HT3129
- http://www.vupen.com/english/advisories/2008/2584
- http://www.securitytracker.com/id?1020579
- https://www.redhat.com/archives/fedora-package-announce/2008-July/msg00402.html
- http://www.vupen.com/english/advisories/2008/2482
- http://secunia.com/advisories/31153
- http://marc.info/?l=bugtraq&m=121630706004256&w=2
- https://oval.cisecurity.org/repository/search/definition/oval%3Aorg.mitre.oval%3Adef%3A12117
- http://blog.invisibledenizen.org/2008/07/kaminskys-dns-issue-accidentally-leaked.html
- http://www.openbsd.org/errata43.html#004_bind
- http://www.ibm.com/support/docview.wss?uid=isg1IZ26669
- http://www.vupen.com/english/advisories/2008/2197/references
- http://secunia.com/advisories/31197
- http://www.ubuntu.com/usn/usn-627-1
- http://marc.info/?l=bugtraq&m=141879471518471&w=2
- http://www.vupen.com/english/advisories/2008/2467
- http://secunia.com/advisories/31588
- http://secunia.com/advisories/31209
- http://www.vupen.com/english/advisories/2008/2052/references
- http://www.vupen.com/english/advisories/2010/0622
- http://secunia.com/advisories/31430
- http://secunia.com/advisories/31199
- http://security.gentoo.org/glsa/glsa-200807-08.xml
- http://www.securityfocus.com/archive/1/495289/100/0/threaded
- http://lists.grok.org.uk/pipermail/full-disclosure/2008-August/064118.html
- http://secunia.com/advisories/31072
- https://www.redhat.com/archives/fedora-package-announce/2008-July/msg00458.html
- http://bugs.debian.org/cgi-bin/bugreport.cgi?bug=494401
- http://www.ibm.com/support/docview.wss?uid=isg1IZ26668

- http://www.phys.uu.nl/~rombouts/pdnsd.html
- http://www.vupen.com/english/advisories/2009/0311
- http://www.vupen.com/english/advisories/2008/2030/references
- http://www.vupen.com/english/advisories/2008/2384
- http://secunia.com/advisories/31687
- http://secunia.com/advisories/31169
- http://www.vupen.com/english/advisories/2008/2019/references
- http://www.phys.uu.nl/~rombouts/pdnsd/ChangeLog
- http://www.vupen.com/english/advisories/2008/2558
- http://www.redhat.com/support/errata/RHSA-2008-0789.html
- http://secunia.com/advisories/31012
- http://secunia.com/advisories/31094
- http://www.vupen.com/english/advisories/2008/2139/references
- http://support.citrix.com/article/CTX117991

=== CVE-2008-2364 ===
Title: CVE-2008-2364
Description: The ap_proxy_http_process_response function in mod_proxy_http.c in the mod_proxy module in the Apache HTTP Server 2.0.63 and 2.2.8 does not limit the number of forwarded interim responses, which allows remote HTTP servers to cause a denial of service (memory consumption) via a large number of interim responses.
CVSS v3 Score: 5.0 (MEDIUM)
Vector: AV:N/AC:L/Au:N/C:N/I:N/A:P
Published: 2008-06-13T18:41:00
References:
- http://www.redhat.com/support/errata/RHSA-2008-0966.html
- http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=c01539432
- http://secunia.com/advisories/30621
- http://secunia.com/advisories/33156
- http://secunia.com/advisories/33797
-
https://lists.apache.org/thread.html/r0276683d8e1e07153fc8642618830ac0ade85b9ae0dc7b07f63bb8fc%40%3Ccvs.h
-
https://lists.apache.org/thread.html/r8c9983f1172a3415f915ddb7e14de632d2d0c326eb1285755a024165%40%3Ccvs.
-
https://lists.apache.org/thread.html/f7f95ac1cd9895db2714fa3ebaa0b94d0c6df360f742a40951384a53%40%3Ccvs.htt
- https://oval.cisecurity.org/repository/search/definition/oval%3Aorg.mitre.oval%3Adef%3A11713
- https://oval.cisecurity.org/repository/search/definition/oval%3Aorg.mitre.oval%3Adef%3A6084
- https://www.redhat.com/archives/fedora-package-announce/2008-August/msg00055.html
- http://www.securityfocus.com/archive/1/498567/100/0/threaded
- http://www.securityfocus.com/archive/1/494858/100/0/threaded
- http://rhn.redhat.com/errata/RHSA-2008-0967.html

Security Scan Report

Generated on: 2025-05-11 16:52:18

-
http://svn.apache.org/viewvc/httpd/httpd/trunk/modules/proxy/mod_proxy_http.c?r1=666154&r2=666153&pathrev=666
- http://marc.info/?l=bugtraq&m=123376588623823&w=2
- http://secunia.com/advisories/31404
-
https://lists.apache.org/thread.html/rfbaf647d52c1cb843e726a0933f156366a806cead84fbd430951591b%40%3Ccvs.ht
- https://exchange.xforce.ibmcloud.com/vulnerabilities/42987
- http://www.ubuntu.com/usn/USN-731-1
-
https://lists.apache.org/thread.html/r75cbe9ea3e2114e4271bbeca7aff96117b50c1b6eb7c4772b0337c1f%40%3Ccvs.h
- https://oval.cisecurity.org/repository/search/definition/oval%3Aorg.mitre.oval%3Adef%3A9577
- http://secunia.com/advisories/31651
-
https://lists.apache.org/thread.html/r7dd6be4dc38148704f2edafb44a8712abaa3a2be120d6c3314d55919%40%3Ccvs.
- http://www.securityfocus.com/bid/29653
- http://www.oracle.com/technetwork/topics/security/cpujuly2013-1899826.html
- http://sunsolve.sun.com/search/document.do?assetkey=1-26-247666-1
- http://lists.opensuse.org/opensuse-security-announce/2009-03/msg00001.html
- http://www-1.ibm.com/support/docview.wss?uid=swg1PK67579
- http://lists.apple.com/archives/security-announce/2008/Oct/msg00001.html
-
https://lists.apache.org/thread.html/r8828e649175df56f1f9e3919938ac7826128525426e2748f0ab62feb%40%3Ccvs.ht
-
https://lists.apache.org/thread.html/r57608dc51b79102f3952ae06f54d5277b649c86d6533dcd6a7d201f7%40%3Ccvs.h
-
https://lists.apache.org/thread.html/rdca61ae990660bacb682295f2a09d34612b7bb5f457577fe17f4d064%40%3Ccvs.h
-
https://lists.apache.org/thread.html/8d63cb8e9100f28a99429b4328e4e7cebce861d5772ac9863ba2ae6f%40%3Ccvs.h
- http://secunia.com/advisories/31904
-
https://lists.apache.org/thread.html/r9e8622254184645bc963a1d47c5d47f6d5a36d6f080d8d2c43b2b142%40%3Ccvs.
- http://www-01.ibm.com/support/docview.wss?uid=swg27008517
-
https://lists.apache.org/thread.html/rc4c53a0d57b2771ecd4b965010580db355e38137c8711311ee1073a8%40%3Ccvs
- http://secunia.com/advisories/34259
- http://support.apple.com/kb/HT3216
- http://secunia.com/advisories/31416
- http://secunia.com/advisories/32222
- http://www.vupen.com/english/advisories/2008/1798
- http://secunia.com/advisories/31026
- http://www.vupen.com/english/advisories/2008/2780
- http://wiki.rpath.com/wiki/Advisories:rPSA-2008-0328
- http://secunia.com/advisories/34219

- http://www.securityfocus.com/bid/31681
-
https://lists.apache.org/thread.html/r9ea3538f229874c80a10af473856a81fbf5f694cd7f471cc679ba70b%40%3Ccvs.http
- http://marc.info/?l=bugtraq&m=125631037611762&w=2
- http://www.securitytracker.com/id?1020267
-
https://lists.apache.org/thread.html/r2cb985de917e7da0848c440535f65a247754db8b2154a10089e4247b%40%3Ccvs
-
https://lists.apache.org/thread.html/r9f93cf6dde308d42a9c807784e8102600d0397f5f834890708bf6920%40%3Ccvs.ht
-
https://lists.apache.org/thread.html/r84d043c2115176958562133d96d851495d712aa49da155d81f6733be%40%3Ccvs
- http://secunia.com/advisories/32838
- http://secunia.com/advisories/32685
- http://www.mandriva.com/security/advisories?name=MDVSA-2008:237
- https://www.redhat.com/archives/fedora-package-announce/2008-August/msg00153.html
- http://www.mandriva.com/security/advisories?name=MDVSA-2008:195
-
https://lists.apache.org/thread.html/5df9bfb86a3b054bb985a45ff9250b0332c9ecc181eec232489e7f79%40%3Ccvs.http
-
https://lists.apache.org/thread.html/rf6449464fd8b7437704c55f88361b66f12d5b5f90bcce66af4be4ba9%40%3Ccvs.http
- http://lists.opensuse.org/opensuse-security-announce/2009-03/msg00004.html
- http://security.gentoo.org/glsa/glsa-200807-06.xml
-
https://lists.apache.org/thread.html/54a42d4b01968df1117cea77fc53d6beb931c0e05936ad02af93e9ac%40%3Ccvs.ht
- http://secunia.com/advisories/34418
- http://www.vupen.com/english/advisories/2009/0320

=== CVE-2008-2939 ===
Title: CVE-2008-2939
Description: Cross-site scripting (XSS) vulnerability in proxy_ftp.c in the mod_proxy_ftp module in Apache 2.0.63 and earlier, and mod_proxy_ftp.c in the mod_proxy_ftp module in Apache 2.2.9 and earlier 2.2 versions, allows remote attackers to inject arbitrary web script or HTML via a wildcard in the last directory component in the pathname in an FTP URI.
CVSS v3 Score: 4.3 (MEDIUM)
Vector: AV:N/AC:M/Au:N/C:N/I:P/A:N
Published: 2008-08-06T18:41:00
References:
- http://www.redhat.com/support/errata/RHSA-2008-0966.html
- http://svn.apache.org/viewvc?view=rev&revision=682871
- http://secunia.com/advisories/33156
- http://secunia.com/advisories/33797
- http://www-1.ibm.com/support/docview.wss?uid=swg1PK70937

-
https://lists.apache.org/thread.html/r0276683d8e1e07153fc8642618830ac0ade85b9ae0dc7b07f63bb8fc%40%3Ccvs.h
- http://www.kb.cert.org/vuls/id/663763
-
https://lists.apache.org/thread.html/f7f95ac1cd9895db2714fa3ebaa0b94d0c6df360f742a40951384a53%40%3Ccvs.http
- https://oval.cisecurity.org/repository/search/definition/oval%3Aorg.mitre.oval%3Adef%3A11316
- http://www.us-cert.gov/cas/techalerts/TA09-133A.html
- http://www.securityfocus.com/archive/1/498567/100/0/threaded
-
https://lists.apache.org/thread.html/54a42d4b01968df1117cea77fc53d6beb931c0e05936ad02af93e9ac%40%3Ccvs.ht
- http://rhn.redhat.com/errata/RHSA-2008-0967.html
- http://marc.info/?l=bugtraq&m=123376588623823&w=2
- http://secunia.com/advisories/31384
-
https://lists.apache.org/thread.html/rfbaf647d52c1cb843e726a0933f156366a806cead84fbd430951591b%40%3Ccvs.ht
- http://www.securityfocus.com/archive/1/495180/100/0/threaded
- http://www.ubuntu.com/usn/USN-731-1
- http://www.securityfocus.com/archive/1/498566/100/0/threaded
-
https://lists.apache.org/thread.html/r7dd6be4dc38148704f2edafb44a8712abaa3a2be120d6c3314d55919%40%3Ccvs.
-
https://lists.apache.org/thread.html/r75cbe9ea3e2114e4271bbeca7aff96117b50c1b6eb7c4772b0337c1f%40%3Ccvs.h
- http://secunia.com/advisories/35074
- http://www.mandriva.com/security/advisories?name=MDVSA-2009:124
- http://sunsolve.sun.com/search/document.do?assetkey=1-26-247666-1
- http://www.securityfocus.com/bid/30560
- http://lists.opensuse.org/opensuse-security-announce/2008-11/msg00000.html
- http://svn.apache.org/viewvc?view=rev&revision=682868
-
https://lists.apache.org/thread.html/r8828e649175df56f1f9e3919938ac7826128525426e2748f0ab62feb%40%3Ccvs.ht
-
https://lists.apache.org/thread.html/r57608dc51b79102f3952ae06f54d5277b649c86d6533dcd6a7d201f7%40%3Ccvs.h
-
https://lists.apache.org/thread.html/rdca61ae990660bacb682295f2a09d34612b7bb5f457577fe17f4d064%40%3Ccvs.h
-
https://lists.apache.org/thread.html/8d63cb8e9100f28a99429b4328e4e7cebce861d5772ac9863ba2ae6f%40%3Ccvs.h
-
https://lists.apache.org/thread.html/rb9c9f42dafa25d2f669dac2a536a03f2575bc5ec1be6f480618aee10%40%3Ccvs.htt
-
https://lists.apache.org/thread.html/r9e8622254184645bc963a1d47c5d47f6d5a36d6f080d8d2c43b2b142%40%3Ccvs.
-
https://lists.apache.org/thread.html/rc4c53a0d57b2771ecd4b965010580db355e38137c8711311ee1073a8%40%3Ccvs
- http://www.vupen.com/english/advisories/2008/2461

- http://lists.apple.com/archives/security-announce/2009/May/msg00002.html
- https://lists.apache.org/thread.html/r5f9c22f9c28adbd9f00556059edc7b03a5d5bb71d4bb80257c0d34e4%40%3Ccvs.h
- http://secunia.com/advisories/31673
- http://www.mandriva.com/security/advisories?name=MDVSA-2008:194
- https://oval.cisecurity.org/repository/search/definition/oval%3Aorg.mitre.oval%3Adef%3A7716
- http://wiki.rpath.com/Advisories:rPSA-2008-0327
- http://www.securitytracker.com/id?1020635
- http://secunia.com/advisories/34219
- http://wiki.rpath.com/wiki/Advisories:rPSA-2008-0328
- https://lists.apache.org/thread.html/r9ea3538f229874c80a10af473856a81fbf5f694cd7f471cc679ba70b%40%3Ccvs.htt
- http://marc.info/?l=bugtraq&m=125631037611762&w=2
- https://lists.apache.org/thread.html/r2cb985de917e7da0848c440535f65a247754db8b2154a10089e4247b%40%3Ccvs
- https://lists.apache.org/thread.html/r9f93cf6dde308d42a9c807784e8102600d0397f5f834890708bf6920%40%3Ccvs.ht
- http://www.rapid7.com/advisories/R7-0033
- https://lists.apache.org/thread.html/r84d043c2115176958562133d96d851495d712aa49da155d81f6733be%40%3Ccvs
- http://secunia.com/advisories/32838
- http://secunia.com/advisories/32685
- http://www.vupen.com/english/advisories/2009/1297
- http://www.mandriva.com/security/advisories?name=MDVSA-2008:195
- https://lists.apache.org/thread.html/5df9bfb86a3b054bb985a45ff9250b0332c9ecc181eec232489e7f79%40%3Ccvs.htt
- http://svn.apache.org/viewvc?view=rev&revision=682870
- https://lists.apache.org/thread.html/rf6449464fd8b7437704c55f88361b66f12d5b5f90bcce66af4be4ba9%40%3Ccvs.htt
- http://support.apple.com/kb/HT3549
- http://www.vupen.com/english/advisories/2008/2315
- https://exchange.xforce.ibmcloud.com/vulnerabilities/44223
- http://www.vupen.com/english/advisories/2009/0320
- http://www-1.ibm.com/support/docview.wss?uid=swg1PK70197

=== CVE-2008-3257 ===

Title: CVE-2008-3257

Description: Stack-based buffer overflow in the Apache Connector (mod_wl) in Oracle WebLogic Server (formerly BEA WebLogic Server) 10.3 and earlier allows remote attackers to execute arbitrary code via a long HTTP version string, as demonstrated by a string after "POST /.jsp" in an HTTP request.

CVSS v3 Score: 10.0 (HIGH)

Vector: AV:N/AC:L/Au:N/C:C/I:C/A:C

Published: 2008-07-22T16:41:00
References:
- http://www.securitytracker.com/id?1020520
- http://www.oracle.com/technology/deploy/security/alerts/alert_cve2008-3257.html
- https://support.bea.com/application_content/product_portlets/securityadvisories/2793.html
- http://secunia.com/advisories/31146
- http://www.securityfocus.com/bid/30273
- http://www.kb.cert.org/vuls/id/716387
- http://blogs.oracle.com/security/2008/07/security_alert_for_cve-2008-3257_released.html
- http://www.vupen.com/english/advisories/2008/2145/references
- https://www.exploit-db.com/exploits/6089
- http://www.attrition.org/pipermail/vim/2008-July/002035.html
- http://www.attrition.org/pipermail/vim/2008-July/002036.html
- https://exchange.xforce.ibmcloud.com/vulnerabilities/43885

=== CVE-2008-3259 ===
Title: CVE-2008-3259
Description: OpenSSH before 5.1 sets the SO_REUSEADDR socket option when the X11UseLocalhost configuration setting is disabled, which allows local users on some platforms to hijack the X11 forwarding port via a bind to a single IP address, as demonstrated on the HP-UX platform.
CVSS v3 Score: 1.2 (LOW)
Vector: AV:L/AC:H/Au:N/C:P/I:N/A:N
Published: 2008-07-22T16:41:00
References:
- http://www.vupen.com/english/advisories/2008/2148
- http://www.securitytracker.com/id?1020537
- http://www.openssh.com/txt/release-5.1
- https://exchange.xforce.ibmcloud.com/vulnerabilities/43940
- http://www.securityfocus.com/bid/30339
- http://secunia.com/advisories/31179
- http://openssh.com/security.html

=== CVE-2008-2079 ===
Title: CVE-2008-2079
Description: MySQL 4.1.x before 4.1.24, 5.0.x before 5.0.60, 5.1.x before 5.1.24, and 6.0.x before 6.0.5 allows local users to bypass certain privilege checks by calling CREATE TABLE on a MyISAM table with modified (1) DATA DIRECTORY or (2) INDEX DIRECTORY arguments that are within the MySQL home data directory, which can point to tables that are created in the future.
CVSS v3 Score: 4.6 (MEDIUM)
Vector: AV:N/AC:H/Au:S/C:P/I:P/A:P
Published: 2008-05-05T16:20:00

References:
- https://oval.cisecurity.org/repository/search/definition/oval%3Aorg.mitre.oval%3Adef%3A10133
- http://dev.mysql.com/doc/refman/5.0/en/releasenotes-es-5-0-60.html
- http://secunia.com/advisories/31226
- http://dev.mysql.com/doc/refman/4.1/en/news-4-1-24.html
- http://secunia.com/advisories/36566
- http://www.redhat.com/support/errata/RHSA-2008-0510.html
- http://secunia.com/advisories/30134
- http://lists.apple.com/archives/security-announce/2008/Oct/msg00001.html
- http://dev.mysql.com/doc/refman/6.0/en/news-6-0-5.html
- http://lists.apple.com/archives/security-announce/2009/Sep/msg00004.html
- http://www.redhat.com/support/errata/RHSA-2008-0768.html
- http://secunia.com/advisories/31066
- http://www.vupen.com/english/advisories/2008/1472/references
- http://www.mandriva.com/security/advisories?name=MDVSA-2008:150
- http://www.securitytracker.com/id?1019995
- http://www.ubuntu.com/usn/USN-671-1
- http://support.apple.com/kb/HT3216
- http://support.apple.com/kb/HT3865
- https://exchange.xforce.ibmcloud.com/vulnerabilities/42267
- http://www.debian.org/security/2008/dsa-1608
- http://secunia.com/advisories/32222
- http://www.mandriva.com/security/advisories?name=MDVSA-2008:149
- http://secunia.com/advisories/31687
- http://www.redhat.com/support/errata/RHSA-2008-0505.html
- http://www.redhat.com/support/errata/RHSA-2009-1289.html
- http://www.vupen.com/english/advisories/2008/2780
- http://www.securityfocus.com/bid/31681
- http://lists.opensuse.org/opensuse-security-announce/2008-08/msg00006.html
- http://dev.mysql.com/doc/refman/5.1/en/news-5-1-24.html
- http://bugs.mysql.com/bug.php?id=32167
- http://secunia.com/advisories/36701
- http://www.securityfocus.com/bid/29106
- http://secunia.com/advisories/32769

=== CVE-2008-3963 ===
Title: CVE-2008-3963
Description: MySQL 5.0 before 5.0.66, 5.1 before 5.1.26, and 6.0 before 6.0.6 does not properly handle a b'' (b single-quote single-quote) token, aka an empty bit-string literal, which allows remote attackers to cause a denial of service (daemon crash) by using this token in a SQL statement.
CVSS v3 Score: 4.0 (MEDIUM)
Vector: AV:N/AC:L/Au:S/C:N/I:N/A:P

Published: 2008-09-11T01:13:47
References:
- https://oval.cisecurity.org/repository/search/definition/oval%3Aorg.mitre.oval%3Adef%3A10521
- http://www.openwall.com/lists/oss-security/2008/09/09/7
- http://www.mandriva.com/security/advisories?name=MDVSA-2009:094
- http://dev.mysql.com/doc/refman/5.1/en/news-5-1-26.html
- http://www.openwall.com/lists/oss-security/2008/09/09/4
- http://dev.mysql.com/doc/refman/5.0/en/releasenotes-es-5-0-66.html
- http://www.debian.org/security/2009/dsa-1783
- http://secunia.com/advisories/36566
- http://www.securitytracker.com/id?1020858
- http://lists.opensuse.org/opensuse-security-announce/2008-11/msg00001.html
- http://secunia.com/advisories/32759
- http://secunia.com/advisories/34907
- http://bugs.mysql.com/bug.php?id=35658
- http://www.ubuntu.com/usn/USN-671-1
- https://bugs.gentoo.org/237166
- http://www.vupen.com/english/advisories/2008/2554
- http://www.redhat.com/support/errata/RHSA-2009-1289.html
- http://dev.mysql.com/doc/refman/6.0/en/news-6-0-6.html
- http://www.redhat.com/support/errata/RHSA-2009-1067.html
- http://secunia.com/advisories/31769
- http://www.ubuntu.com/usn/USN-1397-1
- https://exchange.xforce.ibmcloud.com/vulnerabilities/45042
- http://secunia.com/advisories/32769

=== CVE-2010-4221 ===
Title: CVE-2010-4221
Description: Multiple stack-based buffer overflows in the pr_netio_telnet_gets function in netio.c in ProFTPD before 1.3.3c allow remote attackers to execute arbitrary code via vectors involving a TELNET IAC escape character to a (1) FTP or (2) FTPS server.
CVSS v3 Score: 10.0 (HIGH)
Vector: AV:N/AC:L/Au:N/C:C/I:C/A:C
Published: 2010-11-09T21:00:06
References:
- http://www.zerodayinitiative.com/advisories/ZDI-10-229/
- http://www.vupen.com/english/advisories/2010/2959
- http://lists.fedoraproject.org/pipermail/package-announce/2010-November/050703.html
- http://lists.fedoraproject.org/pipermail/package-announce/2010-November/050687.html
- http://bugs.proftpd.org/show_bug.cgi?id=3521
- http://www.securityfocus.com/bid/44562
- http://www.proftpd.org/docs/NEWS-1.3.3c

Security Scan Report

Generated on: 2025-05-11 16:52:20

- http://secunia.com/advisories/42217
- http://www.vupen.com/english/advisories/2010/2962
- http://secunia.com/advisories/42052
- http://lists.fedoraproject.org/pipermail/package-announce/2010-November/050726.html
- http://www.mandriva.com/security/advisories?name=MDVSA-2010:227
- http://www.vupen.com/english/advisories/2010/2941

=== CVE-2008-1657 ===
Title: CVE-2008-1657
Description: OpenSSH 4.4 up to versions before 4.9 allows remote authenticated users to bypass the sshd_config ForceCommand directive by modifying the .ssh/rc session file.
CVSS v3 Score: 6.5 (MEDIUM)
Vector: AV:N/AC:L/Au:S/C:P/I:P/A:P
Published: 2008-04-02T18:44:00
References:

- http://secunia.com/advisories/32080
- http://secunia.com/advisories/29939
- http://aix.software.ibm.com/aix/efixes/security/ssh_advisory.asc
- http://www.vupen.com/english/advisories/2008/1035/references
- http://wiki.rpath.com/wiki/Advisories:rPSA-2008-0139
- http://www.vupen.com/english/advisories/2008/2396
- http://www.vupen.com/english/advisories/2008/1624/references
- http://www.securityfocus.com/archive/1/490488/100/0/threaded
- http://secunia.com/advisories/29683
- http://secunia.com/advisories/31882
- http://www.gentoo.org/security/en/glsa/glsa-200804-03.xml
- http://secunia.com/advisories/29609
- http://www.openssh.com/txt/release-4.9
- http://www.ubuntu.com/usn/usn-649-1
- http://secunia.com/advisories/29735
- https://exchange.xforce.ibmcloud.com/vulnerabilities/41549
- http://secunia.com/advisories/29602
- http://secunia.com/advisories/32110
- ftp://ftp.netbsd.org/pub/NetBSD/security/advisories/NetBSD-SA2008-005.txt.asc
- http://www.securityfocus.com/bid/28531
- http://secunia.com/advisories/29693
- http://www.mandriva.com/security/advisories?name=MDVSA-2008:098
- http://secunia.com/advisories/31531
- http://lists.apple.com/archives/security-announce//2008/Sep/msg00005.html
- http://secunia.com/advisories/30361
- http://lists.opensuse.org/opensuse-security-announce/2008-04/msg00007.html
- http://www.openbsd.org/errata43.html#001_openssh

- http://www.us-cert.gov/cas/techalerts/TA08-260A.html
- http://support.attachmate.com/techdocs/2374.html
- https://issues.rpath.com/browse/RPL-2419
- http://www.vupen.com/english/advisories/2008/2584
- http://www.securitytracker.com/id?1019733

=== CVE-2008-3214 ===
Title: CVE-2008-3214
Description: dnsmasq 2.25 allows remote attackers to cause a denial of service (daemon crash) by (1) renewing a nonexistent lease or (2) sending a DHCPREQUEST for an IP address that is not in the same network, related to the DHCP NAK response from the daemon.
CVSS v3 Score: 7.8 (HIGH)
Vector: AV:N/AC:L/Au:N/C:N/I:N/A:C
Published: 2008-07-18T16:41:00
References:
- http://www.openwall.com/lists/oss-security/2008/06/30/7
- http://www.openwall.com/lists/oss-security/2008/07/12/3
- https://bugs.launchpad.net/ubuntu/+source/dnsmasq/+bug/47438
- http://www.thekelleys.org.uk/dnsmasq/CHANGELOG
- http://www.openwall.com/lists/oss-security/2008/07/02/4
- http://www.openwall.com/lists/oss-security/2008/07/01/8
- http://www.openwall.com/lists/oss-security/2008/07/03/4
- https://exchange.xforce.ibmcloud.com/vulnerabilities/43929
- http://www.openwall.com/lists/oss-security/2008/07/08/8
- http://freshmeat.net/projects/dnsmasq/?branch_id=1991&release_id=217681

=== CVE-2008-1483 ===
Title: CVE-2008-1483
Description: OpenSSH 4.3p2, and probably other versions, allows local users to hijack forwarded X connections by causing ssh to set DISPLAY to :10, even when another process is listening on the associated port, as demonstrated by opening TCP port 6010 (IPv4) and sniffing a cookie sent by Emacs.
CVSS v3 Score: 6.9 (MEDIUM)
Vector: AV:L/AC:M/Au:N/C:C/I:C/A:C
Published: 2008-03-24T23:44:00
References:
- http://secunia.com/advisories/30347
- http://bugs.debian.org/cgi-bin/bugreport.cgi?bug=463011
- http://security.FreeBSD.org/advisories/FreeBSD-SA-08:05.openssh.asc
- http://www.debian.org/security/2008/dsa-1576
- http://www.securityfocus.com/bid/28444
- http://secunia.com/advisories/29939

- http://aix.software.ibm.com/aix/efixes/security/ssh_advisory.asc
- https://oval.cisecurity.org/repository/search/definition/oval%3Aorg.mitre.oval%3Adef%3A6085
- http://secunia.com/advisories/29537
- http://www.securityfocus.com/archive/1/490054/100/0/threaded
- http://www.vupen.com/english/advisories/2008/1526/references
- http://secunia.com/advisories/30249
- http://secunia.com/advisories/29676
- http://sunsolve.sun.com/search/document.do?assetkey=1-26-237444-1
- http://www.vupen.com/english/advisories/2008/2396
- http://secunia.com/advisories/29686
- http://www.vupen.com/english/advisories/2008/1624/references
- http://secunia.com/advisories/29683
- http://secunia.com/advisories/31882
- http://www.slackware.org/security/viewer.php?l=slackware-security&y=2008&m=slackware-security.540188
- http://secunia.com/advisories/29873
- http://www.gentoo.org/security/en/glsa/glsa-200804-03.xml
- http://secunia.com/advisories/29522
- http://secunia.com/advisories/29735
- http://www.vupen.com/english/advisories/2008/1124/references
- ftp://ftp.netbsd.org/pub/NetBSD/security/advisories/NetBSD-SA2008-005.txt.asc
- http://secunia.com/advisories/29626
- http://wiki.rpath.com/wiki/Advisories:rPSA-2008-0120
- http://secunia.com/advisories/29721
- https://exchange.xforce.ibmcloud.com/vulnerabilities/41438
- http://sunsolve.sun.com/search/document.do?assetkey=1-77-1019235.1-1
- http://www.securitytracker.com/id?1019707
- http://www.mandriva.com/security/advisories?name=MDVSA-2008:078
- https://issues.rpath.com/browse/RPL-2397
- http://tools.cisco.com/security/center/content/CiscoSecurityNotice/CVE-2008-1483
- http://www.globus.org/mail_archive/security-announce/2008/04/msg00000.html
- http://secunia.com/advisories/31531
- http://secunia.com/advisories/29554
- http://lists.apple.com/archives/security-announce//2008/Sep/msg00005.html
- http://www.vupen.com/english/advisories/2008/0994/references
- http://secunia.com/advisories/30230
- https://usn.ubuntu.com/597-1/
- http://www.vupen.com/english/advisories/2008/1123/references
- http://www.vupen.com/english/advisories/2008/1630/references
- http://secunia.com/advisories/30361
- http://www.vupen.com/english/advisories/2008/1448/references
- http://lists.opensuse.org/opensuse-security-announce/2008-04/msg00007.html
- http://www.us-cert.gov/cas/techalerts/TA08-260A.html

- http://support.avaya.com/elmodocs2/security/ASA-2008-205.htm
- http://support.attachmate.com/techdocs/2374.html
- http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=c01462841
- http://secunia.com/advisories/30086
- http://www.vupen.com/english/advisories/2008/2584
- http://sourceforge.net/project/shownotes.php?release_id=590180&group_id=69227

=== CVE-2008-4456 ===
Title: CVE-2008-4456
Description: Cross-site scripting (XSS) vulnerability in the command-line client in MySQL 5.0.26 through 5.0.45, and other versions including versions later than 5.0.45, when the --html option is enabled, allows attackers to inject arbitrary web script or HTML by placing it in a database cell, which might be accessed by this client when composing an HTML document. NOTE: as of 20081031, the issue has not been fixed in MySQL 5.0.67.
CVSS v3 Score: 2.6 (LOW)
Vector: AV:N/AC:H/Au:N/C:N/I:P/A:N
Published: 2008-10-06T23:25:50
References:
- https://oval.cisecurity.org/repository/search/definition/oval%3Aorg.mitre.oval%3Adef%3A11456
- http://www.securityfocus.com/archive/1/497158/100/0/threaded
- http://seclists.org/bugtraq/2008/Oct/0026.html
- http://www.mandriva.com/security/advisories?name=MDVSA-2009:094
- http://lists.apple.com/archives/security-announce/2010//Mar/msg00001.html
- http://www.debian.org/security/2009/dsa-1783
- http://securityreason.com/securityalert/4357
- http://secunia.com/advisories/36566
- http://www.securityfocus.com/archive/1/496877/100/0/threaded
- http://secunia.com/advisories/38517
- http://www.redhat.com/support/errata/RHSA-2010-0110.html
- http://www.securityfocus.com/archive/1/497885/100/0/threaded
- http://secunia.com/advisories/34907
- http://www.henlich.de/it-security/mysql-command-line-client-html-injection-vulnerability
- http://bugs.mysql.com/bug.php?id=27884
- http://www.redhat.com/support/errata/RHSA-2009-1289.html
- http://www.securityfocus.com/archive/1/496842/100/0/threaded
- http://www.ubuntu.com/usn/USN-1397-1
- http://support.apple.com/kb/HT4077
- http://ubuntu.com/usn/usn-897-1
- https://exchange.xforce.ibmcloud.com/vulnerabilities/45590
- http://www.securityfocus.com/bid/31486
- http://secunia.com/advisories/32072