NMAPTEST EXECUTIVE SUMMARY OF PRELIMINARY RESULTS

April 18, 2019

Automatically generated by MARPT

Contents

1 Executive Summary 2
2 Technical Specifics 3
2.1 Overall results summary 3
2.2 Vulnerability details of host: 192.168.1.101 4
3 Raw Scripts Information 184

1 EXECUTIVE SUMMARY

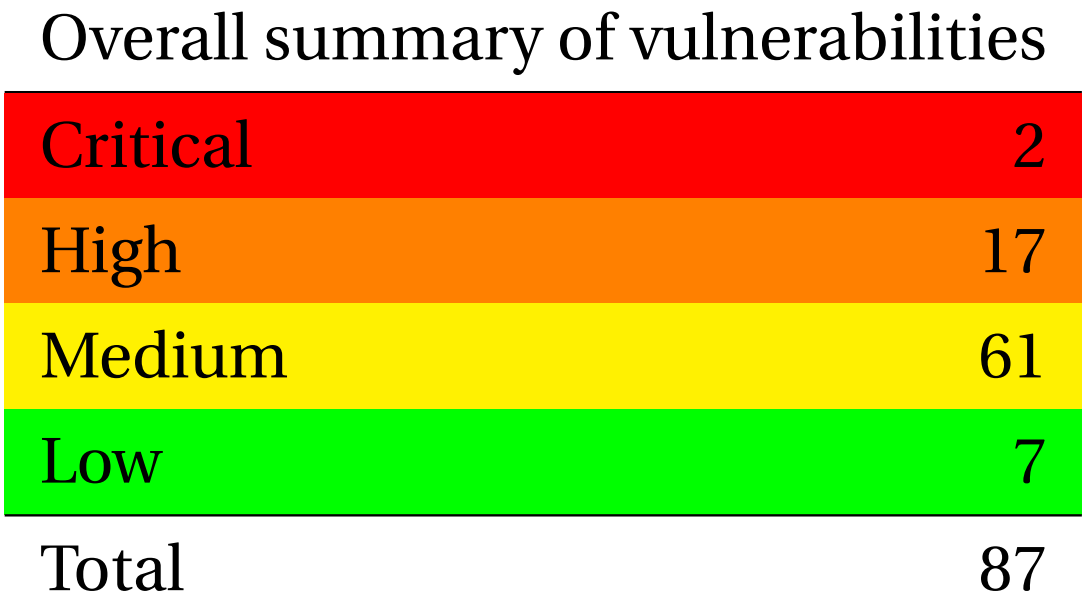
This report was generated to provide the senior management of NmapTest with information from the preliminary information gathering and vulnerability analysis steps taken.Initial results show MEDIUM risk to the tested infrastructure. A risk assessment should be completed soon to allow controls to be implemented to reduce the risk to a manageable level as there is a medium probability of a threat occuring.

2 TECHNICAL SPECIFICS

Beneath is information on the Hosts that have been scanned so far, including the IP Address, Port and discovered Vendors. Information on potential vulnerabilities identified and the severity scores of each is also available.

Host information		
Host	Ports	OS
192.168.1.101	21 22 25 80 139 443 445 512 513 514 666 3306 5901 6001 8080 8443 9080	No OS identifi
Scan start time	Thu Apr 18 12:00:46 2019	
Scan end time	Thu Apr 18 12:03:29 2019	

2.1 Overall results summary



2.2 Vulnerability details of host: 192.168.1.101

Overall summary of vulnerabilities	
Critical	2
High	17
Medium	61
Low	7
Total	87

Summary

OpenSSH 5.6 and earlier, when J-PAKE is enabled, does not properly validate the public parameters in the J-PAKE protocol, which 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, a related issue to CVE-2010-4252.

CVE-2010-4478 Information	
CVSS Score	7.5
CWE	CWE-287
Vulnerability impact	
Confidentiality	PARTIAL
Integrity	PARTIAL
Availability	PARTIAL
Access methodology information	
Vector	NETWORK
Complexity	LOW
Authentication	NONE

Vulnerable configs

OpenBSD OpenSSH 1.2 OpenBSD OpenSSH 1.2.1 OpenBSD OpenSSH 1.2.2

OpenBSD OpenSSH 1.2.27
OpenBSD OpenSSH 1.5
OpenBSD OpenSSH 2.1
OpenBSD OpenSSH 2.3
OpenBSD OpenSSH 2.5.1
OpenBSD OpenSSH 2.9.9
OpenBSD OpenSSH 2.9 p2
OpenBSD OpenSSH 3.0.1 p1
OpenBSD OpenSSH 3.0 p1
OpenBSD OpenSSH 3.2
OpenBSD OpenSSH 3.2.3 p1
OpenBSD OpenSSH 3.4
OpenBSD OpenSSH 3.5 p1
OpenBSD OpenSSH 3.6.1 p1
OpenBSD OpenSSH 3.7.1
OpenBSD OpenSSH 3.8
OpenBSD OpenSSH 3.9
OpenBSD OpenSSH 4.0
OpenBSD OpenSSH Portable 4.1.p1
OpenBSD OpenSSH 4.3
OpenBSD OpenSSH 4.4
OpenBSD OpenSSH 4.6
OpenBSD OpenSSH 4.8
OpenBSD OpenSSH 5.5
OpenBSD OpenSSH 5.2

OpenBSD OpenSSH 1.2.3
OpenBSD OpenSSH 1.5.7
OpenBSD OpenSSH 2.1.1
OpenBSD OpenSSH 2.3.1
OpenBSD OpenSSH 2.5.2
OpenBSD OpenSSH 2.9.9 p2
OpenBSD OpenSSH 3.0
OpenBSD OpenSSH 3.0.2
OpenBSD OpenSSH 3.1
OpenBSD OpenSSH 3.2.2
OpenBSD OpenSSH 3.3
OpenBSD OpenSSH 3.4 p1
OpenBSD OpenSSH 3.6
OpenBSD OpenSSH 3.6.1 p2
OpenBSD OpenSSH 3.7.1 p1
OpenBSD OpenSSH 3.8.1
OpenBSD OpenSSH 3.9.1
OpenBSD OpenSSH Portable 4.0.p1
OpenBSD OpenSSH 4.2
OpenBSD OpenSSH Portable 4.3.p1
OpenBSD OpenSSH Portable 4.4.p1
OpenBSD OpenSSH 4.7
OpenBSD OpenSSH 4.9
OpenBSD OpenSSH 5.4
OpenBSD OpenSSH 5.1

OpenBSD OpenSSH 1.3
OpenBSD OpenSSH 1.5.8
OpenBSD OpenSSH 2.2
OpenBSD OpenSSH 2.5
OpenBSD OpenSSH 2.9
OpenBSD OpenSSH 2.9 p1
OpenBSD OpenSSH 3.0.1
OpenBSD OpenSSH 3.0.2p1
OpenBSD OpenSSH 3.1 p1
OpenBSD OpenSSH 3.2.2 p1
OpenBSD OpenSSH 3.3 p1
OpenBSD OpenSSH 3.5
OpenBSD OpenSSH 3.6.1
OpenBSD OpenSSH 3.7
OpenBSD OpenSSH 3.7.1 p2
OpenBSD OpenSSH 3.8.1 p1
OpenBSD OpenSSH 3.9.1 p1
OpenBSD OpenSSH 4.1
OpenBSD OpenSSH Portable 4.2.p1
OpenBSD OpenSSH Portable 4.3.p2
OpenBSD OpenSSH 4.5
OpenBSD OpenSSH 4.7p1
OpenBSD OpenSSH 5.6
OpenBSD OpenSSH 5.3
OpenBSD OpenSSH 5.0

References

http://kb.juniper.net/InfoCenter/index?page=content&id=JSA10673

http://seb.dbzteam.org/crypto/jpake-session-key-retrieval.pdf

http://www.openbsd.org/cgi-bin/cvsweb/src/usr.bin/ssh/jpake.c##rev1.5

http://www.openbsd.org/cgi-bin/cvsweb/src/usr.bin/ssh/jpake.c.diff?r1=1.4;r2=1.5;f=h

https://bugzilla.redhat.com/show_bug.cgi?id=659297

https://github.com/seb-m/jpake

Summary

sshd in OpenSSH before 7.4 allows remote attackers to cause a denial of service (NULL pointer dereference and daemon crash) via an out-of-sequence NEWKEYS message, as demonstrated by Honggfuzz, related to kex.c and packet.c.

CVE-2016-10708 Information	
CVSS Score	5.0
CWE	CWE-476

Vulnerable configs

OpenBSD OpenSSH
OpenBSD OpenSSH 1.2
OpenBSD OpenSSH 1.2.1
OpenBSD OpenSSH 1.2.2
OpenBSD OpenSSH 1.2.3
OpenBSD OpenSSH 1.2.27
OpenBSD OpenSSH 1.3
OpenBSD OpenSSH 1.5
OpenBSD OpenSSH 1.5.7
OpenBSD OpenSSH 1.5.8
OpenBSD OpenSSH 2
OpenBSD OpenSSH 2.1
OpenBSD OpenSSH 2.1.1
OpenBSD OpenSSH 2.2
OpenBSD OpenSSH 2.3
OpenBSD OpenSSH 2.3.1
OpenBSD OpenSSH 2.5
OpenBSD OpenSSH 2.5.1
OpenBSD OpenSSH 2.5.2
OpenBSD OpenSSH 2.9
OpenBSD OpenSSH 2.9.9
OpenBSD OpenSSH 2.9.9 p2
OpenBSD OpenSSH 2.9 p1
OpenBSD OpenSSH 2.9 p2
OpenBSD OpenSSH 3.0
OpenBSD OpenSSH 3.0.1
OpenBSD OpenSSH 3.0.1 p1
OpenBSD OpenSSH 3.0.2
OpenBSD OpenSSH 3.0.2p1
OpenBSD OpenSSH 3.0 p1
OpenBSD OpenSSH 3.1
OpenBSD OpenSSH 3.1 p1
OpenBSD OpenSSH 3.2
OpenBSD OpenSSH 3.2.2
OpenBSD OpenSSH 3.2.2 p1
OpenBSD OpenSSH 3.2.3 p1
OpenBSD OpenSSH 3.3
OpenBSD OpenSSH 3.3 p1
OpenBSD OpenSSH 3.4
OpenBSD OpenSSH 3.4 p1
OpenBSD OpenSSH 3.5
OpenBSD OpenSSH 3.5 p1
OpenBSD OpenSSH 3.6
OpenBSD OpenSSH 3.6.1
OpenBSD OpenSSH 3.6.1 p1
OpenBSD OpenSSH 3.6.1 p2
OpenBSD OpenSSH 3.7
OpenBSD OpenSSH 3.7.1
OpenBSD OpenSSH 3.7.1 p1
OpenBSD OpenSSH 3.7.1 p2
OpenBSD OpenSSH 3.8
OpenBSD OpenSSH 3.8.1
OpenBSD OpenSSH 3.8.1 p1
OpenBSD OpenSSH 3.9
OpenBSD OpenSSH 3.9.1
OpenBSD OpenSSH 3.9.1 p1
OpenBSD OpenSSH 4.0
OpenBSD OpenSSH Portable 4.0.p1
OpenBSD OpenSSH 4.1
OpenBSD OpenSSH Portable 4.1.p1
OpenBSD OpenSSH 4.2
OpenBSD OpenSSH Portable 4.2.p1
OpenBSD OpenSSH 4.3
OpenBSD OpenSSH Portable 4.3.p1
OpenBSD OpenSSH Portable 4.3.p2
OpenBSD OpenSSH 4.4
OpenBSD OpenSSH Portable 4.4.p1
OpenBSD OpenSSH 4.5
OpenBSD OpenSSH 4.6
OpenBSD OpenSSH 4.7
OpenBSD OpenSSH 4.7p1
OpenBSD OpenSSH 4.8
OpenBSD OpenSSH 4.9
OpenBSD OpenSSH 5.0
OpenBSD OpenSSH 5.0 Patch 1
OpenBSD OpenSSH 5.1
OpenBSD OpenSSH 5.1 Patch 1
OpenBSD OpenSSH 5.2
OpenBSD OpenSSH 5.2 Patch 1
OpenBSD OpenSSH 5.3
OpenBSD OpenSSH 5.3 Patch 1
OpenBSD OpenSSH 5.4
OpenBSD OpenSSH 5.4 Patch 1
OpenBSD OpenSSH 5.5
OpenBSD OpenSSH 5.5 Patch 1
OpenBSD OpenSSH 5.6
OpenBSD OpenSSH 5.6 Patch 1
OpenBSD OpenSSH 5.7
OpenBSD OpenSSH 5.7 Patch 1
OpenBSD OpenSSH 5.8
OpenBSD OpenSSH 5.8 Patch 1
OpenBSD OpenSSH 5.8p2
OpenBSD OpenSSH 5.9
OpenBSD OpenSSH 5.9 Patch 1
OpenBSD OpenSSH 6.0
OpenBSD OpenSSH 6.0 Patch 1
OpenBSD OpenSSH 6.1
OpenBSD OpenSSH 6.1 Patch 1
OpenBSD OpenSSH 6.2
OpenBSD OpenSSH 6.2 Patch 1
OpenBSD OpenSSH 6.2 Patch 2
OpenBSD OpenSSH 6.3
OpenBSD OpenSSH 6.3 Patch 1
OpenBSD OpenSSH 6.4
OpenBSD OpenSSH 6.4 Patch 1
OpenBSD OpenSSH 6.5
OpenBSD OpenSSH 6.5 Patch 1
OpenBSD OpenSSH 6.6
OpenBSD OpenSSH 6.6 Patch 1
OpenBSD OpenSSH 6.7
OpenBSD OpenSSH 6.7 Patch 1
OpenBSD OpenSSH 6.8
OpenBSD OpenSSH 6.8 Patch 1
OpenBSD OpenSSH 6.9
OpenBSD OpenSSH 6.9 Patch 1
OpenBSD OpenSSH 7.0
OpenBSD OpenSSH 7.0 Patch 1
OpenBSD OpenSSH 7.1
OpenBSD OpenSSH 7.1 Patch 1
OpenBSD OpenSSH 7.1 P2
OpenBSD OpenSSH 7.2 Patch 2
OpenBSD OpenSSH 7.3
OpenBSD OpenSSH 7.3 p1
Debian Linux 7.0

References

http://blog.swiecki.net/2018/01/fuzzing-tcp-servers.html
http://www.securityfocus.com/bid/102780
https://anongit.mindrot.org/openssh.git/commit/?id=28652bca29046f62c7045e933e6b931de1d16737
https://lists.debian.org/debian-lts-announce/2018/01/msg00031.html
https://lists.debian.org/debian-lts-announce/2018/09/msg00010.html

https://security.netapp.com/advisory/ntap-20180423-0003/
https://usn.ubuntu.com/3809-1/
https://www.openssh.com/releasenotes.html

Summary

The process_open function in sftp-server.c in OpenSSH before 7.6 does not properly prevent write operations in readonly mode, which allows attackers to create zero-length files.

CVE-2017-15906 Information	
CVSS Score	5.0
CWE	CWE-275

Vulnerable configs

OpenBSD OpenSSH 1.2
OpenBSD OpenSSH 1.2.1
OpenBSD OpenSSH 1.2.2
OpenBSD OpenSSH 1.2.3
OpenBSD OpenSSH 1.2.27
OpenBSD OpenSSH 1.3
OpenBSD OpenSSH 1.5
OpenBSD OpenSSH 1.5.7
OpenBSD OpenSSH 1.5.8
OpenBSD OpenSSH 2
OpenBSD OpenSSH 2.1
OpenBSD OpenSSH 2.1.1
OpenBSD OpenSSH 2.2
OpenBSD OpenSSH 2.3
OpenBSD OpenSSH 2.3.1
OpenBSD OpenSSH 2.5
OpenBSD OpenSSH 2.5.1
OpenBSD OpenSSH 2.5.2
OpenBSD OpenSSH 2.9
OpenBSD OpenSSH 2.9.9
OpenBSD OpenSSH 2.9.9 p2
OpenBSD OpenSSH 2.9 p1
OpenBSD OpenSSH 2.9 p2
OpenBSD OpenSSH 3.0
OpenBSD OpenSSH 3.0.1
OpenBSD OpenSSH 3.0.1 p1
OpenBSD OpenSSH 3.0.2
OpenBSD OpenSSH 3.0.2p1
OpenBSD OpenSSH 3.0 p1
OpenBSD OpenSSH 3.1
OpenBSD OpenSSH 3.1 p1
OpenBSD OpenSSH 3.2
OpenBSD OpenSSH 3.2.2
OpenBSD OpenSSH 3.2.2 p1
OpenBSD OpenSSH 3.2.3 p1
OpenBSD OpenSSH 3.3
OpenBSD OpenSSH 3.3 p1
OpenBSD OpenSSH 3.4
OpenBSD OpenSSH 3.4 p1
OpenBSD OpenSSH 3.5
OpenBSD OpenSSH 3.5 p1
OpenBSD OpenSSH 3.6
OpenBSD OpenSSH 3.6.1
OpenBSD OpenSSH 3.6.1 p1
OpenBSD OpenSSH 3.6.1 p2
OpenBSD OpenSSH 3.7
OpenBSD OpenSSH 3.7.1
OpenBSD OpenSSH 3.7.1 p1
OpenBSD OpenSSH 3.7.1 p2
OpenBSD OpenSSH 3.8
OpenBSD OpenSSH 3.8.1
OpenBSD OpenSSH 3.8.1 p1
OpenBSD OpenSSH 3.9
OpenBSD OpenSSH 3.9.1
OpenBSD OpenSSH 3.9.1 p1
OpenBSD OpenSSH 4.0
OpenBSD OpenSSH Portable 4.0.p1
OpenBSD OpenSSH 4.1
OpenBSD OpenSSH Portable 4.1.p1
OpenBSD OpenSSH 4.2
OpenBSD OpenSSH Portable 4.2.p1
OpenBSD OpenSSH 4.3
OpenBSD OpenSSH Portable 4.3.p1
OpenBSD OpenSSH Portable 4.3.p2
OpenBSD OpenSSH 4.4
OpenBSD OpenSSH Portable 4.4.p1
OpenBSD OpenSSH 4.5
OpenBSD OpenSSH 4.6
OpenBSD OpenSSH 4.7
OpenBSD OpenSSH 4.7p1
OpenBSD OpenSSH 4.8
OpenBSD OpenSSH 4.9
OpenBSD OpenSSH 5.0
OpenBSD OpenSSH 5.0 Patch 1
OpenBSD OpenSSH 5.1
OpenBSD OpenSSH 5.1 Patch 1
OpenBSD OpenSSH 5.2
OpenBSD OpenSSH 5.2 Patch 1
OpenBSD OpenSSH 5.3
OpenBSD OpenSSH 5.3 Patch 1
OpenBSD OpenSSH 5.4
OpenBSD OpenSSH 5.4 Patch 1
OpenBSD OpenSSH 5.5
OpenBSD OpenSSH 5.5 Patch 1
OpenBSD OpenSSH 5.6
OpenBSD OpenSSH 5.6 Patch 1
OpenBSD OpenSSH 5.7
OpenBSD OpenSSH 5.7 Patch 1
OpenBSD OpenSSH 5.8
OpenBSD OpenSSH 5.8 Patch 1
OpenBSD OpenSSH 5.8p2
OpenBSD OpenSSH 5.9
OpenBSD OpenSSH 5.9 Patch 1
OpenBSD OpenSSH 6.0
OpenBSD OpenSSH 6.0 Patch 1
OpenBSD OpenSSH 6.1
OpenBSD OpenSSH 6.1 Patch 1
OpenBSD OpenSSH 6.2
OpenBSD OpenSSH 6.2 Patch 1
OpenBSD OpenSSH 6.2 Patch 2
OpenBSD OpenSSH 6.3
OpenBSD OpenSSH 6.3 Patch 1
OpenBSD OpenSSH 6.4
OpenBSD OpenSSH 6.4 Patch 1
OpenBSD OpenSSH 6.5
OpenBSD OpenSSH 6.5 Patch 1
OpenBSD OpenSSH 6.6
OpenBSD OpenSSH 6.6 Patch 1
OpenBSD OpenSSH 6.7
OpenBSD OpenSSH 6.7 Patch 1
OpenBSD OpenSSH 6.8
OpenBSD OpenSSH 6.8 Patch 1
OpenBSD OpenSSH 6.9
OpenBSD OpenSSH 6.9 Patch 1
OpenBSD OpenSSH 7.0
OpenBSD OpenSSH 7.0 Patch 1
OpenBSD OpenSSH 7.1
OpenBSD OpenSSH 7.1 Patch 1
OpenBSD OpenSSH 7.2 Patch 2
OpenBSD OpenSSH 7.3
OpenBSD OpenSSH 7.3 p1
OpenBSD OpenSSH 7.4
OpenBSD OpenSSH 7.4 p1
OpenBSD OpenSSH 7.5
OpenBSD OpenSSH 7.5 p1

References

http://www.securityfocus.com/bid/101552
https://access.redhat.com/errata/RHSA-2018:0980
https://github.com/openbsd/src/commit/a6981567e8e215acc1ef690c8dbb30f2d9b00a19
https://lists.debian.org/debian-lts-announce/2018/09/msg00010.html
https://security.gentoo.org/glsa/201801-05
https://security.netapp.com/advisory/ntap-20180423-0004/

https://www.openssh.com/txt/release-7.6

Summary

The (1) remote_glob function in sftp-glob.c and the (2) process_put function in sftp.c in OpenSSH 5.8 and earlier, as used in FreeBSD 7.3 and 8.1, NetBSD 5.0.2, OpenBSD 4.7, and other products, allow remote authenticated users to cause a denial of service (CPU and memory consumption) via crafted glob expressions that do not match any pathnames, as demonstrated by glob expressions in SSH_FXP_STAT requests to an sftp daemon, a different vulnerability than CVE-2010-2632.

CVE-2010-4755 Information	
CVSS Score	4.0
CWE	CWE-399
Vulnerability impact	
Confidentiality	NONE
Integrity	NONE
Availability	PARTIAL
Access methodology information	
Vector	NETWORK
Complexity	LOW
Authentication	SINGLE_INSTANCE

Vulnerable configs

OpenBSD OpenSSH 1.2	OpenBSD OpenSSH 1.2.1	OpenBSD OpenSSH 1.2.2
OpenBSD OpenSSH 1.2.27	OpenBSD OpenSSH 1.2.3	OpenBSD OpenSSH 1.3
OpenBSD OpenSSH 1.5	OpenBSD OpenSSH 1.5.7	OpenBSD OpenSSH 1.5.8
OpenBSD OpenSSH 2.1	OpenBSD OpenSSH 2.1.1	OpenBSD OpenSSH 2.2
OpenBSD OpenSSH 2.3	OpenBSD OpenSSH 2.3.1	OpenBSD OpenSSH 2.5
OpenBSD OpenSSH 2.5.1	OpenBSD OpenSSH 2.5.2	OpenBSD OpenSSH 2.9
OpenBSD OpenSSH 2.9.9	OpenBSD OpenSSH 2.9.9 p2	OpenBSD OpenSSH 2.9 p1
OpenBSD OpenSSH 2.9 p2	OpenBSD OpenSSH 3.0	OpenBSD OpenSSH 3.0.1
OpenBSD OpenSSH 3.0.1 p1	OpenBSD OpenSSH 3.0.2	OpenBSD OpenSSH 3.0.2p1
OpenBSD OpenSSH 3.0 p1	OpenBSD OpenSSH 3.1	OpenBSD OpenSSH 3.1 p1
OpenBSD OpenSSH 3.2	OpenBSD OpenSSH 3.2.2	OpenBSD OpenSSH 3.2.2 p1
OpenBSD OpenSSH 3.2.3 p1	OpenBSD OpenSSH 3.3	OpenBSD OpenSSH 3.3 p1
OpenBSD OpenSSH 3.4	OpenBSD OpenSSH 3.4 p1	OpenBSD OpenSSH 3.5
OpenBSD OpenSSH 3.5 p1	OpenBSD OpenSSH 3.6	OpenBSD OpenSSH 3.6.1
OpenBSD OpenSSH 3.6.1 p1	OpenBSD OpenSSH 3.6.1 p2	OpenBSD OpenSSH 3.7
OpenBSD OpenSSH 3.7.1	OpenBSD OpenSSH 3.7.1 p1	OpenBSD OpenSSH 3.7.1 p2
OpenBSD OpenSSH 3.8	OpenBSD OpenSSH 3.8.1	OpenBSD OpenSSH 3.8.1 p1
OpenBSD OpenSSH 3.9	OpenBSD OpenSSH 3.9.1	OpenBSD OpenSSH 3.9.1 p1
OpenBSD OpenSSH 4.0	OpenBSD OpenSSH Portable 4.0.p1	OpenBSD OpenSSH 4.1
OpenBSD OpenSSH Portable 4.1.p1	OpenBSD OpenSSH 4.2	OpenBSD OpenSSH Portable 4.2.p1
OpenBSD OpenSSH 4.3	OpenBSD OpenSSH Portable 4.3.p1	OpenBSD OpenSSH Portable 4.3.p2
OpenBSD OpenSSH 4.4	OpenBSD OpenSSH Portable 4.4.p1	OpenBSD OpenSSH 4.5
OpenBSD OpenSSH 4.6	OpenBSD OpenSSH 4.7	OpenBSD OpenSSH 4.7p1
OpenBSD OpenSSH 4.8	OpenBSD OpenSSH 4.9	OpenBSD OpenSSH 5.8

OpenBSD OpenSSH 5.7
OpenBSD OpenSSH 5.4
OpenBSD OpenSSH 5.1
FreeBSD 8.1
OpenBSD OpenSSH 5.6
OpenBSD OpenSSH 5.3
OpenBSD OpenSSH 5.0
cpe:2.3:o:netbsd:netbsd:5.0.2
OpenBSD OpenSSH 5.5
OpenBSD OpenSSH 5.2
FreeBSD 7.3
OpenBSD 4.7

References

http://cvsweb.netbsd.org/cgi-bin/cvsweb.cgi/src/crypto/dist/ssh/Attic/sftp-glob.c##rev1.13.12.1

http://cvsweb.netbsd.org/cgi-bin/cvsweb.cgi/src/crypto/dist/ssh/Attic/sftp.c##rev1.21.6.1

http://cxib.net/stuff/glob-0day.c

http://ftp.netbsd.org/pub/NetBSD/security/advisories/NetBSD-SA2010-008.txt.asc

http://securityreason.com/achievement_securityalert/89

http://securityreason.com/exploitalert/9223

http://securityreason.com/securityalert/8116

Summary

Error handling in the SSH protocol in (1) SSH Tectia Client and Server and Connector 4.0 through 4.4.11, 5.0 through 5.2.4, and 5.3 through 5.3.8; Client and Server and ConnectSecure 6.0 through 6.0.4; Server for Linux on IBM System z 6.0.4; Server for IBM z/OS 5.5.1 and earlier, 6.0.0, and 6.0.1; and Client 4.0-J through 4.3.3-J and 4.0-K through 4.3.10-K; and (2) OpenSSH 4.7p1 and possibly other versions, when using a block cipher algorithm in Cipher Block Chaining (CBC) mode, makes it easier for remote attackers to recover certain plaintext data from an arbitrary block of ciphertext in an SSH session via unknown vectors.

CVE-2008-5161 Information	
CVSS Score	2.6
CWE	CWE-200
Vulnerability impact	
Confidentiality	PARTIAL
Integrity	NONE
Availability	NONE
Access methodology information	
Vector	NETWORK
Complexity	HIGH
Authentication	NONE

Vulnerable configs

OpenBSD OpenSSH 4.7p1	SSH Communications Security Tectia Client 4.0	SSH Communications Security Tectia Client 4.0.1
SSH Communications Security Tectia Client 4.0.3	SSH Communications Security Tectia Client 4.0.4	SSH Communications Security Tectia Client 4.0.5
SSH Communications Security Tectia Client 4.2	SSH Communications Security Tectia Client 4.2.1	SSH Communications Security Tectia Client 4.3
SSH Communications Security Tectia Client 4.3.1	SSH Communications Security Tectia Client 4.3.1 J	SSH Communications Security Tectia Client 4.3.2
SSH Communications Security SSH Tectia Client 4.3.2J	SSH Communications Security Tectia Client 4.3.3	SSH Communications Security Tectia Client 4.3.4
SSH Communications Security Tectia Client 4.3.5	SSH Communications Security Tectia Client 4.3.6	SSH Communications Security Tectia Client 4.3.7
SSH Communications Security Tectia Client 4.3.8 K	SSH Communications Security SSH Tectia Client 4.3.9K	SSH Communications Security Tectia Client 4.4
SSH Communications Security Tectia Client 4.4.1	SSH Communications Security Tectia Client 4.4.2	SSH Communications Security Tectia Client 4.4.3
SSH Communications Security Tectia Client 4.4.4	SSH Communications Security Tectia Client 4.4.6	SSH Communications Security Tectia Client 4.4.7
SSH Communications Security Tectia Client 4.4.8	SSH Communications Security Tectia Client 4.4.9	SSH Communications Security Tectia Client 4.4.10
SSH Communications Security Tectia Client 4.4.11	SSH Communications Security SSH Tectia Client 5.0.0	SSH Communications Security SSH Tectia Client 5.0.0f
SSH Communications Security SSH Tectia Client 5.0.1	SSH Communications Security SSH Tectia Client 5.0.1f	SSH Communications Security SSH Tectia Client 5.0.2
SSH Communications Security SSH Tectia Client 5.0.2f	SSH Communications Security SSH Tectia Client 5.0.3	SSH Communications Security SSH Tectia Client 5.0.3f
SSH Communications Security SSH Tectia Client 5.1.0	SSH Communications Security SSH Tectia Client 5.1.1	SSH Communications Security SSH Tectia Client 5.1.2
SSH Communications Security SSH Tectia Client 5.1.3	SSH Communications Security SSH Tectia Client 5.2.0	SSH Communications Security SSH Tectia Client 5.2.1
SSH Communications Security SSH Tectia Client 5.2.2	SSH Communications Security SSH Tectia Client 5.2.3	SSH Communications Security SSH Tectia Client 5.2.4
SSH Communications Security SSH Tectia Client 5.3.0	SSH Communications Security SSH Tectia Client 5.3.1	SSH Communications Security SSH Tectia Client 5.3.2
SSH Communications Security SSH Tectia Client 5.3.3	SSH Communications Security SSH Tectia Client 5.3.5	SSH Communications Security SSH Tectia Client 5.3.6
SSH Communications Security SSH Tectia Client 5.3.7	SSH Communications Security SSH Tectia Client 5.3.8	SSH Communications Security SSH Tectia Client 6.0.0
SSH Communications Security SSH Tectia Client 6.0.1	SSH Communications Security SSH Tectia Client 6.0.2	SSH Communications Security SSH Tectia Client 6.0.4
SSH Communications Security SSH Tectia Client 6.0.4	SSH Communications Security Tectia Connector 4.0.7	SSH Communications Security Tectia Connector 4.1.2
SSH Communications Security Tectia Connector 4.1.3	SSH Communications Security Tectia Connector 4.1.5	SSH Communications Security Tectia Connector 4.2.0

SSH Communications Security Tectia Connector 4.3.0
SSH Communications Security Tectia Connector 4.3.4
SSH Communications Security Tectia Connector 4.3.5
SSH Communications Security Tectia Connector 4.4.0
SSH Communications Security Tectia Connector 4.4.2
SSH Communications Security Tectia Connector 4.4.4
SSH Communications Security Tectia Connector 4.4.6
SSH Communications Security Tectia Connector 4.4.7
SSH Communications Security Tectia Connector 4.4.9
SSH Communications Security Tectia Connector 4.4.10
SSH Communications Security Tectia Connector 5.0.0
SSH Communications Security Tectia Connector 5.0.1
SSH Communications Security Tectia Connector 5.0.2
SSH Communications Security Tectia Connector 5.0.3
SSH Communications Security Tectia Connector 5.1.0
SSH Communications Security Tectia Connector 5.1.1
SSH Communications Security Tectia Connector 5.1.2
SSH Communications Security Tectia Connector 5.1.3
SSH Communications Security Tectia Connector 5.2.2
SSH Communications Security Tectia Connector 5.3.0
SSH Communications Security Tectia Connector 5.3.1
SSH Communications Security Tectia Connector 5.3.2
SSH Communications Security Tectia Connector 5.3.3
SSH Communications Security Tectia Connector 5.3.7
SSH Communications Security Tectia Connector 5.3.8
cpe:2.3:a:ssh:tectia_connectsecure:6.0.0
cpe:2.3:a:ssh:tectia_connectsecure:6.0.1
cpe:2.3:a:ssh:tectia_connectsecure:6.0.2
cpe:2.3:a:ssh:tectia_connectsecure:6.0.3
cpe:2.3:a:ssh:tectia_connectsecure:6.0.4
SSH Communications Security Tectia Server 4.0
SSH Communications Security Tectia Server 4.0.3
SSH Communications Security Tectia Server 4.0.4
SSH Communications Security Tectia Server 4.0.5
SSH Communications Security Tectia Server 4.0.7
SSH Communications Security Tectia Server 4.1.2
SSH Communications Security Tectia Server 4.1.3
SSH Communications Security Tectia Server 4.1.5
SSH Communications Security Tectia Server 4.2.0
SSH Communications Security Tectia Server 4.2.1
SSH Communications Security Tectia Server 4.2.2
SSH Communications Security Tectia Server 4.3
SSH Communications Security Tectia Server 4.3.0
SSH Communications Security Tectia Server 4.3.1
SSH Communications Security Tectia Server 4.3.2
SSH Communications Security Tectia Server 4.3.3
SSH Communications Security Tectia Server 4.3.4
SSH Communications Security Tectia Server 4.3.5
SSH Communications Security Tectia Server 4.3.6
SSH Communications Security Tectia Server 4.3.7
SSH Communications Security Tectia Server 4.4
SSH Communications Security Tectia Server 4.4.0
SSH Communications Security Tectia Server 4.4.1
SSH Communications Security Tectia Server 4.4.2
SSH Communications Security Tectia Server 4.4.4
SSH Communications Security Tectia Server 4.4.5
SSH Communications Security Tectia Server 4.4.6
SSH Communications Security Tectia Server 4.4.7
SSH Communications Security Tectia Server 4.4.8
SSH Communications Security Tectia Server 4.4.9
SSH Communications Security Tectia Server 4.4.10
SSH Communications Security Tectia Server 4.4.11
SSH Communications Security Tectia Server 5.0.0
SSH Communications Security Tectia Server 5.0.1
SSH Communications Security Tectia Server 5.0.2
SSH Communications Security Tectia Server 5.0.3
SSH Communications Security Tectia Server 5.1.0
SSH Communications Security Tectia Server 5.1.1
cpe:2.3:a:ssh:tectia_server:5.1.1:-:ibm_zos
SSH Communications Security Tectia Server 5.1.2
SSH Communications Security Tectia Server 5.1.3
SSH Communications Security Tectia Server 5.2.0
cpe:2.3:a:ssh:tectia_server:5.2.0:-:ibm_zos
cpe:2.3:a:ssh:tectia_server:5.2.1:-:ibm_zos
SSH Communications Security Tectia Server 5.2.2
cpe:2.3:a:ssh:tectia_server:5.2.2:-:ibm_zos
SSH Communications Security Tectia Server 5.2.3
SSH Communications Security Tectia Server 5.2.4
SSH Communications Security SSH Tectia Server 5.3.0
cpe:2.3:a:ssh:tectia_server:5.3.0:-:ibm_zos
SSH Communications Security SSH Tectia Server 5.3.1
SSH Communications Security SSH Tectia Server 5.3.2
SSH Communications Security SSH Tectia Server 5.3.3
SSH Communications Security SSH Tectia Server 5.3.4
SSH Communications Security SSH Tectia Server 5.3.5
SSH Communications Security SSH Tectia Server 5.3.6
SSH Communications Security SSH Tectia Server 5.3.7
SSH Communications Security SSH Tectia Server 5.3.8
cpe:2.3:a:ssh:tectia_server:5.4.0:-:ibm_zos
cpe:2.3:a:ssh:tectia_server:5.4.1:-:ibm_zos
cpe:2.3:a:ssh:tectia_server:5.4.2:-:ibm_zos
cpe:2.3:a:ssh:tectia_server:5.5.0:-:ibm_zos
cpe:2.3:a:ssh:tectia_server:5.5.1:-:ibm_zos
SSH Communications Security SSH Tectia Server 6.0.0
cpe:2.3:a:ssh:tectia_server:6.0.0:-:ibm_zos
SSH Communications Security SSH Tectia Server 6.0.1
cpe:2.3:a:ssh:tectia_server:6.0.1:-:ibm_zos
SSH Communications Security SSH Tectia Server 6.0.2
SSH Communications Security SSH Tectia Server 6.0.3
SSH Communications Security SSH Tectia Server 6.0.4
SSH Communications Security Tectia Server 6.0.4 for Linux on IBM System Z

References

http://isc.sans.org/diary.html?storyid=5366

http://kb.juniper.net/InfoCenter/index?page=content&id=JSA10705

http://lists.apple.com/archives/security-announce/2009/Nov/msg00000.html

http://marc.info/?l=bugtraq&m=125017764422557&w=2

http://openssh.org/txt/cbc.adv

http://rhn.redhat.com/errata/RHSA-2009-1287.html

http://sunsolve.sun.com/search/document.do?assetkey=1-66-247186-1

http://support.apple.com/kb/HT3937

http://support.attachmate.com/techdocs/2398.html

http://support.avaya.com/elmodocs2/security/ASA-2008-503.htm

http://www.cpni.gov.uk/Docs/Vulnerability_Advisory_SSH.txt

http://www.kb.cert.org/vuls/id/958563

http://www.rtpro.yamaha.co.jp/RT/FAQ/Security/CPNI957037.html

http://www.securityfocus.com/archive/1/498558/100/0/threaded

http://www.securityfocus.com/archive/1/498579/100/0/threaded

http://www.securityfocus.com/bid/32319

http://www.securitytracker.com/id?1021235

http://www.securitytracker.com/id?1021236

http://www.securitytracker.com/id?1021382
http://www.ssh.com/company/news/article/953/
http://www.vupen.com/english/advisories/2008/3172
http://www.vupen.com/english/advisories/2008/3173
http://www.vupen.com/english/advisories/2008/3409
http://www.vupen.com/english/advisories/2009/1135
http://www.vupen.com/english/advisories/2009/3184
https://exchange.xforce.ibmcloud.com/vulnerabilities/46620
https://h20566.www2.hpe.com/portal/site/hpsc/public/kb/docDisplay?docId=emr_na-c05157667
https://kc.mcafee.com/corporate/index?page=content&id=SB10106
https://kc.mcafee.com/corporate/index?page=content&id=SB10163

Summary

modules/arch/win32/mod_isapi.c in mod_isapi in the Apache HTTP Server 2.0.37 through 2.0.63, 2.2.0 through 2.2.14, and 2.3.x before 2.3.7, when running on Windows, does not ensure that request processing is complete before calling isapi_unload for an ISAPI .dll module, which allows remote attackers to execute arbitrary code via unspecified vectors related to a crafted request, a reset packet, and "orphaned callback pointers."

CVE-2010-0425 Information	
CVSS Score	10.0
CWE	Unknown
Vulnerability impact	
Confidentiality	COMPLETE
Integrity	COMPLETE
Availability	COMPLETE
Access methodology information	
Vector	NETWORK
Complexity	LOW
Authentication	NONE

Vulnerable configs

Apache Software Foundation Apache HTTP Server 2.3.0
Apache Software Foundation Apache HTTP Server 2.3.1 Apache Software Foundation Apache HTTP Server 2.3.2 Apache Software Foundation Apache HTTP Server 2.3.3
Apache Software Foundation Apache HTTP Server 2.3.4 Apache Software Foundation Apache HTTP Server 2.3.5 Apache Software Foundation Apache HTTP Server 2.3.6
Microsoft Windows Apache Software Foundation Apache HTTP Server 2.0.9a Apache Software Foundation Apache HTTP Server 2.0.28
Apache Software Foundation Apache HTTP Server 2.0.28 Beta Apache Software Foundation Apache HTTP Server 2.0.32 Apache Software Foundation Apache HTTP Server 2.0.32 Beta
Apache Software Foundation Apache HTTP Server 2.0.34 Beta Apache Software Foundation Apache HTTP Server 2.0.35 Apache Software Foundation Apache HTTP Server 2.0.36
Apache Software Foundation Apache HTTP Server 2.0.37 Apache Software Foundation Apache HTTP Server 2.0.38 Apache Software Foundation Apache HTTP Server 2.0.39
Apache Software Foundation Apache HTTP Server 2.0.40 Apache Software Foundation Apache HTTP Server 2.0.41 Apache Software Foundation Apache HTTP Server 2.0.42
Apache Software Foundation Apache HTTP Server 2.0.43 Apache Software Foundation Apache HTTP Server 2.0.44 Apache Software Foundation Apache HTTP Server 2.0.45
Apache Software Foundation Apache HTTP Server 2.0.46 Apache Software Foundation Apache HTTP Server 2.0.47 Apache Software Foundation Apache HTTP Server 2.0.48
Apache Software Foundation Apache HTTP Server 2.0.49 Apache Software Foundation Apache HTTP Server 2.0.50 Apache Software Foundation Apache HTTP Server 2.0.51
Apache Software Foundation Apache HTTP Server 2.0.52 Apache Software Foundation Apache HTTP Server 2.0.53 Apache Software Foundation Apache HTTP Server 2.0.54
Apache Software Foundation Apache HTTP Server 2.0.55 Apache Software Foundation Apache HTTP Server 2.0.56 Apache Software Foundation Apache HTTP Server 2.0.57
Apache Software Foundation Apache HTTP Server 2.0.58 Apache Software Foundation HTTP Server 2.0.59 Apache Software Foundation Apache HTTP Server 2.0.60 dev
Apache Software Foundation HTTP Server 2.0.61 Apache Software Foundation Apache HTTP Server 2.0.63 Microsoft Windows
Apache Software Foundation Apache HTTP Server Apache Software Foundation Apache HTTP Server 2.2.0 Apache Software Foundation Apache HTTP Server 2.2.1
Apache Software Foundation Apache HTTP Server 2.2.2 Apache Software Foundation Apache HTTP Server 2.2.3 Apache Software Foundation Apache HTTP Server 2.2.4
Apache Software Foundation Apache HTTP Server 2.2.6 cpe:2.3:a:apache:http_server:2.2.7 Apache Software Foundation Apache HTTP Server 2.2.8
Apache Software Foundation Apache HTTP Server 2.2.9 Apache Software Foundation Apache HTTP Server 2.2.10 Apache Software Foundation Apache HTTP Server 2.2.11
Apache Software Foundation Apache HTTP Server 2.2.12 Apache Software Foundation Apache HTTP Server 2.2.13 Apache Software Foundation Apache HTTP Server 2.2.14
Microsoft Windows

References

http://httpd.apache.org/security/vulnerabilities_20.html
http://httpd.apache.org/security/vulnerabilities_22.html
http://lists.vmware.com/pipermail/security-announce/2010/000105.html
http://svn.apache.org/viewvc/httpd/httpd/trunk/CHANGES?r1=917870&r2=917869&pathrev=917870
http://svn.apache.org/viewvc/httpd/httpd/trunk/modules/arch/win32/mod_isapi.c?r1=917870&r2=917869
http://svn.apache.org/viewvc?view=revision&revision=917870
http://www-01.ibm.com/support/docview.wss?uid=swg1PM09447
http://www-01.ibm.com/support/docview.wss?uid=swg1PM12247
http://www.kb.cert.org/vuls/id/280613
http://www.oracle.com/technetwork/topics/security/cpujuly2013-1899826.html
http://www.securityfocus.com/bid/38494
http://www.securitytracker.com/id?1023701
http://www.senseofsecurity.com.au/advisories/SOS-10-002
http://www.vmware.com/security/advisories/VMSA-2010-0014.html
http://www.vupen.com/english/advisories/2010/0634
http://www.vupen.com/english/advisories/2010/0994
https://exchange.xforce.ibmcloud.com/vulnerabilities/56624

Summary

The byterange filter in the Apache HTTP Server 1.3.x, 2.0.x through 2.0.64, and 2.2.x through 2.2.19 allows remote attackers to cause a denial of service (memory and CPU consumption) via a Range header that expresses multiple overlapping ranges, as exploited in the wild in August 2011, a different vulnerability than CVE-2007-0086.

CVE-2011-3192 Information	
CVSS Score	7.8
CWE	CWE-399
Vulnerability impact	
Confidentiality	NONE
Integrity	NONE
Availability	COMPLETE
Access methodology information	
Vector	NETWORK
Complexity	LOW
Authentication	NONE

Vulnerable configs

Apache Software Foundation Apache HTTP Server 1.3		Apache Software Foundation Apache HTTP Server 1.3.0
Apache Software Foundation Apache HTTP Server 1.3.1	Apache Software Foundation Apache HTTP Server 1.3.1.1	Apache Software Foundation Apache HTTP Server 1.3.2
Apache Software Foundation Apache HTTP Server 1.3.3	Apache Software Foundation Apache HTTP Server 1.3.4	Apache Software Foundation Apache HTTP Server 1.3.5
Apache Software Foundation Apache HTTP Server 1.3.6	Apache Software Foundation Apache HTTP Server 1.3.7	Apache Software Foundation Apache HTTP Server 1.3.8
Apache Software Foundation Apache HTTP Server 1.3.9	Apache Software Foundation Apache 1.3.10	Apache Software Foundation Apache HTTP Server 1.3.11
Apache Software Foundation Apache HTTP Server 1.3.12	Apache Software Foundation Apache 1.3.13	Apache Software Foundation Apache HTTP Server 1.3.14
Apache Software Foundation Apache 1.3.15	Apache Software Foundation Apache 1.3.16	Apache Software Foundation Apache HTTP Server 1.3.17
Apache Software Foundation Apache HTTP Server 1.3.18	Apache Software Foundation Apache HTTP Server 1.3.19	Apache Software Foundation Apache HTTP Server 1.3.20
Apache Software Foundation Apache HTTP Server 1.3.22	Apache Software Foundation Apache HTTP Server 1.3.23	Apache Software Foundation Apache HTTP Server 1.3.24
Apache Software Foundation Apache HTTP Server 1.3.25	Apache Software Foundation Apache HTTP Server 1.3.26	Apache Software Foundation Apache HTTP Server 1.3.27
Apache Software Foundation Apache HTTP Server 1.3.28	Apache Software Foundation Apache HTTP Server 1.3.29	Apache Software Foundation Apache HTTP Server 1.3.30
Apache Software Foundation Apache HTTP Server 1.3.31	Apache Software Foundation Apache HTTP Server 1.3.32	Apache Software Foundation Apache HTTP Server 1.3.33
Apache Software Foundation Apache HTTP Server 1.3.34	Apache Software Foundation Apache HTTP Server 1.3.35	Apache Software Foundation Apache HTTP Server 1.3.36
Apache Software Foundation Apache HTTP Server 1.3.37	Apache Software Foundation Apache HTTP Server 1.3.38	Apache Software Foundation Apache HTTP Server 1.3.39
Apache Software Foundation Apache HTTP Server 1.3.41	Apache Software Foundation Apache HTTP Server 1.3.42	Apache Software Foundation Apache HTTP Server 1.3.65
Apache Software Foundation Apache HTTP Server 1.3.68	Apache Software Foundation Apache HTTP Server 2.0	Apache Software Foundation Apache HTTP Server 2.0.9a
Apache Software Foundation Apache HTTP Server 2.0.28	Apache Software Foundation Apache HTTP Server 2.0.28 Beta	Apache Software Foundation Apache HTTP Server 2.0.32
Apache Software Foundation Apache HTTP Server 2.0.32 Beta	Apache Software Foundation Apache HTTP Server 2.0.34 Beta	Apache Software Foundation Apache HTTP Server 2.0.35
Apache Software Foundation Apache HTTP Server 2.0.36	Apache Software Foundation Apache HTTP Server 2.0.37	Apache Software Foundation Apache HTTP Server 2.0.38
Apache Software Foundation Apache HTTP Server 2.0.39	Apache Software Foundation Apache HTTP Server 2.0.40	Apache Software Foundation Apache HTTP Server 2.0.41
Apache Software Foundation Apache HTTP Server 2.0.42	Apache Software Foundation Apache HTTP Server 2.0.43	Apache Software Foundation Apache HTTP Server 2.0.44
Apache Software Foundation Apache HTTP Server 2.0.45	Apache Software Foundation Apache HTTP Server 2.0.46	Apache Software Foundation Apache HTTP Server 2.0.47
Apache Software Foundation Apache HTTP Server 2.0.48	Apache Software Foundation Apache HTTP Server 2.0.49	Apache Software Foundation Apache HTTP Server 2.0.50
Apache Software Foundation Apache HTTP Server 2.0.51	Apache Software Foundation Apache HTTP Server 2.0.52	Apache Software Foundation Apache HTTP Server 2.0.53
Apache Software Foundation Apache HTTP Server 2.0.54	Apache Software Foundation Apache HTTP Server 2.0.55	Apache Software Foundation Apache HTTP Server 2.0.56
Apache Software Foundation Apache HTTP Server 2.0.57	Apache Software Foundation Apache HTTP Server 2.0.58	Apache Software Foundation HTTP Server 2.0.59
Apache Software Foundation Apache HTTP Server 2.0.60 dev	Apache Software Foundation HTTP Server 2.0.61	Apache Software Foundation Apache HTTP Server 2.0.63
Apache Software Foundation Apache HTTP Server 2.0.64	Apache Software Foundation Apache HTTP Server 2.2.0	Apache Software Foundation Apache HTTP Server 2.2.1
Apache Software Foundation Apache HTTP Server 2.2.2	Apache Software Foundation Apache HTTP Server 2.2.3	Apache Software Foundation Apache HTTP Server 2.2.4

Apache Software Foundation Apache HTTP Server 2.2.6
Apache Software Foundation Apache HTTP Server 2.2.8
Apache Software Foundation Apache HTTP Server 2.2.9
Apache Software Foundation Apache HTTP Server 2.2.10
Apache Software Foundation Apache HTTP Server 2.2.11
Apache Software Foundation Apache HTTP Server 2.2.12
Apache Software Foundation Apache HTTP Server 2.2.13
Apache Software Foundation Apache HTTP Server 2.2.14
Apache Software Foundation Apache HTTP Server 2.2.15
Apache Software Foundation Apache HTTP Server 2.2.16
Apache Software Foundation Apache HTTP Server 2.2.18
Apache Software Foundation Apache HTTP Server 2.2.19

References

http://archives.neohapsis.com/archives/fulldisclosure/2011-08/0285.html
http://blogs.oracle.com/security/entry/security_alert_for_cve_2011
http://lists.apple.com/archives/Security-announce/2011//Oct/msg00003.html
http://lists.opensuse.org/opensuse-security-announce/2011-09/msg00006.html
http://lists.opensuse.org/opensuse-security-announce/2011-09/msg00009.html
http://lists.opensuse.org/opensuse-security-announce/2011-09/msg00010.html
http://lists.opensuse.org/opensuse-security-announce/2011-09/msg00011.html
http://lists.opensuse.org/opensuse-security-announce/2011-11/msg00008.html
http://lists.opensuse.org/opensuse-security-announce/2011-11/msg00011.html
http://mail-archives.apache.org/mod_mbox/httpd-announce/201108.mbox/\%3c20110824161640.122D38
http://mail-archives.apache.org/mod_mbox/httpd-dev/201108.mbox/\%3cCAAPSnn2PO-d-C4nQt_TES2RRWiZr7urefhTKPWBC1b+K1Dqc7g@mail.gmail.com\%3e
http://marc.info/?l=bugtraq&m=131551295528105&w=2
http://marc.info/?l=bugtraq&m=131731002122529&w=2
http://marc.info/?l=bugtraq&m=132033751509019&w=2
http://marc.info/?l=bugtraq&m=133477473521382&w=2
http://marc.info/?l=bugtraq&m=133951357207000&w=2
http://marc.info/?l=bugtraq&m=134987041210674&w=2
http://seclists.org/fulldisclosure/2011/Aug/175
http://securitytracker.com/id?1025960
http://support.apple.com/kb/HT5002
http://www.apache.org/dist/httpd/Announcement2.2.html
http://www.cisco.com/en/US/products/products_security_advisory09186a0080b90d73.shtml
http://www.exploit-db.com/exploits/17696
http://www.gossamer-threads.com/lists/apache/dev/401638
http://www.kb.cert.org/vuls/id/405811
http://www.mandriva.com/security/advisories?name=MDVSA-2011:130
http://www.mandriva.com/security/advisories?name=MDVSA-2013:150
http://www.oracle.com/technetwork/topics/security/alert-cve-2011-3192-485304.html

http://www.oracle.com/technetwork/topics/security/cpujan2012-366304.html
http://www.oracle.com/technetwork/topics/security/cpujul2012-392727.html
http://www.oracle.com/technetwork/topics/security/cpuoct2011-330135.html
http://www.redhat.com/support/errata/RHSA-2011-1245.html
http://www.redhat.com/support/errata/RHSA-2011-1294.html
http://www.redhat.com/support/errata/RHSA-2011-1300.html
http://www.redhat.com/support/errata/RHSA-2011-1329.html
http://www.redhat.com/support/errata/RHSA-2011-1330.html
http://www.redhat.com/support/errata/RHSA-2011-1369.html
http://www.securityfocus.com/bid/49303
http://www.ubuntu.com/usn/USN-1199-1
https://bugzilla.redhat.com/show_bug.cgi?id=732928
https://exchange.xforce.ibmcloud.com/vulnerabilities/69396
https://help.ecostruxureit.com/display/public/UADCE725/Security+fixes+in+StruxureWare+Data+Center+
https://issues.apache.org/bugzilla/show_bug.cgi?id=51714

Summary

mod_session_dbd.c in the mod_session_dbd module in the Apache HTTP Server before 2.4.5 proceeds with save operations for a session without considering the dirty flag and the requirement for a new session ID, which has unspecified impact and remote attack vectors.

CVE-2013-2249 Information	
CVSS Score	7.5
CWE	Vulnerability impact
Confidentiality	PARTIAL
Integrity	PARTIAL
Availability	PARTIAL
Access methodology information	
Vector	NETWORK
Complexity	LOW
Authentication	NONE

Vulnerable configs

Apache Software Foundation Apache HTTP Server 1.3.35	Apache Software Foundation Apache HTTP Server 1.3.20	Apache Software Foundation Apache HTTP Server 1.3.34
Apache Software Foundation Apache HTTP Server 1.3.36	Apache Software Foundation Apache HTTP Server 2.1.1	Apache Software Foundation Apache HTTP Server 2.1.2
Apache Software Foundation Apache HTTP Server 1.3.39	Apache Software Foundation HTTP Server 2.0.61	Apache Software Foundation Apache HTTP Server 2.0.58
Apache Software Foundation Apache HTTP Server 2.1	Apache Software Foundation Apache HTTP Server 2.0.55	Apache Software Foundation Apache HTTP Server 2.0.54
Apache Software Foundation Apache HTTP Server 2.0.57	Apache Software Foundation Apache HTTP Server 2.0.56	Apache Software Foundation Apache HTTP Server 2.0.51
Apache Software Foundation Apache HTTP Server 2.0.50	Apache Software Foundation Apache HTTP Server 2.0.53	Apache Software Foundation Apache HTTP Server 2.0.52
Apache Software Foundation Apache HTTP Server 2.0.47	Apache Software Foundation Apache HTTP Server 2.0.46	Apache Software Foundation Apache HTTP Server 2.0.49
Apache Software Foundation Apache HTTP Server 2.0.48	Apache Software Foundation Apache HTTP Server 2.0.43	Apache Software Foundation Apache HTTP Server 1.3.19
Apache Software Foundation Apache HTTP Server 2.0.42	Apache Software Foundation Apache HTTP Server 1.3.18	Apache Software Foundation Apache HTTP Server 2.0.45
Apache Software Foundation Apache HTTP Server 1.3.17	Apache Software Foundation Apache HTTP Server 2.0.44	Apache Software Foundation Apache HTTP Server 1.3.14
Apache Software Foundation Apache HTTP Server 1.3.41	Apache Software Foundation Apache HTTP Server 1.3.0	Apache Software Foundation Apache HTTP Server 1.3.38
Apache Software Foundation Apache HTTP Server 2.0.63	Apache Software Foundation Apache HTTP Server 1.3.24	Apache Software Foundation Apache HTTP Server 1.3.25
Apache Software Foundation Apache HTTP Server 1.3.22	Apache Software Foundation Apache HTTP Server 1.3.23	Apache Software Foundation Apache HTTP Server 2.0.64
Apache Software Foundation Apache HTTP Server 1.3.27	Apache Software Foundation Apache HTTP Server 1.3.26	Apache Software Foundation Apache HTTP Server 1.3.42
Apache Software Foundation Apache HTTP Server 1.3.2	Apache Software Foundation Apache 1.3.10	Apache Software Foundation Apache 1.29
Apache Software Foundation Apache 1.2	Apache Software Foundation Apache 1.3.16	Apache Software Foundation Apache 1.3.15
Apache Software Foundation Apache 1.3.13	Apache Software Foundation Apache HTTP Server 1.3.37	Apache Software Foundation HTTP Server 2.0.59
Apache Software Foundation Apache HTTP Server 2.0.9a	Apache Software Foundation Apache HTTP Server 2.0.60 dev	Apache Software Foundation Apache HTTP Server 1.0
Apache Software Foundation Apache HTTP Server 0.8.14	Apache Software Foundation Apache HTTP Server 0.8.11	Apache Software Foundation Apache HTTP Server 1.1
Apache Software Foundation Apache HTTP Server 1.0.5	Apache Software Foundation Apache HTTP Server 1.0.3	Apache Software Foundation Apache HTTP Server 1.0.2
Apache Software Foundation Apache HTTP Server 1.1.1	Apache Software Foundation Apache HTTP Server 1.2.5	Apache Software Foundation Apache HTTP Server 1.3.65
Apache Software Foundation Apache HTTP Server 1.3.1	Apache Software Foundation Apache HTTP Server 1.3.11	Apache Software Foundation Apache HTTP Server 1.99
Apache Software Foundation Apache HTTP Server 1.3.12	Apache Software Foundation Apache HTTP Server 1.3.68	Apache Software Foundation Apache HTTP Server 1.3.28
Apache Software Foundation Apache HTTP Server 1.3.29	Apache Software Foundation Apache HTTP Server 1.3.3	Apache Software Foundation Apache HTTP Server 1.3.30
Apache Software Foundation Apache HTTP Server 1.3.31	Apache Software Foundation Apache HTTP Server 1.3	Apache Software Foundation Apache HTTP Server 1.3.32
Apache Software Foundation Apache HTTP Server 1.2.4	Apache Software Foundation Apache HTTP Server 1.3.33	Apache Software Foundation Apache HTTP Server 1.3.1.1
Apache Software Foundation Apache HTTP Server 1.3.4	Apache Software Foundation Apache HTTP Server 1.2.6	Apache Software Foundation Apache HTTP Server 1.3.5
Apache Software Foundation Apache HTTP Server 1.4.0	Apache Software Foundation Apache HTTP Server 1.3.6	Apache Software Foundation Apache HTTP Server 1.3.8
Apache Software Foundation Apache HTTP Server 1.3.7	Apache Software Foundation Apache HTTP Server 2.0	Apache Software Foundation Apache HTTP Server 1.3.9
Apache Software Foundation Apache HTTP Server 2.0.28 Beta	Apache Software Foundation Apache HTTP Server 2.0.28	Apache Software Foundation Apache HTTP Server 2.0.32 Beta
Apache Software Foundation Apache HTTP Server 2.0.32	Apache Software Foundation Apache HTTP Server 2.0.35	Apache Software Foundation Apache HTTP Server 2.0.34 Beta
Apache Software Foundation Apache HTTP Server 2.0.37	Apache Software Foundation Apache HTTP Server 2.0.36	Apache Software Foundation Apache HTTP Server 2.0.39
Apache Software Foundation Apache HTTP Server 2.0.38	Apache Software Foundation Apache HTTP Server 2.0.41	Apache Software Foundation Apache HTTP Server 2.0.40
Apache Software Foundation Apache HTTP Server 2.1.5	Apache Software Foundation Apache HTTP Server 2.1.6	Apache Software Foundation Apache HTTP Server 2.2
Apache Software Foundation Apache HTTP Server 2.2.1	Apache Software Foundation Apache HTTP Server 2.1.3	Apache Software Foundation Apache HTTP Server 2.2.6
Apache Software Foundation Apache HTTP Server 2.1.4	Apache Software Foundation Apache HTTP Server 2.2.11	Apache Software Foundation Apache HTTP Server 2.2.9

Apache Software Foundation Apache HTTP Server 2.2.10
Apache Software Foundation Apache HTTP Server 2.2.8
Apache Software Foundation Apache HTTP Server 2.2.13
Apache Software Foundation Apache HTTP Server 2.3.0
Apache Software Foundation Apache HTTP Server 2.2.19
Apache Software Foundation Apache HTTP Server 2.3.4
Apache Software Foundation Apache HTTP Server 2.3.3
Apache Software Foundation Apache HTTP Server 2.3.5
Apache Software Foundation Apache HTTP Server 2.2.20
Apache Software Foundation Apache HTTP Server 2.2.16
Apache Software Foundation Apache HTTP Server 2.3.6
Apache Software Foundation Apache HTTP Server 2.2.15
Apache Software Foundation Apache HTTP Server 2.2.18
Apache Software Foundation Apache HTTP Server 2.2.14
Apache Software Foundation Apache HTTP Server 2.2.22
Apache Software Foundation Apache HTTP Server 2.2.23
Apache Software Foundation Apache HTTP Server 2.4.3
Apache Software Foundation Apache HTTP Server 2.3.2
Apache Software Foundation Apache HTTP Server 2.3.1
Apache Software Foundation Apache HTTP Server 2.2.3
Apache Software Foundation Apache HTTP Server 2.2.25
Apache Software Foundation Apache HTTP Server 2.2.24
Apache Software Foundation Apache HTTP Server 2.1.7
Apache Software Foundation Apache HTTP Server 2.1.8
Apache Software Foundation Apache HTTP Server 2.2.12
Apache Software Foundation Apache HTTP Server 2.2.0
Apache Software Foundation Apache HTTP Server 2.4.2
Apache Software Foundation Apache HTTP Server 2.3.16
Apache Software Foundation Apache HTTP Server 2.4.0
Apache Software Foundation Apache HTTP Server 2.3.14
Apache Software Foundation Apache HTTP Server 2.3.15
Apache Software Foundation Apache HTTP Server 2.3.12
Apache Software Foundation Apache HTTP Server 2.3.13
Apache Software Foundation Apache HTTP Server 2.3.10
Apache Software Foundation Apache HTTP Server 2.3.11
Apache Software Foundation Apache HTTP Server 2.3.8
Apache HTTP Server 2.2.21
Apache Software Foundation Apache HTTP Server 2.3.9
Apache Software Foundation Apache HTTP Server 2.2.2
Apache Software Foundation Apache HTTP Server 2.1.9
Apache Software Foundation Apache HTTP Server 2.3.7
Apache Software Foundation Apache HTTP Server 2.2.4
Apache Software Foundation Apache HTTP Server 2.2.17
Apache Software Foundation Apache HTTP Server 2.4.1
Apache Software Foundation Apache HTTP Server 2.4.4
Juniper JUNOS Space 15.1 R1

References

http://kb.juniper.net/InfoCenter/index?page=content&id=JSA10698

http://svn.apache.org/viewvc/httpd/httpd/trunk/modules/session/mod_session_dbd.c?r1=1409170&r2=14

http://tools.cisco.com/security/center/content/CiscoSecurityNotice/CVE-2013-2249

http://www.apache.org/dist/httpd/CHANGES_2.4.6

https://httpd.apache.org/security/vulnerabilities_24.html

Summary

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.

CVE-2017-7679 Information	
CVSS Score	7.5
CWE	CWE-119

Vulnerable configs

Apache Software Foundation Apache HTTP Server 2.2.0		Apache Software Foundation Apache HTTP Server 2.2.1
Apache Software Foundation Apache HTTP Server 2.2.2	Apache Software Foundation Apache HTTP Server 2.2.3	Apache Software Foundation Apache HTTP Server 2.2.4
Apache Software Foundation Apache HTTP Server	Apache Software Foundation Apache HTTP Server 2.2.6	Apache Software Foundation Apache HTTP Server 2.2.8
Apache Software Foundation Apache HTTP Server 2.2.9	Apache Software Foundation Apache HTTP Server 2.2.10	Apache Software Foundation Apache HTTP Server 2.2.11
Apache Software Foundation Apache HTTP Server 2.2.12	Apache Software Foundation Apache HTTP Server 2.2.13	Apache Software Foundation Apache HTTP Server 2.2.14
Apache Software Foundation Apache HTTP Server 2.2.15	Apache Software Foundation Apache HTTP Server 2.2.16	Apache Software Foundation Apache HTTP Server 2.2.17
Apache Software Foundation Apache HTTP Server 2.2.18	Apache Software Foundation Apache HTTP Server 2.2.19	Apache Software Foundation Apache HTTP Server 2.2.20
Apache HTTP Server 2.2.21	Apache Software Foundation Apache HTTP Server 2.2.22	Apache Software Foundation Apache HTTP Server 2.2.23
Apache Software Foundation Apache HTTP Server 2.2.24	Apache Software Foundation Apache HTTP Server 2.2.25	Apache Software Foundation Apache HTTP Server 2.2.26
Apache Software Foundation Apache HTTP Server 2.2.27	Apache Software Foundation Apache HTTP Server 2.2.29	Apache Software Foundation Apache HTTP Server 2.2.31
Apache Software Foundation Apache HTTP Server 2.2.32	Apache Software Foundation Apache HTTP Server 2.4.0	Apache Software Foundation Apache HTTP Server 2.4.1
Apache Software Foundation Apache HTTP Server 2.4.2	Apache Software Foundation Apache HTTP Server 2.4.3	Apache Software Foundation Apache HTTP Server 2.4.4
Apache Software Foundation Apache HTTP Server 2.4.6	Apache Software Foundation Apache HTTP Server 2.4.7	Apache Software Foundation Apache HTTP Server 2.4.8
Apache Software Foundation Apache HTTP Server 2.4.9	Apache Software Foundation Apache HTTP Server 2.4.10	Apache Software Foundation Apache HTTP Server 2.4.12
Apache Software Foundation Apache HTTP Server 2.4.14	Apache Software Foundation Apache HTTP Server 2.4.16	Apache Software Foundation Apache HTTP Server 2.4.17
Apache Software Foundation Apache HTTP Server 2.4.18	Apache Software Foundation HTTP Server 2.4.19	Apache Software Foundation HTTP Server 2.4.20
Apache Software Foundation Apache HTTP Server 2.4.21	Apache Software Foundation Apache HTTP Server 2.4.22	Apache Software Foundation HTTP Server 2.4.23
Apache Software Foundation HTTP Server 2.4.24		Apache Software Foundation Apache HTTP Server 2.4.25

References

http://www.debian.org/security/2017/dsa-3896
http://www.oracle.com/technetwork/security-advisory/cpuoct2017-3236626.html
http://www.securityfocus.com/bid/99170
http://www.securitytracker.com/id/1038711
https://access.redhat.com/errata/RHSA-2017:2478
https://access.redhat.com/errata/RHSA-2017:2479
https://access.redhat.com/errata/RHSA-2017:2483
https://access.redhat.com/errata/RHSA-2017:3193
https://access.redhat.com/errata/RHSA-2017:3194
https://access.redhat.com/errata/RHSA-2017:3195
https://access.redhat.com/errata/RHSA-2017:3475
https://access.redhat.com/errata/RHSA-2017:3476
https://access.redhat.com/errata/RHSA-2017:3477
https://github.com/gottburgm/Exploits/tree/master/CVE-2017-7679
https://lists.apache.org/thread.html/f4515e580dfb6eeca589a5cdebd4c4c709ce632b12924f343c3b7751@\%3

https://security.gentoo.org/glsa/201710-32
https://security.netapp.com/advisory/ntap-20180601-0002/
https://support.apple.com/HT208221
https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf03821en_us
https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbux03908en_us
https://www.nomachine.com/SU08O00185

Summary

The stream_reqbody_cl function in mod_proxy_http.c in the mod_proxy module in the Apache HTTP Server before 2.3.3, when a reverse proxy is configured, does not properly handle an amount of streamed data that exceeds the Content-Length value, which allows remote attackers to cause a denial of service (CPU consumption) via crafted requests.

CVE-2009-1890 Information	
CVSS Score	7.1
CWE	CWE-189
Vulnerability impact	
Confidentiality	NONE
Integrity	NONE
Availability	COMPLETE
Access methodology information	
Vector	NETWORK
Complexity	MEDIUM
Authentication	NONE

Vulnerable configs

cpe:2.3:a:apache:http_server:-:win32
Apache Software Foundation Apache HTTP Server
Apache Software Foundation Apache HTTP Server 0.8.11
Apache Software Foundation Apache HTTP Server 0.8.14
Apache Software Foundation Apache HTTP Server 1.0
Apache Software Foundation Apache HTTP Server 1.0.2
Apache Software Foundation Apache HTTP Server 1.0.3
Apache Software Foundation Apache HTTP Server 1.0.5
Apache Software Foundation Apache HTTP Server 1.1
Apache Software Foundation Apache HTTP Server 1.1.1
Apache Software Foundation Apache 1.2
Apache Software Foundation Apache HTTP Server 1.2.4
Apache Software Foundation Apache HTTP Server 1.2.5
Apache Software Foundation Apache HTTP Server 1.2.6
Apache Software Foundation Apache 1.29
Apache Software Foundation Apache HTTP Server 1.3
Apache Software Foundation Apache HTTP Server 1.3.0
Apache Software Foundation Apache HTTP Server 1.3.1
Apache Software Foundation Apache HTTP Server 1.3.1.1
Apache Software Foundation Apache HTTP Server 1.3.2
Apache Software Foundation Apache HTTP Server 1.3.3
Apache Software Foundation Apache HTTP Server 1.3.4
Apache Software Foundation Apache HTTP Server 1.3.5
Apache Software Foundation Apache HTTP Server 1.3.6
cpe:2.3:a:apache:http_server:1.3.6:-:win32
Apache Software Foundation Apache HTTP Server 1.3.7
cpe:2.3:a:apache:http_server:1.3.7:-:dev
Apache Software Foundation Apache HTTP Server 1.3.8
Apache Software Foundation Apache HTTP Server 1.3.9
cpe:2.3:a:apache:http_server:1.3.9:-:win32
Apache Software Foundation Apache 1.3.10
Apache Software Foundation Apache HTTP Server 1.3.11
cpe:2.3:a:apache:http_server:1.3.11:-:win32
Apache Software Foundation Apache HTTP Server 1.3.12
cpe:2.3:a:apache:http_server:1.3.12:-:win32
Apache Software Foundation Apache 1.3.13
cpe:2.3:a:apache:http_server:1.3.13:-:win32
Apache Software Foundation Apache HTTP Server 1.3.14
cpe:2.3:a:apache:http_server:1.3.14:-:mac_os
cpe:2.3:a:apache:http_server:1.3.14:-:win32
Apache Software Foundation Apache 1.3.15
cpe:2.3:a:apache:http_server:1.3.15:-:win32
Apache Software Foundation Apache 1.3.16
cpe:2.3:a:apache:http_server:1.3.16:-:win32
Apache Software Foundation Apache HTTP Server 1.3.17
cpe:2.3:a:apache:http_server:1.3.17:-:win32
Apache Software Foundation Apache HTTP Server 1.3.18
cpe:2.3:a:apache:http_server:1.3.18:-:win32
Apache Software Foundation Apache HTTP Server 1.3.19
cpe:2.3:a:apache:http_server:1.3.19:-:win32
Apache Software Foundation Apache HTTP Server 1.3.20
cpe:2.3:a:apache:http_server:1.3.20:-:win32
Apache Software Foundation Apache HTTP Server 1.3.22
cpe:2.3:a:apache:http_server:1.3.22:-:win32
Apache Software Foundation Apache HTTP Server 1.3.23
cpe:2.3:a:apache:http_server:1.3.23:-:win32
Apache Software Foundation Apache HTTP Server 1.3.24
cpe:2.3:a:apache:http_server:1.3.24:-:win32
Apache Software Foundation Apache HTTP Server 1.3.25
cpe:2.3:a:apache:http_server:1.3.25:-:win32
Apache Software Foundation Apache HTTP Server 1.3.26
cpe:2.3:a:apache:http_server:1.3.26:-:win32
Apache Software Foundation Apache HTTP Server 1.3.27
Apache Software Foundation Apache HTTP Server 1.3.28
Apache Software Foundation Apache HTTP Server 1.3.29
Apache Software Foundation Apache HTTP Server 1.3.30
Apache Software Foundation Apache HTTP Server 1.3.31
Apache Software Foundation Apache HTTP Server 1.3.32
Apache Software Foundation Apache HTTP Server 1.3.33
Apache Software Foundation Apache HTTP Server 1.3.34
Apache Software Foundation Apache HTTP Server 1.3.35
Apache Software Foundation Apache HTTP Server 1.3.36
Apache Software Foundation Apache HTTP Server 1.3.37
Apache Software Foundation Apache HTTP Server 1.3.38
Apache Software Foundation Apache HTTP Server 1.3.39
Apache Software Foundation Apache HTTP Server 1.3.65
Apache Software Foundation Apache HTTP Server 1.3.68
Apache Software Foundation Apache HTTP Server 1.4.0
Apache Software Foundation Apache HTTP Server 1.99
Apache Software Foundation Apache HTTP Server 2.0
Apache Software Foundation Apache HTTP Server 2.0.9a
Apache Software Foundation Apache HTTP Server 2.0.28
Apache Software Foundation Apache HTTP Server 2.0.28 Beta
cpe:2.3:a:apache:http_server:2.0.28:beta:win32
Apache Software Foundation Apache HTTP Server 2.0.32
Apache Software Foundation Apache HTTP Server 2.0.32 Beta
cpe:2.3:a:apache:http_server:2.0.32:beta:win32
Apache Software Foundation Apache HTTP Server 2.0.34 Beta

cpe:2.3:a:apache:http_server:2.0.34:beta:win32	Apache Software Foundation Apache HTTP Server 2.0.35	Apache Software Foundation Apache HTTP Server 2.0.36
Apache Software Foundation Apache HTTP Server 2.0.37	Apache Software Foundation Apache HTTP Server 2.0.38	Apache Software Foundation Apache HTTP Server 2.0.39
Apache Software Foundation Apache HTTP Server 2.0.40	Apache Software Foundation Apache HTTP Server 2.0.41	Apache Software Foundation Apache HTTP Server 2.0.42
Apache Software Foundation Apache HTTP Server 2.0.43	Apache Software Foundation Apache HTTP Server 2.0.44	Apache Software Foundation Apache HTTP Server 2.0.45
Apache Software Foundation Apache HTTP Server 2.0.46	cpe:2.3:a:apache:http_server:2.0.46:-:win32	Apache Software Foundation Apache HTTP Server 2.0.47
Apache Software Foundation Apache HTTP Server 2.0.48	Apache Software Foundation Apache HTTP Server 2.0.49	Apache Software Foundation Apache HTTP Server 2.0.50
Apache Software Foundation Apache HTTP Server 2.0.51	Apache Software Foundation Apache HTTP Server 2.0.52	Apache Software Foundation Apache HTTP Server 2.0.53
Apache Software Foundation Apache HTTP Server 2.0.54	Apache Software Foundation Apache HTTP Server 2.0.55	Apache Software Foundation Apache HTTP Server 2.0.56
Apache Software Foundation Apache HTTP Server 2.0.57	Apache Software Foundation Apache HTTP Server 2.0.58	cpe:2.3:a:apache:http_server:2.0.58:-:win32
Apache Software Foundation HTTP Server 2.0.59	Apache Software Foundation Apache HTTP Server 2.0.60 dev	Apache Software Foundation HTTP Server 2.0.61
Apache Software Foundation Apache HTTP Server 2.1	Apache Software Foundation Apache HTTP Server 2.1.1	Apache Software Foundation Apache HTTP Server 2.1.2
Apache Software Foundation Apache HTTP Server 2.1.3	Apache Software Foundation Apache HTTP Server 2.1.4	Apache Software Foundation Apache HTTP Server 2.1.5
Apache Software Foundation Apache HTTP Server 2.1.6	Apache Software Foundation Apache HTTP Server 2.1.7	Apache Software Foundation Apache HTTP Server 2.1.8
Apache Software Foundation Apache HTTP Server 2.1.9	Apache Software Foundation Apache HTTP Server 2.2	Apache Software Foundation Apache HTTP Server 2.2.0
Apache Software Foundation Apache HTTP Server 2.2.1	Apache Software Foundation Apache HTTP Server 2.2.2	cpe:2.3:a:apache:http_server:2.2.2:-:windows
Apache Software Foundation Apache HTTP Server 2.2.3	cpe:2.3:a:apache:http_server:2.2.3:-:windows	Apache Software Foundation Apache HTTP Server 2.2.4
Apache Software Foundation Apache HTTP Server 2.2.6	cpe:2.3:a:apache:http_server:2.2.7	Apache Software Foundation Apache HTTP Server 2.2.8
Apache Software Foundation Apache HTTP Server 2.2.9	Apache Software Foundation Apache HTTP Server 2.2.10	Apache Software Foundation Apache HTTP Server 2.2.11
Apache Software Foundation Apache HTTP Server 2.3.0	Apache Software Foundation Apache HTTP Server 2.3.1	Apache Software Foundation Apache HTTP Server 2.3.2

References

http://lists.apple.com/archives/security-announce/2009/Nov/msg00000.html

http://lists.opensuse.org/opensuse-security-announce/2009-10/msg00006.html

http://marc.info/?l=bugtraq&m=129190899612998&w=2

http://security.gentoo.org/glsa/glsa-200907-04.xml

http://support.apple.com/kb/HT3937

http://svn.apache.org/viewvc/httpd/httpd/trunk/CHANGES?r1=790587&r2=790586&pathrev=790587

http://svn.apache.org/viewvc/httpd/httpd/trunk/CHANGES?revision=790587

http://svn.apache.org/viewvc/httpd/httpd/trunk/modules/proxy/mod_proxy_http.c?r1=790587&r2=790586

http://svn.apache.org/viewvc?view=rev&revision=790587

http://wiki.rpath.com/Advisories:rPSA-2009-0142

http://www-01.ibm.com/support/docview.wss?uid=swg1PK91259

http://www-01.ibm.com/support/docview.wss?uid=swg1PK99480

http://www.debian.org/security/2009/dsa-1834

http://www.mandriva.com/security/advisories?name=MDVSA-2009:149

http://www.mandriva.com/security/advisories?name=MDVSA-2013:150

http://www.oracle.com/technetwork/topics/security/cpuapr2013-1899555.html

http://www.redhat.com/support/errata/RHSA-2009-1156.html

http://www.securityfocus.com/archive/1/507852/100/0/threaded

http://www.securityfocus.com/archive/1/507857/100/0/threaded

http://www.securityfocus.com/bid/35565

http://www.securitytracker.com/id?1022509

http://www.ubuntu.com/usn/USN-802-1

http://www.vupen.com/english/advisories/2009/3184

https://rhn.redhat.com/errata/RHSA-2009-1148.html

https://www.redhat.com/archives/fedora-package-announce/2009-August/msg01363.html

Summary

The mod_deflate module in Apache httpd 2.2.11 and earlier compresses large files until completion even after the associated network connection is closed, which allows remote attackers to cause a denial of service (CPU consumption).

CVE-2009-1891 Information	
CVSS Score	7.1
CWE	CWE-399
Vulnerability impact	
Confidentiality	NONE
Integrity	NONE
Availability	COMPLETE
Access methodology information	
Vector	NETWORK
Complexity	MEDIUM
Authentication	NONE

Vulnerable configs

Apache Software Foundation Apache HTTP Server	Apache Software Foundation Apache HTTP Server 0.8.11	Apache Software Foundation Apache HTTP Server 0.8.14
Apache Software Foundation Apache HTTP Server 1.0.2	Apache Software Foundation Apache HTTP Server 1.0.3	Apache Software Foundation Apache HTTP Server 1.0.5
Apache Software Foundation Apache HTTP Server 1.1	Apache Software Foundation Apache HTTP Server 1.1.1	Apache Software Foundation Apache 1.2
Apache Software Foundation Apache HTTP Server 1.2.4	Apache Software Foundation Apache 1.29	Apache Software Foundation Apache HTTP Server 1.3.3
Apache Software Foundation Apache HTTP Server 1.3.6	Apache Software Foundation Apache HTTP Server 1.3.7	Apache Software Foundation Apache HTTP Server 1.3.9
Apache Software Foundation Apache 1.3.13	Apache Software Foundation Apache HTTP Server 1.3.14	Apache Software Foundation Apache HTTP Server 1.3.18
Apache Software Foundation Apache HTTP Server 1.3.19	Apache Software Foundation Apache HTTP Server 1.3.20	Apache Software Foundation Apache HTTP Server 1.3.22
Apache Software Foundation Apache HTTP Server 1.3.23	Apache Software Foundation Apache HTTP Server 1.3.27	Apache Software Foundation Apache HTTP Server 1.3.29
Apache Software Foundation Apache HTTP Server 1.3.31	Apache Software Foundation Apache HTTP Server 1.3.33	Apache Software Foundation Apache HTTP Server 1.3.38
Apache Software Foundation Apache HTTP Server 1.99	Apache Software Foundation Apache HTTP Server 2.0.9a	Apache Software Foundation Apache HTTP Server 2.0.28
Apache Software Foundation Apache HTTP Server 2.0.34 Beta	Apache Software Foundation Apache HTTP Server 2.0.38	Apache Software Foundation Apache HTTP Server 2.0.39
Apache Software Foundation Apache HTTP Server 2.0.40	Apache Software Foundation Apache HTTP Server 2.0.41	Apache Software Foundation Apache HTTP Server 2.0.42
Apache Software Foundation Apache HTTP Server 2.0.45	Apache Software Foundation Apache HTTP Server 2.0.46	Apache Software Foundation Apache HTTP Server 2.0.47
Apache Software Foundation Apache HTTP Server 2.0.48	Apache Software Foundation Apache HTTP Server 2.0.49	Apache Software Foundation Apache HTTP Server 2.0.50
Apache Software Foundation Apache HTTP Server 2.0.51	Apache Software Foundation Apache HTTP Server 2.0.52	Apache Software Foundation Apache HTTP Server 2.0.53
Apache Software Foundation Apache HTTP Server 2.0.54	Apache Software Foundation Apache HTTP Server 2.0.55	Apache Software Foundation Apache HTTP Server 2.0.56
Apache Software Foundation Apache HTTP Server 2.0.57	Apache Software Foundation Apache HTTP Server 2.0.58	Apache Software Foundation HTTP Server 2.0.59
Apache Software Foundation Apache HTTP Server 2.0.60 dev	Apache Software Foundation HTTP Server 2.0.61	Apache Software Foundation Apache HTTP Server 2.1
Apache Software Foundation Apache HTTP Server 2.1.1	Apache Software Foundation Apache HTTP Server 2.1.2	Apache Software Foundation Apache HTTP Server 2.1.3
Apache Software Foundation Apache HTTP Server 2.1.4	Apache Software Foundation Apache HTTP Server 2.1.5	Apache Software Foundation Apache HTTP Server 2.1.6
Apache Software Foundation Apache HTTP Server 2.1.7	Apache Software Foundation Apache HTTP Server 2.1.8	Apache Software Foundation Apache HTTP Server 2.1.9
Apache Software Foundation Apache HTTP Server 2.2	Apache Software Foundation Apache HTTP Server 2.2.0	Apache Software Foundation Apache HTTP Server 2.2.1
Apache Software Foundation Apache HTTP Server 2.2.2	Apache Software Foundation Apache HTTP Server 2.2.3	Apache Software Foundation Apache HTTP Server 2.2.4
Apache Software Foundation Apache HTTP Server 2.2.6	cpe:2.3:a:apache:http_server:2.2.7	Apache Software Foundation Apache HTTP Server 2.2.8
Apache Software Foundation Apache HTTP Server 2.2.9	Apache Software Foundation Apache HTTP Server 2.2.10	Apache Software Foundation Apache HTTP Server 2.2.11

References

http://bugs.debian.org/cgi-bin/bugreport.cgi?bug=534712
http://lists.apple.com/archives/security-announce/2009/Nov/msg00000.html
http://lists.opensuse.org/opensuse-security-announce/2009-10/msg00006.html
http://marc.info/?l=apache-httpd-dev&m=124621326524824&w=2
http://marc.info/?l=apache-httpd-dev&m=124661528519546&w=2
http://marc.info/?l=bugtraq&m=129190899612998&w=2
http://marc.info/?l=bugtraq&m=130497311408250&w=2
http://security.gentoo.org/glsa/glsa-200907-04.xml
http://support.apple.com/kb/HT3937
http://wiki.rpath.com/Advisories:rPSA-2009-0142
http://wiki.rpath.com/wiki/Advisories:rPSA-2009-0142
http://www-01.ibm.com/support/docview.wss?uid=swg1PK91361
http://www-01.ibm.com/support/docview.wss?uid=swg1PK99480
http://www.debian.org/security/2009/dsa-1834
http://www.mandriva.com/security/advisories?name=MDVSA-2009:149
http://www.redhat.com/support/errata/RHSA-2009-1156.html
http://www.securityfocus.com/archive/1/507857/100/0/threaded
http://www.securitytracker.com/id?1022529
http://www.ubuntu.com/usn/USN-802-1
http://www.vupen.com/english/advisories/2009/1841
http://www.vupen.com/english/advisories/2009/3184
https://bugzilla.redhat.com/show_bug.cgi?id=509125
https://rhn.redhat.com/errata/RHSA-2009-1148.html
https://www.redhat.com/archives/fedora-package-announce/2009-August/msg01363.html

Summary

envvars (aka envvars-std) in the Apache HTTP Server before 2.4.2 places a zero-length directory name in the LD_LIBRARY_PATH, which allows local users to gain privileges via a Trojan horse DSO in the current working directory during execution of apachectl.

CVE-2012-0883 Information	
CVSS Score	6.9
CWE	CWE-264
Vulnerability impact	
Confidentiality	COMPLETE
Integrity	COMPLETE
Availability	COMPLETE
Access methodology information	
Vector	LOCAL
Complexity	MEDIUM
Authentication	NONE

Vulnerable configs

Apache Software Foundation Apache HTTP Server 0.8.11 Apache Software Foundation Apache HTTP Server 0.8.14 Apache Software Foundation Apache HTTP Server 1.0
Apache Software Foundation Apache HTTP Server 1.0.2 Apache Software Foundation Apache HTTP Server 1.0.3 Apache Software Foundation Apache HTTP Server 1.0.5
Apache Software Foundation Apache HTTP Server 1.1 Apache Software Foundation Apache HTTP Server 1.1.1 Apache Software Foundation Apache 1.2
Apache Software Foundation Apache HTTP Server 1.2.4 Apache Software Foundation Apache HTTP Server 1.2.5 Apache Software Foundation Apache HTTP Server 1.2.6
Apache Software Foundation Apache 1.29 Apache Software Foundation Apache HTTP Server 1.3 Apache Software Foundation Apache HTTP Server 1.3.0
Apache Software Foundation Apache HTTP Server 1.3.1 Apache Software Foundation Apache HTTP Server 1.3.1.1 Apache Software Foundation Apache HTTP Server 1.3.2
Apache Software Foundation Apache HTTP Server 1.3.3 Apache Software Foundation Apache HTTP Server 1.3.4 Apache Software Foundation Apache HTTP Server 1.3.5
Apache Software Foundation Apache HTTP Server 1.3.6 Apache Software Foundation Apache HTTP Server 1.3.7 Apache Software Foundation Apache HTTP Server 1.3.8
Apache Software Foundation Apache HTTP Server 1.3.9 Apache Software Foundation Apache 1.3.10 Apache Software Foundation Apache HTTP Server 1.3.11
Apache Software Foundation Apache HTTP Server 1.3.12 Apache Software Foundation Apache 1.3.13 Apache Software Foundation Apache HTTP Server 1.3.14
Apache Software Foundation Apache 1.3.15 Apache Software Foundation Apache 1.3.16 Apache Software Foundation Apache HTTP Server 1.3.17
Apache Software Foundation Apache HTTP Server 1.3.18 Apache Software Foundation Apache HTTP Server 1.3.19 Apache Software Foundation Apache HTTP Server 1.3.20
Apache Software Foundation Apache HTTP Server 1.3.22 Apache Software Foundation Apache HTTP Server 1.3.23 Apache Software Foundation Apache HTTP Server 1.3.24
Apache Software Foundation Apache HTTP Server 1.3.25 Apache Software Foundation Apache HTTP Server 1.3.26 Apache Software Foundation Apache HTTP Server 1.3.27
Apache Software Foundation Apache HTTP Server 1.3.28 Apache Software Foundation Apache HTTP Server 1.3.29 Apache Software Foundation Apache HTTP Server 1.3.30
Apache Software Foundation Apache HTTP Server 1.3.31 Apache Software Foundation Apache HTTP Server 1.3.32 Apache Software Foundation Apache HTTP Server 1.3.33
Apache Software Foundation Apache HTTP Server 1.3.34 Apache Software Foundation Apache HTTP Server 1.3.35 Apache Software Foundation Apache HTTP Server 1.3.36
Apache Software Foundation Apache HTTP Server 1.3.37 Apache Software Foundation Apache HTTP Server 1.3.38 Apache Software Foundation Apache HTTP Server 1.3.39
Apache Software Foundation Apache HTTP Server 1.3.41 Apache Software Foundation Apache HTTP Server 1.3.42 Apache Software Foundation Apache HTTP Server 1.3.65
Apache Software Foundation Apache HTTP Server 1.3.68 Apache Software Foundation Apache HTTP Server 1.4.0 Apache Software Foundation Apache HTTP Server 1.99
Apache Software Foundation Apache HTTP Server 2.0 Apache Software Foundation Apache HTTP Server 2.0.9a Apache Software Foundation Apache HTTP Server 2.0.28
Apache Software Foundation Apache HTTP Server 2.0.28 Beta Apache Software Foundation Apache HTTP Server 2.0.32 Apache Software Foundation Apache HTTP Server 2.0.32 Beta
Apache Software Foundation Apache HTTP Server 2.0.34 Beta Apache Software Foundation Apache HTTP Server 2.0.35 Apache Software Foundation Apache HTTP Server 2.0.36
Apache Software Foundation Apache HTTP Server 2.0.37 Apache Software Foundation Apache HTTP Server 2.0.38 Apache Software Foundation Apache HTTP Server 2.0.39
Apache Software Foundation Apache HTTP Server 2.0.40 Apache Software Foundation Apache HTTP Server 2.0.41 Apache Software Foundation Apache HTTP Server 2.0.42
Apache Software Foundation Apache HTTP Server 2.0.43 Apache Software Foundation Apache HTTP Server 2.0.44 Apache Software Foundation Apache HTTP Server 2.0.45
Apache Software Foundation Apache HTTP Server 2.0.46 Apache Software Foundation Apache HTTP Server 2.0.47 Apache Software Foundation Apache HTTP Server 2.0.48
Apache Software Foundation Apache HTTP Server 2.0.49 Apache Software Foundation Apache HTTP Server 2.0.50 Apache Software Foundation Apache HTTP Server 2.0.51
Apache Software Foundation Apache HTTP Server 2.0.52 Apache Software Foundation Apache HTTP Server 2.0.53 Apache Software Foundation Apache HTTP Server 2.0.54
Apache Software Foundation Apache HTTP Server 2.0.55 Apache Software Foundation Apache HTTP Server 2.0.56 Apache Software Foundation Apache HTTP Server 2.0.57
Apache Software Foundation Apache HTTP Server 2.0.58 Apache Software Foundation HTTP Server 2.0.59 Apache Software Foundation Apache HTTP Server 2.0.60 dev
Apache Software Foundation HTTP Server 2.0.61 Apache Software Foundation Apache HTTP Server 2.0.63 Apache Software Foundation Apache HTTP Server 2.1

Apache Software Foundation Apache HTTP Server 2.1.1 Apache Software Foundation Apache HTTP Server 2.1.2 Apache Software Foundation Apache HTTP Server 2.1.3
Apache Software Foundation Apache HTTP Server 2.1.4 Apache Software Foundation Apache HTTP Server 2.1.5 Apache Software Foundation Apache HTTP Server 2.1.6
Apache Software Foundation Apache HTTP Server 2.1.7 Apache Software Foundation Apache HTTP Server 2.1.8 Apache Software Foundation Apache HTTP Server 2.1.9
Apache Software Foundation Apache HTTP Server 2.2 Apache Software Foundation Apache HTTP Server 2.2.0 Apache Software Foundation Apache HTTP Server 2.2.1
Apache Software Foundation Apache HTTP Server 2.2.2 Apache Software Foundation Apache HTTP Server 2.2.3 Apache Software Foundation Apache HTTP Server 2.2.4
Apache Software Foundation Apache HTTP Server 2.2.6 Apache Software Foundation Apache HTTP Server 2.2.8 Apache Software Foundation Apache HTTP Server 2.2.9
Apache Software Foundation Apache HTTP Server 2.2.10 Apache Software Foundation Apache HTTP Server 2.2.11 Apache Software Foundation Apache HTTP Server 2.2.12
Apache Software Foundation Apache HTTP Server 2.2.13 Apache Software Foundation Apache HTTP Server 2.2.14 Apache Software Foundation Apache HTTP Server 2.2.15
Apache Software Foundation Apache HTTP Server 2.2.16 Apache Software Foundation Apache HTTP Server 2.2.17 Apache Software Foundation Apache HTTP Server 2.2.18
Apache Software Foundation Apache HTTP Server 2.2.19 Apache Software Foundation Apache HTTP Server 2.2.20 Apache HTTP Server 2.2.21
Apache Software Foundation Apache HTTP Server 2.3.0 Apache Software Foundation Apache HTTP Server 2.3.1 Apache Software Foundation Apache HTTP Server 2.3.2
Apache Software Foundation Apache HTTP Server 2.3.3 Apache Software Foundation Apache HTTP Server 2.3.4 Apache Software Foundation Apache HTTP Server 2.3.5
Apache Software Foundation Apache HTTP Server 2.3.6 Apache Software Foundation Apache HTTP Server 2.3.7 Apache Software Foundation Apache HTTP Server 2.3.8
Apache Software Foundation Apache HTTP Server 2.3.9 Apache Software Foundation Apache HTTP Server 2.3.10 Apache Software Foundation Apache HTTP Server 2.3.11
Apache Software Foundation Apache HTTP Server 2.3.12 Apache Software Foundation Apache HTTP Server 2.3.13 Apache Software Foundation Apache HTTP Server 2.3.14
Apache Software Foundation Apache HTTP Server 2.3.15 Apache Software Foundation Apache HTTP Server 2.3.16 Apache Software Foundation Apache HTTP Server 2.4.0
Apache Software Foundation Apache HTTP Server 2.4.1

References

http://article.gmane.org/gmane.comp.apache.devel/48158
http://lists.apple.com/archives/security-announce/2013/Sep/msg00002.html
http://lists.opensuse.org/opensuse-updates/2013-02/msg00009.html
http://lists.opensuse.org/opensuse-updates/2013-02/msg00012.html
http://marc.info/?l=bugtraq&m=134012830914727&w=2
http://support.apple.com/kb/HT5880
http://svn.apache.org/viewvc?view=revision&revision=1296428
http://www.apache.org/dist/httpd/Announcement2.4.html
http://www.apachelounge.com/Changelog-2.4.html
http://www.securityfocus.com/bid/53046
http://www.securitytracker.com/id?1026932
http://www.xerox.com/download/security/security-bulletin/16287-4d6b7b0c81f7b/cert_XRX13-003_v1.0.pdf
https://exchange.xforce.ibmcloud.com/vulnerabilities/74901
https://h20564.www2.hp.com/portal/site/hpsc/public/kb/docDisplay?docId=emr_na-c03839862
https://httpd.apache.org/security/vulnerabilities_24.html

Summary

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 Information	
CVSS Score	5.1
CWE	CWE-310
Vulnerability impact	
Confidentiality	PARTIAL
Integrity	PARTIAL
Availability	PARTIAL
Access methodology information	
Vector	NETWORK
Complexity	HIGH
Authentication	NONE

Vulnerable configs

Apache Software Foundation Apache HTTP Server 2.2.24
Apache Software Foundation Apache HTTP Server 2.2.23
Apache Software Foundation Apache HTTP Server 2.2.1
Apache Software Foundation Apache HTTP Server 2.2.6
Apache Software Foundation Apache HTTP Server 2.2.2
Apache Software Foundation Apache HTTP Server 2.2.0
Apache Software Foundation Apache HTTP Server 2.2.9
Apache Software Foundation Apache HTTP Server 2.2.8
Apache Software Foundation Apache HTTP Server 2.2.14
Apache Software Foundation Apache HTTP Server 2.2.19
Apache Software Foundation Apache HTTP Server 2.2.16
Apache HTTP Server 2.2.21
Apache Software Foundation Apache HTTP Server 2.2.4
Apache Software Foundation Apache HTTP Server 2.2.11
Apache Software Foundation Apache HTTP Server 2.2.13
Apache Software Foundation Apache HTTP Server 2.2.3
Apache Software Foundation Apache HTTP Server 2.2.22
Apache Software Foundation Apache HTTP Server 2.2
Apache Software Foundation Apache HTTP Server 2.2.15
Apache Software Foundation Apache HTTP Server 2.2.12
Apache Software Foundation Apache HTTP Server 2.2.17
Apache Software Foundation Apache HTTP Server 2.2.18
Apache Software Foundation Apache HTTP Server 2.2.10
Apache Software Foundation Apache HTTP Server 2.2.20

References

http://lists.opensuse.org/opensuse-updates/2013-08/msg00026.html
http://lists.opensuse.org/opensuse-updates/2013-08/msg00029.html
http://lists.opensuse.org/opensuse-updates/2013-08/msg00030.html
http://people.apache.org/~jorton/mod_rewrite-CVE-2013-1862.patch
http://rhn.redhat.com/errata/RHSA-2013-0815.html

http://rhn.redhat.com/errata/RHSA-2013-1207.html
http://rhn.redhat.com/errata/RHSA-2013-1208.html
http://rhn.redhat.com/errata/RHSA-2013-1209.html
http://support.apple.com/kb/HT6150
http://svn.apache.org/viewvc?view=revision&revision=r1469311
http://tools.cisco.com/security/center/content/CiscoSecurityNotice/CVE-2013-1862
http://www-01.ibm.com/support/docview.wss?uid=swg21644047
http://www.fujitsu.com/global/support/software/security/products-f/interstage-201303e.html
http://www.mandriva.com/security/advisories?name=MDVSA-2013:174
http://www.oracle.com/technetwork/topics/security/cpujan2014-1972949.html
http://www.securityfocus.com/bid/59826
http://www.securityfocus.com/bid/64758
http://www.ubuntu.com/usn/USN-1903-1
https://bugzilla.redhat.com/show_bug.cgi?id=953729
https://h20566.www2.hp.com/portal/site/hpsc/template.PAGE/public/kb/docDisplay/?spf_p.tpst=kbDocD
navigationalState\%3DdocId\%253Demr_na-c03922406-1\%257CdocLocale\%253D\%257CcalledBy\%253

Summary

The mod_cgid module in the Apache HTTP Server before 2.4.10 does not have a timeout mechanism, which allows remote attackers to cause a denial of service (process hang) via a request to a CGI script that does not read from its stdin file descriptor.

CVE-2014-0231 Information	
CVSS Score	5.0
CWE	CWE-399
Vulnerability impact	
Confidentiality	NONE
Integrity	NONE
Availability	PARTIAL
Access methodology information	
Vector	NETWORK
Complexity	LOW
Authentication	NONE

Vulnerable configs

Apache Software Foundation Apache HTTP Server		Apache Software Foundation Apache HTTP Server 2.2.0
Apache Software Foundation Apache HTTP Server 2.2.2	Apache Software Foundation Apache HTTP Server 2.2.3	Apache Software Foundation Apache HTTP Server 2.2.4
Apache Software Foundation Apache HTTP Server 2.2.6	Apache Software Foundation Apache HTTP Server 2.2.8	Apache Software Foundation Apache HTTP Server 2.2.9
Apache Software Foundation Apache HTTP Server 2.2.10	Apache Software Foundation Apache HTTP Server 2.2.11	Apache Software Foundation Apache HTTP Server 2.2.12
Apache Software Foundation Apache HTTP Server 2.2.13	Apache Software Foundation Apache HTTP Server 2.2.14	Apache Software Foundation Apache HTTP Server 2.2.15
Apache Software Foundation Apache HTTP Server 2.2.16	Apache Software Foundation Apache HTTP Server 2.2.17	Apache Software Foundation Apache HTTP Server 2.2.18
Apache Software Foundation Apache HTTP Server 2.2.19	Apache Software Foundation Apache HTTP Server 2.2.20	Apache HTTP Server 2.2.21
Apache Software Foundation Apache HTTP Server 2.2.22	Apache Software Foundation Apache HTTP Server 2.2.23	Apache Software Foundation Apache HTTP Server 2.2.24
Apache Software Foundation Apache HTTP Server 2.2.25	Apache Software Foundation Apache HTTP Server 2.2.26	Apache Software Foundation Apache HTTP Server 2.2.27
Apache Software Foundation Apache HTTP Server 2.4.1	Apache Software Foundation Apache HTTP Server 2.4.2	Apache Software Foundation Apache HTTP Server 2.4.3
Apache Software Foundation Apache HTTP Server 2.4.4	Apache Software Foundation Apache HTTP Server 2.4.6	Apache Software Foundation Apache HTTP Server 2.4.7
Apache Software Foundation Apache HTTP Server 2.4.8		Apache Software Foundation Apache HTTP Server 2.4.9

References

http://advisories.mageia.org/MGASA-2014-0304.html
http://advisories.mageia.org/MGASA-2014-0305.html
http://httpd.apache.org/security/vulnerabilities_24.html
http://lists.apple.com/archives/security-announce/2015/Apr/msg00001.html
http://marc.info/?l=bugtraq&m=143403519711434&w=2

http://marc.info/?l=bugtraq&m=143748090628601&w=2
http://marc.info/?l=bugtraq&m=144050155601375&w=2
http://marc.info/?l=bugtraq&m=144493176821532&w=2
http://packetstormsecurity.com/files/130769/RSA-Digital-Certificate-Solution-XSS-Denial-Of-Service.html
http://rhn.redhat.com/errata/RHSA-2014-1019.html
http://rhn.redhat.com/errata/RHSA-2014-1020.html
http://rhn.redhat.com/errata/RHSA-2014-1021.html
http://svn.apache.org/repos/asf/httpd/httpd/branches/2.2.x/CHANGES
http://svn.apache.org/viewvc/httpd/httpd/trunk/modules/generators/mod_cgid.c
http://svn.apache.org/viewvc/httpd/httpd/trunk/modules/generators/mod_cgid.c?r1=1482522&r2=153512
http://svn.apache.org/viewvc/httpd/httpd/trunk/modules/generators/mod_cgid.c?r1=1565711&r2=161050
http://www.debian.org/security/2014/dsa-2989
http://www.mandriva.com/security/advisories?name=MDVSA-2014:142
http://www.oracle.com/technetwork/topics/security/cpujan2015-1972971.html
http://www.securityfocus.com/bid/68742
https://bugzilla.redhat.com/show_bug.cgi?id=1120596
https://h20564.www2.hpe.com/portal/site/hpsc/public/kb/docDisplay?docId=emr_na-c04832246
https://puppet.com/security/cve/cve-2014-0231
https://security.gentoo.org/glsa/201504-03
https://support.apple.com/HT204659

Summary

The dav_xml_get_cdata function in main/util.c in the mod_dav module in the Apache HTTP Server before 2.4.8 does not properly remove whitespace characters from CDATA sections, which allows remote attackers to cause a denial of service (daemon crash) via a crafted DAV WRITE request.

CVE-2013-6438 Information	
CVSS Score	5.0
CWE	CWE-20
Vulnerability impact	
Confidentiality	NONE
Integrity	NONE
Availability	PARTIAL
Access methodology information	
Vector	NETWORK
Complexity	LOW
Authentication	NONE

Vulnerable configs

Apache Software Foundation Apache HTTP Server 2.0		
Apache Software Foundation Apache HTTP Server 2.0.9a	Apache Software Foundation Apache HTTP Server 2.0.28	Apache Software Foundation Apache HTTP Server 2.0.28 Beta
Apache Software Foundation Apache HTTP Server 2.0.32	Apache Software Foundation Apache HTTP Server 2.0.32 Beta	Apache Software Foundation Apache HTTP Server 2.0.34 Beta
Apache Software Foundation Apache HTTP Server 2.0.35	Apache Software Foundation Apache HTTP Server 2.0.36	Apache Software Foundation Apache HTTP Server 2.0.37
Apache Software Foundation Apache HTTP Server 2.0.38	Apache Software Foundation Apache HTTP Server 2.0.39	Apache Software Foundation Apache HTTP Server 2.0.40
Apache Software Foundation Apache HTTP Server 2.0.41	Apache Software Foundation Apache HTTP Server 2.0.42	Apache Software Foundation Apache HTTP Server 2.0.43
Apache Software Foundation Apache HTTP Server 2.0.44	Apache Software Foundation Apache HTTP Server 2.0.45	Apache Software Foundation Apache HTTP Server 2.0.46
Apache Software Foundation Apache HTTP Server 2.0.47	Apache Software Foundation Apache HTTP Server 2.0.48	Apache Software Foundation Apache HTTP Server 2.0.49
Apache Software Foundation Apache HTTP Server 2.0.50	Apache Software Foundation Apache HTTP Server 2.0.51	Apache Software Foundation Apache HTTP Server 2.0.52
Apache Software Foundation Apache HTTP Server 2.0.53	Apache Software Foundation Apache HTTP Server 2.0.54	Apache Software Foundation Apache HTTP Server 2.0.55
Apache Software Foundation Apache HTTP Server 2.0.56	Apache Software Foundation Apache HTTP Server 2.0.57	Apache Software Foundation Apache HTTP Server 2.0.58
Apache Software Foundation HTTP Server 2.0.59	Apache Software Foundation Apache HTTP Server 2.0.60 dev	Apache Software Foundation HTTP Server 2.0.61
Apache Software Foundation Apache HTTP Server 2.0.63	Apache Software Foundation Apache HTTP Server 2.0.64	Apache Software Foundation Apache HTTP Server 2.1
Apache Software Foundation Apache HTTP Server 2.1.1	Apache Software Foundation Apache HTTP Server 2.1.2	Apache Software Foundation Apache HTTP Server 2.1.3
Apache Software Foundation Apache HTTP Server 2.1.4	Apache Software Foundation Apache HTTP Server 2.1.5	Apache Software Foundation Apache HTTP Server 2.1.6
Apache Software Foundation Apache HTTP Server 2.1.7	Apache Software Foundation Apache HTTP Server 2.1.8	Apache Software Foundation Apache HTTP Server 2.1.9
Apache Software Foundation Apache HTTP Server 2.2	Apache Software Foundation Apache HTTP Server 2.2.0	Apache Software Foundation Apache HTTP Server 2.2.1
Apache Software Foundation Apache HTTP Server 2.2.2	Apache Software Foundation Apache HTTP Server 2.2.3	Apache Software Foundation Apache HTTP Server 2.2.4
Apache Software Foundation Apache HTTP Server 2.2.6	Apache Software Foundation Apache HTTP Server 2.2.8	Apache Software Foundation Apache HTTP Server 2.2.9
Apache Software Foundation Apache HTTP Server 2.2.10	Apache Software Foundation Apache HTTP Server 2.2.11	Apache Software Foundation Apache HTTP Server 2.2.12
Apache Software Foundation Apache HTTP Server 2.2.13	Apache Software Foundation Apache HTTP Server 2.2.14	Apache Software Foundation Apache HTTP Server 2.2.15
Apache Software Foundation Apache HTTP Server 2.2.16	Apache Software Foundation Apache HTTP Server 2.2.17	Apache Software Foundation Apache HTTP Server 2.2.18
Apache Software Foundation Apache HTTP Server 2.2.19	Apache Software Foundation Apache HTTP Server 2.2.20	Apache HTTP Server 2.2.21
Apache Software Foundation Apache HTTP Server 2.2.22	Apache Software Foundation Apache HTTP Server 2.2.23	Apache Software Foundation Apache HTTP Server 2.2.24
Apache Software Foundation Apache HTTP Server 2.2.25	Apache Software Foundation Apache HTTP Server 2.3.0	Apache Software Foundation Apache HTTP Server 2.3.1
Apache Software Foundation Apache HTTP Server 2.3.2	Apache Software Foundation Apache HTTP Server 2.3.3	Apache Software Foundation Apache HTTP Server 2.3.4
Apache Software Foundation Apache HTTP Server 2.3.5	Apache Software Foundation Apache HTTP Server 2.3.6	Apache Software Foundation Apache HTTP Server 2.3.7
Apache Software Foundation Apache HTTP Server 2.3.8	Apache Software Foundation Apache HTTP Server 2.3.9	Apache Software Foundation Apache HTTP Server 2.3.10
Apache Software Foundation Apache HTTP Server 2.3.11	Apache Software Foundation Apache HTTP Server 2.3.12	Apache Software Foundation Apache HTTP Server 2.3.13
Apache Software Foundation Apache HTTP Server 2.3.14	Apache Software Foundation Apache HTTP Server 2.3.15	Apache Software Foundation Apache HTTP Server 2.3.16

Apache Software Foundation Apache HTTP Server 2.4.0
Apache Software Foundation Apache HTTP Server 2.4.1
Apache Software Foundation Apache HTTP Server 2.4.2
Apache Software Foundation Apache HTTP Server 2.4.3
Apache Software Foundation Apache HTTP Server 2.4.4
Apache Software Foundation Apache HTTP Server 2.4.6
Apache Software Foundation Apache HTTP Server 2.4.7

References

http://advisories.mageia.org/MGASA-2014-0135.html
http://archives.neohapsis.com/archives/bugtraq/2014-10/0101.html
http://kb.juniper.net/InfoCenter/index?page=content&id=JSA10698
http://lists.apple.com/archives/security-announce/2015/Apr/msg00001.html
http://marc.info/?l=bugtraq&m=141017844705317&w=2
http://marc.info/?l=bugtraq&m=141390017113542&w=2
http://seclists.org/fulldisclosure/2014/Dec/23
http://security.gentoo.org/glsa/glsa-201408-12.xml
http://svn.apache.org/repos/asf/httpd/httpd/branches/2.2.x/CHANGES
http://svn.apache.org/viewvc/httpd/httpd/trunk/modules/dav/main/util.c
http://svn.apache.org/viewvc/httpd/httpd/trunk/modules/dav/main/util.c?r1=1528718&r2=1556428&diff_
http://www-01.ibm.com/support/docview.wss?uid=swg21669554
http://www-01.ibm.com/support/docview.wss?uid=swg21676091
http://www-01.ibm.com/support/docview.wss?uid=swg21676092
http://www.apache.org/dist/httpd/CHANGES_2.4.9
http://www.oracle.com/technetwork/topics/security/cpujan2015-1972971.html
http://www.oracle.com/technetwork/topics/security/cpujul2014-1972956.html
http://www.securityfocus.com/archive/1/534161/100/0/threaded
http://www.securityfocus.com/bid/66303
http://www.ubuntu.com/usn/USN-2152-1
http://www.vmware.com/security/advisories/VMSA-2014-0012.html
https://blogs.oracle.com/sunsecurity/entry/multiple_input_validation_vulnerabilities_in1
https://httpd.apache.org/security/vulnerabilities_24.html
https://puppet.com/security/cve/cve-2013-6438
https://support.apple.com/HT204659
https://support.apple.com/kb/HT6535

Summary

The mod_proxy module in the Apache HTTP Server 1.3.x through 1.3.42, 2.0.x through 2.0.64, and 2.2.x through 2.2.21 does not properly interact with use of (1) RewriteRule and (2) ProxyPassMatch pattern matches for configuration of a reverse proxy, which allows remote attackers to send requests to intranet servers via a malformed URI containing an initial @ (at sign) character.

CVE-2011-3368 Information	
CVSS Score	5.0
CWE	CWE-20
Vulnerability impact	
Confidentiality	PARTIAL
Integrity	NONE
Availability	NONE
Access methodology information	
Vector	NETWORK
Complexity	LOW
Authentication	NONE

Vulnerable configs

Apache Software Foundation Apache HTTP Server 1.3		Apache Software Foundation Apache HTTP Server 1.3.0
Apache Software Foundation Apache HTTP Server 1.3.1	Apache Software Foundation Apache HTTP Server 1.3.1.1	Apache Software Foundation Apache HTTP Server 1.3.2
Apache Software Foundation Apache HTTP Server 1.3.3	Apache Software Foundation Apache HTTP Server 1.3.4	Apache Software Foundation Apache HTTP Server 1.3.5
Apache Software Foundation Apache HTTP Server 1.3.6	Apache Software Foundation Apache HTTP Server 1.3.7	Apache Software Foundation Apache HTTP Server 1.3.8
Apache Software Foundation Apache HTTP Server 1.3.9	Apache Software Foundation Apache 1.3.10	Apache Software Foundation Apache HTTP Server 1.3.11
Apache Software Foundation Apache HTTP Server 1.3.12	Apache Software Foundation Apache 1.3.13	Apache Software Foundation Apache HTTP Server 1.3.14
Apache Software Foundation Apache 1.3.15	Apache Software Foundation Apache 1.3.16	Apache Software Foundation Apache HTTP Server 1.3.17
Apache Software Foundation Apache HTTP Server 1.3.18	Apache Software Foundation Apache HTTP Server 1.3.19	Apache Software Foundation Apache HTTP Server 1.3.20
Apache Software Foundation Apache HTTP Server 1.3.22	Apache Software Foundation Apache HTTP Server 1.3.23	Apache Software Foundation Apache HTTP Server 1.3.24
Apache Software Foundation Apache HTTP Server 1.3.25	Apache Software Foundation Apache HTTP Server 1.3.26	Apache Software Foundation Apache HTTP Server 1.3.27
Apache Software Foundation Apache HTTP Server 1.3.28	Apache Software Foundation Apache HTTP Server 1.3.29	Apache Software Foundation Apache HTTP Server 1.3.30
Apache Software Foundation Apache HTTP Server 1.3.31	Apache Software Foundation Apache HTTP Server 1.3.32	Apache Software Foundation Apache HTTP Server 1.3.33
Apache Software Foundation Apache HTTP Server 1.3.34	Apache Software Foundation Apache HTTP Server 1.3.35	Apache Software Foundation Apache HTTP Server 1.3.36
Apache Software Foundation Apache HTTP Server 1.3.37	Apache Software Foundation Apache HTTP Server 1.3.38	Apache Software Foundation Apache HTTP Server 1.3.39
Apache Software Foundation Apache HTTP Server 1.3.41	Apache Software Foundation Apache HTTP Server 1.3.42	Apache Software Foundation Apache HTTP Server 1.3.65
Apache Software Foundation Apache HTTP Server 1.3.68	Apache Software Foundation Apache HTTP Server 2.0	Apache Software Foundation Apache HTTP Server 2.0.9a
Apache Software Foundation Apache HTTP Server 2.0.28	Apache Software Foundation Apache HTTP Server 2.0.28 Beta	Apache Software Foundation Apache HTTP Server 2.0.32
Apache Software Foundation Apache HTTP Server 2.0.32 Beta	Apache Software Foundation Apache HTTP Server 2.0.34 Beta	Apache Software Foundation Apache HTTP Server 2.0.35
Apache Software Foundation Apache HTTP Server 2.0.36	Apache Software Foundation Apache HTTP Server 2.0.37	Apache Software Foundation Apache HTTP Server 2.0.38
Apache Software Foundation Apache HTTP Server 2.0.39	Apache Software Foundation Apache HTTP Server 2.0.40	Apache Software Foundation Apache HTTP Server 2.0.41
Apache Software Foundation Apache HTTP Server 2.0.42	Apache Software Foundation Apache HTTP Server 2.0.43	Apache Software Foundation Apache HTTP Server 2.0.44
Apache Software Foundation Apache HTTP Server 2.0.45	Apache Software Foundation Apache HTTP Server 2.0.46	Apache Software Foundation Apache HTTP Server 2.0.47
Apache Software Foundation Apache HTTP Server 2.0.48	Apache Software Foundation Apache HTTP Server 2.0.49	Apache Software Foundation Apache HTTP Server 2.0.50
Apache Software Foundation Apache HTTP Server 2.0.51	Apache Software Foundation Apache HTTP Server 2.0.52	Apache Software Foundation Apache HTTP Server 2.0.53
Apache Software Foundation Apache HTTP Server 2.0.54	Apache Software Foundation Apache HTTP Server 2.0.55	Apache Software Foundation Apache HTTP Server 2.0.56
Apache Software Foundation Apache HTTP Server 2.0.57	Apache Software Foundation Apache HTTP Server 2.0.58	Apache Software Foundation HTTP Server 2.0.59
Apache Software Foundation Apache HTTP Server 2.0.60 dev	Apache Software Foundation HTTP Server 2.0.61	Apache Software Foundation Apache HTTP Server 2.0.63

Apache Software Foundation Apache HTTP Server 2.0.64
Apache Software Foundation Apache HTTP Server 2.2.0
Apache Software Foundation Apache HTTP Server 2.2.1
Apache Software Foundation Apache HTTP Server 2.2.2
Apache Software Foundation Apache HTTP Server 2.2.3
Apache Software Foundation Apache HTTP Server 2.2.4
Apache Software Foundation Apache HTTP Server 2.2.6
Apache Software Foundation Apache HTTP Server 2.2.8
Apache Software Foundation Apache HTTP Server 2.2.9
Apache Software Foundation Apache HTTP Server 2.2.10
Apache Software Foundation Apache HTTP Server 2.2.11
Apache Software Foundation Apache HTTP Server 2.2.12
Apache Software Foundation Apache HTTP Server 2.2.13
Apache Software Foundation Apache HTTP Server 2.2.14
Apache Software Foundation Apache HTTP Server 2.2.15
Apache Software Foundation Apache HTTP Server 2.2.16
Apache Software Foundation Apache HTTP Server 2.2.18
Apache Software Foundation Apache HTTP Server 2.2.19
Apache Software Foundation Apache HTTP Server 2.2.20
Apache HTTP Server 2.2.21

References

http://kb.juniper.net/JSA10585
http://lists.apple.com/archives/security-announce/2012/Sep/msg00004.html
http://lists.opensuse.org/opensuse-security-announce/2011-11/msg00011.html
http://lists.opensuse.org/opensuse-updates/2013-02/msg00009.html
http://lists.opensuse.org/opensuse-updates/2013-02/msg00012.html
http://marc.info/?l=bugtraq&m=133294460209056&w=2
http://marc.info/?l=bugtraq&m=134987041210674&w=2
http://rhn.redhat.com/errata/RHSA-2012-0542.html
http://rhn.redhat.com/errata/RHSA-2012-0543.html
http://seclists.org/fulldisclosure/2011/Oct/232
http://seclists.org/fulldisclosure/2011/Oct/273
http://support.apple.com/kb/HT5501
http://svn.apache.org/viewvc?view=revision&revision=1179239
http://web.archiveorange.com/archive/v/ZyS0hzECD5zzb2NkvQlt
http://www-01.ibm.com/support/docview.wss?uid=nas2064c7e5f53452ff6862579270003c8d42
http://www-01.ibm.com/support/docview.wss?uid=nas2b7c57b1f1035675186257927003c8d48
http://www.contextis.com/research/blog/reverseproxybypass/
http://www.debian.org/security/2012/dsa-2405
http://www.exploit-db.com/exploits/17969
http://www.mandriva.com/security/advisories?name=MDVSA-2011:144
http://www.mandriva.com/security/advisories?name=MDVSA-2013:150
http://www.oracle.com/technetwork/topics/security/cpujan2015-1972971.html
http://www.oracle.com/technetwork/topics/security/cpujul2012-392727.html
http://www.redhat.com/support/errata/RHSA-2011-1391.html
http://www.redhat.com/support/errata/RHSA-2011-1392.html
http://www.securityfocus.com/bid/49957
http://www.securitytracker.com/id?1026144
https://bugzilla.redhat.com/show_bug.cgi?id=740045
https://exchange.xforce.ibmcloud.com/vulnerabilities/70336

Summary

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.

CVE-2008-2364 Information	
CVSS Score	5.0
CWE	CWE-399
Vulnerability impact	
Confidentiality	NONE
Integrity	NONE
Availability	PARTIAL
Access methodology information	
Vector	NETWORK
Complexity	LOW
Authentication	NONE

Vulnerable configs

Apache Software Foundation Apache HTTP Server 2.0.63
Apache Software Foundation Apache HTTP Server 2.2.8

References

http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=c01539432
http://lists.apple.com/archives/security-announce/2008/Oct/msg00001.html
http://lists.opensuse.org/opensuse-security-announce/2009-03/msg00001.html
http://lists.opensuse.org/opensuse-security-announce/2009-03/msg00004.html
http://marc.info/?l=bugtraq&m=123376588623823&w=2
http://marc.info/?l=bugtraq&m=125631037611762&w=2
http://rhn.redhat.com/errata/RHSA-2008-0967.html
http://security.gentoo.org/glsa/glsa-200807-06.xml

http://sunsolve.sun.com/search/document.do?assetkey=1-26-247666-1
http://support.apple.com/kb/HT3216
http://svn.apache.org/viewvc/httpd/httpd/trunk/modules/proxy/mod_proxy_http.c?r1=666154&r2=66615
http://wiki.rpath.com/wiki/Advisories:rPSA-2008-0328
http://www-01.ibm.com/support/docview.wss?uid=swg27008517
http://www-1.ibm.com/support/docview.wss?uid=swg1PK67579
http://www.mandriva.com/security/advisories?name=MDVSA-2008:195
http://www.mandriva.com/security/advisories?name=MDVSA-2008:237
http://www.oracle.com/technetwork/topics/security/cpujuly2013-1899826.html
http://www.redhat.com/support/errata/RHSA-2008-0966.html
http://www.securityfocus.com/archive/1/494858/100/0/threaded
http://www.securityfocus.com/archive/1/498567/100/0/threaded
http://www.securityfocus.com/bid/29653
http://www.securityfocus.com/bid/31681
http://www.securitytracker.com/id?1020267
http://www.ubuntu.com/usn/USN-731-1
http://www.vupen.com/english/advisories/2008/1798
http://www.vupen.com/english/advisories/2008/2780
http://www.vupen.com/english/advisories/2009/0320
https://exchange.xforce.ibmcloud.com/vulnerabilities/42987
https://www.redhat.com/archives/fedora-package-announce/2008-August/msg00055.html
https://www.redhat.com/archives/fedora-package-announce/2008-August/msg00153.html

Summary

The log_cookie function in mod_log_config.c in the mod_log_config module in the Apache HTTP Server before 2.4.8 allows remote attackers to cause a denial of service (segmentation fault and daemon crash) via a crafted cookie that is not properly handled during truncation.

CVE-2014-0098 Information	
CVSS Score	5.0
CWE	CWE-20
Vulnerability impact	
Confidentiality	NONE
Integrity	NONE
Availability	PARTIAL
Access methodology information	
Vector	NETWORK
Complexity	LOW
Authentication	NONE

Vulnerable configs

Apache Software Foundation Apache HTTP Server 2.0		Apache Software Foundation Apache HTTP Server 2.0.9a
Apache Software Foundation Apache HTTP Server 2.0.28	Apache Software Foundation Apache HTTP Server 2.0.28 Beta	Apache Software Foundation Apache HTTP Server 2.0.32
Apache Software Foundation Apache HTTP Server 2.0.32 Beta	Apache Software Foundation Apache HTTP Server 2.0.34 Beta	Apache Software Foundation Apache HTTP Server 2.0.35
Apache Software Foundation Apache HTTP Server 2.0.36	Apache Software Foundation Apache HTTP Server 2.0.37	Apache Software Foundation Apache HTTP Server 2.0.38
Apache Software Foundation Apache HTTP Server 2.0.39	Apache Software Foundation Apache HTTP Server 2.0.40	Apache Software Foundation Apache HTTP Server 2.0.41
Apache Software Foundation Apache HTTP Server 2.0.42	Apache Software Foundation Apache HTTP Server 2.0.43	Apache Software Foundation Apache HTTP Server 2.0.44
Apache Software Foundation Apache HTTP Server 2.0.45	Apache Software Foundation Apache HTTP Server 2.0.46	Apache Software Foundation Apache HTTP Server 2.0.47
Apache Software Foundation Apache HTTP Server 2.0.48	Apache Software Foundation Apache HTTP Server 2.0.49	Apache Software Foundation Apache HTTP Server 2.0.50
Apache Software Foundation Apache HTTP Server 2.0.51	Apache Software Foundation Apache HTTP Server 2.0.52	Apache Software Foundation Apache HTTP Server 2.0.53
Apache Software Foundation Apache HTTP Server 2.0.54	Apache Software Foundation Apache HTTP Server 2.0.55	Apache Software Foundation Apache HTTP Server 2.0.56
Apache Software Foundation Apache HTTP Server 2.0.57	Apache Software Foundation Apache HTTP Server 2.0.58	Apache Software Foundation HTTP Server 2.0.59
Apache Software Foundation Apache HTTP Server 2.0.60 dev	Apache Software Foundation HTTP Server 2.0.61	Apache Software Foundation Apache HTTP Server 2.0.63
Apache Software Foundation Apache HTTP Server 2.0.64	Apache Software Foundation Apache HTTP Server 2.1	Apache Software Foundation Apache HTTP Server 2.1.1
Apache Software Foundation Apache HTTP Server 2.1.2	Apache Software Foundation Apache HTTP Server 2.1.3	Apache Software Foundation Apache HTTP Server 2.1.4
Apache Software Foundation Apache HTTP Server 2.1.5	Apache Software Foundation Apache HTTP Server 2.1.6	Apache Software Foundation Apache HTTP Server 2.1.7
Apache Software Foundation Apache HTTP Server 2.1.8	Apache Software Foundation Apache HTTP Server 2.1.9	Apache Software Foundation Apache HTTP Server 2.2
Apache Software Foundation Apache HTTP Server 2.2.0	Apache Software Foundation Apache HTTP Server 2.2.1	Apache Software Foundation Apache HTTP Server 2.2.2
Apache Software Foundation Apache HTTP Server 2.2.3	Apache Software Foundation Apache HTTP Server 2.2.4	Apache Software Foundation Apache HTTP Server 2.2.6
Apache Software Foundation Apache HTTP Server 2.2.8	Apache Software Foundation Apache HTTP Server 2.2.9	Apache Software Foundation Apache HTTP Server 2.2.10
Apache Software Foundation Apache HTTP Server 2.2.11	Apache Software Foundation Apache HTTP Server 2.2.12	Apache Software Foundation Apache HTTP Server 2.2.13
Apache Software Foundation Apache HTTP Server 2.2.14	Apache Software Foundation Apache HTTP Server 2.2.15	Apache Software Foundation Apache HTTP Server 2.2.16
Apache Software Foundation Apache HTTP Server 2.2.17	Apache Software Foundation Apache HTTP Server 2.2.18	Apache Software Foundation Apache HTTP Server 2.2.19
Apache Software Foundation Apache HTTP Server 2.2.20	Apache HTTP Server 2.2.21	Apache Software Foundation Apache HTTP Server 2.2.22
Apache Software Foundation Apache HTTP Server 2.2.23	Apache Software Foundation Apache HTTP Server 2.2.24	Apache Software Foundation Apache HTTP Server 2.2.25
Apache Software Foundation Apache HTTP Server 2.3.0	Apache Software Foundation Apache HTTP Server 2.3.1	Apache Software Foundation Apache HTTP Server 2.3.2
Apache Software Foundation Apache HTTP Server 2.3.3	Apache Software Foundation Apache HTTP Server 2.3.4	Apache Software Foundation Apache HTTP Server 2.3.5
Apache Software Foundation Apache HTTP Server 2.3.6	Apache Software Foundation Apache HTTP Server 2.3.7	Apache Software Foundation Apache HTTP Server 2.3.8
Apache Software Foundation Apache HTTP Server 2.3.9	Apache Software Foundation Apache HTTP Server 2.3.10	Apache Software Foundation Apache HTTP Server 2.3.11
Apache Software Foundation Apache HTTP Server 2.3.12	Apache Software Foundation Apache HTTP Server 2.3.13	Apache Software Foundation Apache HTTP Server 2.3.14
Apache Software Foundation Apache HTTP Server 2.3.15	Apache Software Foundation Apache HTTP Server 2.3.16	Apache Software Foundation Apache HTTP Server 2.4.0
Apache Software Foundation Apache HTTP Server 2.4.1	Apache Software Foundation Apache HTTP Server 2.4.2	Apache Software Foundation Apache HTTP Server 2.4.3
Apache Software Foundation Apache HTTP Server 2.4.4	Apache Software Foundation Apache HTTP Server 2.4.6	Apache Software Foundation Apache HTTP Server 2.4.7

References

http://advisories.mageia.org/MGASA-2014-0135.html
http://archives.neohapsis.com/archives/bugtraq/2014-10/0101.html
http://kb.juniper.net/InfoCenter/index?page=content&id=JSA10698
http://lists.apple.com/archives/security-announce/2015/Apr/msg00001.html
http://marc.info/?l=bugtraq&m=141017844705317&w=2
http://marc.info/?l=bugtraq&m=141390017113542&w=2
http://seclists.org/fulldisclosure/2014/Dec/23
http://secunia.com/advisories/59219
http://security.gentoo.org/glsa/glsa-201408-12.xml
http://support.f5.com/kb/en-us/solutions/public/15000/300/sol15320.html
http://svn.apache.org/repos/asf/httpd/httpd/branches/2.2.x/CHANGES
http://svn.apache.org/viewvc/httpd/httpd/trunk/modules/loggers/mod_log_config.c
http://svn.apache.org/viewvc/httpd/httpd/trunk/modules/loggers/mod_log_config.c?r1=1575394&r2=1575
http://www-01.ibm.com/support/docview.wss?uid=swg21668973
http://www-01.ibm.com/support/docview.wss?uid=swg21676091
http://www-01.ibm.com/support/docview.wss?uid=swg21676092
http://www.apache.org/dist/httpd/CHANGES_2.4.9
http://www.oracle.com/technetwork/topics/security/cpujan2015-1972971.html
http://www.oracle.com/technetwork/topics/security/cpujul2014-1972956.html
http://www.securityfocus.com/archive/1/534161/100/0/threaded
http://www.securityfocus.com/bid/66303
http://www.ubuntu.com/usn/USN-2152-1
http://www.vmware.com/security/advisories/VMSA-2014-0012.html
https://blogs.oracle.com/sunsecurity/entry/multiple_input_validation_vulnerabilities_in1
https://httpd.apache.org/security/vulnerabilities_24.html
https://puppet.com/security/cve/cve-2014-0098
https://support.apple.com/HT204659
https://support.apple.com/kb/HT6535

Summary

The Apache HTTP Server 1.x and 2.x allows remote attackers to cause a denial of service (daemon outage) via partial HTTP requests, as demonstrated by Slowloris, related to the lack of the mod_reqtimeout module in versions before 2.2.15.

CVE-2007-6750 Information	
CVSS Score	5.0
CWE	CWE-399
Vulnerability impact	
Confidentiality	NONE
Integrity	NONE
Availability	PARTIAL
Access methodology information	
Vector	NETWORK
Complexity	LOW
Authentication	NONE

Vulnerable configs

Apache Software Foundation Apache HTTP Server 1.0	Apache Software Foundation Apache HTTP Server 1.0.2	Apache Software Foundation Apache HTTP Server 1.0.3
Apache Software Foundation Apache HTTP Server 1.0.5	Apache Software Foundation Apache HTTP Server 1.1	Apache Software Foundation Apache HTTP Server 1.1.1
Apache Software Foundation Apache 1.2	Apache Software Foundation Apache HTTP Server 1.2.4	Apache Software Foundation Apache HTTP Server 1.2.5
Apache Software Foundation Apache HTTP Server 1.2.6	Apache Software Foundation Apache 1.29	Apache Software Foundation Apache HTTP Server 1.3
Apache Software Foundation Apache HTTP Server 1.3.0	Apache Software Foundation Apache HTTP Server 1.3.1	Apache Software Foundation Apache HTTP Server 1.3.1.1
Apache Software Foundation Apache HTTP Server 1.3.2	Apache Software Foundation Apache HTTP Server 1.3.3	Apache Software Foundation Apache HTTP Server 1.3.4
Apache Software Foundation Apache HTTP Server 1.3.5	Apache Software Foundation Apache HTTP Server 1.3.6	Apache Software Foundation Apache HTTP Server 1.3.7
Apache Software Foundation Apache HTTP Server 1.3.8	Apache Software Foundation Apache HTTP Server 1.3.9	Apache Software Foundation Apache 1.3.10
Apache Software Foundation Apache HTTP Server 1.3.11	Apache Software Foundation Apache HTTP Server 1.3.12	Apache Software Foundation Apache 1.3.13
Apache Software Foundation Apache HTTP Server 1.3.14	Apache Software Foundation Apache 1.3.15	Apache Software Foundation Apache 1.3.16
Apache Software Foundation Apache HTTP Server 1.3.17	Apache Software Foundation Apache HTTP Server 1.3.18	Apache Software Foundation Apache HTTP Server 1.3.19
Apache Software Foundation Apache HTTP Server 1.3.20	Apache Software Foundation Apache HTTP Server 1.3.22	Apache Software Foundation Apache HTTP Server 1.3.23
Apache Software Foundation Apache HTTP Server 1.3.24	Apache Software Foundation Apache HTTP Server 1.3.25	Apache Software Foundation Apache HTTP Server 1.3.26
Apache Software Foundation Apache HTTP Server 1.3.27	Apache Software Foundation Apache HTTP Server 1.3.28	Apache Software Foundation Apache HTTP Server 1.3.29
Apache Software Foundation Apache HTTP Server 1.3.30	Apache Software Foundation Apache HTTP Server 1.3.31	Apache Software Foundation Apache HTTP Server 1.3.32
Apache Software Foundation Apache HTTP Server 1.3.33	Apache Software Foundation Apache HTTP Server 1.3.34	Apache Software Foundation Apache HTTP Server 1.3.35
Apache Software Foundation Apache HTTP Server 1.3.36	Apache Software Foundation Apache HTTP Server 1.3.37	Apache Software Foundation Apache HTTP Server 1.3.38
Apache Software Foundation Apache HTTP Server 1.3.39	Apache Software Foundation Apache HTTP Server 1.3.41	Apache Software Foundation Apache HTTP Server 1.3.42
Apache Software Foundation Apache HTTP Server 1.3.65	Apache Software Foundation Apache HTTP Server 1.3.68	Apache Software Foundation Apache HTTP Server 1.4.0
Apache Software Foundation Apache HTTP Server 1.99	Apache Software Foundation Apache HTTP Server 2.0	Apache Software Foundation Apache HTTP Server 2.0.9a
Apache Software Foundation Apache HTTP Server 2.0.28	Apache Software Foundation Apache HTTP Server 2.0.28 Beta	Apache Software Foundation Apache HTTP Server 2.0.32
Apache Software Foundation Apache HTTP Server 2.0.32 Beta	Apache Software Foundation Apache HTTP Server 2.0.34 Beta	Apache Software Foundation Apache HTTP Server 2.0.35
Apache Software Foundation Apache HTTP Server 2.0.36	Apache Software Foundation Apache HTTP Server 2.0.37	Apache Software Foundation Apache HTTP Server 2.0.38
Apache Software Foundation Apache HTTP Server 2.0.39	Apache Software Foundation Apache HTTP Server 2.0.40	Apache Software Foundation Apache HTTP Server 2.0.41
Apache Software Foundation Apache HTTP Server 2.0.42	Apache Software Foundation Apache HTTP Server 2.0.43	Apache Software Foundation Apache HTTP Server 2.0.44
Apache Software Foundation Apache HTTP Server 2.0.45	Apache Software Foundation Apache HTTP Server 2.0.46	Apache Software Foundation Apache HTTP Server 2.0.47
Apache Software Foundation Apache HTTP Server 2.0.48	Apache Software Foundation Apache HTTP Server 2.0.49	Apache Software Foundation Apache HTTP Server 2.0.50
Apache Software Foundation Apache HTTP Server 2.0.51	Apache Software Foundation Apache HTTP Server 2.0.52	Apache Software Foundation Apache HTTP Server 2.0.53
Apache Software Foundation Apache HTTP Server 2.0.54	Apache Software Foundation Apache HTTP Server 2.0.55	Apache Software Foundation Apache HTTP Server 2.0.56
Apache Software Foundation Apache HTTP Server 2.0.57	Apache Software Foundation Apache HTTP Server 2.0.58	Apache Software Foundation HTTP Server 2.0.59
Apache Software Foundation Apache HTTP Server 2.0.60 dev	Apache Software Foundation HTTP Server 2.0.61	Apache Software Foundation Apache HTTP Server 2.0.63
Apache Software Foundation Apache HTTP Server 2.1	Apache Software Foundation Apache HTTP Server 2.1.1	Apache Software Foundation Apache HTTP Server 2.1.2

Apache Software Foundation Apache HTTP Server 2.1.3	Apache Software Foundation Apache HTTP Server 2.1.4	Apache Software Foundation Apache HTTP Server 2.1.5
Apache Software Foundation Apache HTTP Server 2.1.6	Apache Software Foundation Apache HTTP Server 2.1.7	Apache Software Foundation Apache HTTP Server 2.1.8
Apache Software Foundation Apache HTTP Server 2.1.9	Apache Software Foundation Apache HTTP Server 2.2	Apache Software Foundation Apache HTTP Server 2.2.0
Apache Software Foundation Apache HTTP Server 2.2.1	Apache Software Foundation Apache HTTP Server 2.2.2	Apache Software Foundation Apache HTTP Server 2.2.3
Apache Software Foundation Apache HTTP Server 2.2.4	Apache Software Foundation Apache HTTP Server 2.2.6	Apache Software Foundation Apache HTTP Server 2.2.8
Apache Software Foundation Apache HTTP Server 2.2.9	Apache Software Foundation Apache HTTP Server 2.2.10	Apache Software Foundation Apache HTTP Server 2.2.11
Apache Software Foundation Apache HTTP Server 2.2.12	Apache Software Foundation Apache HTTP Server 2.2.13	Apache Software Foundation Apache HTTP Server 2.2.14

References

http://archives.neohapsis.com/archives/bugtraq/2007-01/0229.html

http://ha.ckers.org/slowloris/

http://lists.opensuse.org/opensuse-security-announce/2012-02/msg00026.html

http://lists.opensuse.org/opensuse-security-announce/2012-03/msg00002.html

http://marc.info/?l=bugtraq&m=136612293908376&w=2

http://www.securityfocus.com/bid/21865

http://www.securitytracker.com/id/1038144

https://exchange.xforce.ibmcloud.com/vulnerabilities/72345

https://h20566.www2.hpe.com/portal/site/hpsc/public/kb/docDisplay?docId=emr_na-c05111017

https://h20566.www2.hpe.com/portal/site/hpsc/public/kb/docDisplay?docId=emr_na-c05158380

Summary

The (1) mod_cache and (2) mod_dav modules in the Apache HTTP Server 2.2.x before 2.2.16 allow remote attackers to cause a denial of service (process crash) via a request that lacks a path.

CVE-2010-1452 Information	
CVSS Score	5.0
CWE	Unknown
Vulnerability impact	
Confidentiality	NONE
Integrity	NONE
Availability	PARTIAL
Access methodology information	
Vector	NETWORK
Complexity	LOW
Authentication	NONE

Vulnerable configs

Apache Software Foundation Apache HTTP Server	Apache Software Foundation Apache HTTP Server 2.2	Apache Software Foundation Apache HTTP Server 2.2.0
Apache Software Foundation Apache HTTP Server 2.2.1	Apache Software Foundation Apache HTTP Server 2.2.2	Apache Software Foundation Apache HTTP Server 2.2.3
Apache Software Foundation Apache HTTP Server 2.2.4	Apache Software Foundation Apache HTTP Server 2.2.6	cpe:2.3:a:apache:http_server:2.2.7
Apache Software Foundation Apache HTTP Server 2.2.8	Apache Software Foundation Apache HTTP Server 2.2.9	Apache Software Foundation Apache HTTP Server 2.2.10
Apache Software Foundation Apache HTTP Server 2.2.11	Apache Software Foundation Apache HTTP Server 2.2.12	Apache Software Foundation Apache HTTP Server 2.2.13
Apache Software Foundation Apache HTTP Server 2.2.14		Apache Software Foundation Apache HTTP Server 2.2.15

References

http://blogs.sun.com/security/entry/cve_2010_1452_mod_dav
http://httpd.apache.org/security/vulnerabilities_22.html
http://lists.apple.com/archives/security-announce/2011/Mar/msg00006.html
http://lists.opensuse.org/opensuse-security-announce/2011-09/msg00009.html
http://lists.opensuse.org/opensuse-security-announce/2011-11/msg00008.html
http://marc.info/?l=apache-announce&m=128009718610929&w=2
http://marc.info/?l=bugtraq&m=129190899612998&w=2

http://marc.info/?l=bugtraq&m=133355494609819&w=2
http://slackware.com/security/viewer.php?l=slackware-security&y=2010&m=slackware-security.467395
http://support.apple.com/kb/HT4581
http://ubuntu.com/usn/usn-1021-1
http://www.redhat.com/support/errata/RHSA-2010-0659.html
http://www.redhat.com/support/errata/RHSA-2011-0896.html
http://www.redhat.com/support/errata/RHSA-2011-0897.html
http://www.vupen.com/english/advisories/2010/2218
http://www.vupen.com/english/advisories/2010/3064
http://www.vupen.com/english/advisories/2011/0291
https://issues.apache.org/bugzilla/show_bug.cgi?id=49246

Summary

The ap_proxy_ajp_request function in mod_proxy_ajp.c in mod_proxy_ajp in the Apache HTTP Server 2.2.x before 2.2.15 does not properly handle certain situations in which a client sends no request body, which allows remote attackers to cause a denial of service (backend server outage) via a crafted request, related to use of a 500 error code instead of the appropriate 400 error code.

CVE-2010-0408 Information	
CVSS Score	5.0
CWE	Unknown
Vulnerability impact	
Confidentiality	NONE
Integrity	NONE
Availability	PARTIAL
Access methodology information	
Vector	NETWORK
Complexity	LOW
Authentication	NONE

Vulnerable configs

Apache Software Foundation Apache HTTP Server
Apache Software Foundation Apache HTTP Server 2.2
Apache Software Foundation Apache HTTP Server 2.2.0
Apache Software Foundation Apache HTTP Server 2.2.2
Apache Software Foundation Apache HTTP Server 2.2.3
Apache Software Foundation Apache HTTP Server 2.2.4
Apache Software Foundation Apache HTTP Server 2.2.6
Apache Software Foundation Apache HTTP Server 2.2.8
Apache Software Foundation Apache HTTP Server 2.2.9
Apache Software Foundation Apache HTTP Server 2.2.11
Apache Software Foundation Apache HTTP Server 2.2.12
Apache Software Foundation Apache HTTP Server 2.2.13
Apache Software Foundation Apache HTTP Server 2.2.14

References

http://httpd.apache.org/security/vulnerabilities_22.html
http://lists.apple.com/archives/security-announce/2010//Nov/msg00000.html
http://lists.fedoraproject.org/pipermail/package-announce/2010-April/039957.html
http://lists.fedoraproject.org/pipermail/package-announce/2010-May/040652.html
http://lists.opensuse.org/opensuse-security-announce/2010-04/msg00006.html

http://marc.info/?l=bugtraq&m=127557640302499&w=2
http://support.apple.com/kb/HT4435
http://svn.apache.org/viewvc/httpd/httpd/branches/2.2.x/modules/proxy/mod_proxy_ajp.c?r1=917876&r2
http://svn.apache.org/viewvc?view=revision&revision=917876
http://www-01.ibm.com/support/docview.wss?uid=swg1PM08939
http://www-01.ibm.com/support/docview.wss?uid=swg1PM12247
http://www-01.ibm.com/support/docview.wss?uid=swg1PM15829
http://www.debian.org/security/2010/dsa-2035
http://www.mandriva.com/security/advisories?name=MDVSA-2010:053
http://www.mandriva.com/security/advisories?name=MDVSA-2013:150
http://www.oracle.com/technetwork/topics/security/cpuapr2013-1899555.html
http://www.redhat.com/support/errata/RHSA-2010-0168.html
http://www.securityfocus.com/bid/38491
http://www.vupen.com/english/advisories/2010/0911
http://www.vupen.com/english/advisories/2010/0994
http://www.vupen.com/english/advisories/2010/1001
http://www.vupen.com/english/advisories/2010/1057
http://www.vupen.com/english/advisories/2010/1411
https://bugzilla.redhat.com/show_bug.cgi?id=569905

Summary

The Solaris pollset feature in the Event Port backend in poll/unix/port.c in the Apache Portable Runtime (APR) library before 1.3.9, as used in the Apache HTTP Server before 2.2.14 and other products, does not properly handle errors, which allows remote attackers to cause a denial of service (daemon hang) via unspecified HTTP requests, related to the prefork and event MPMs.

CVE-2009-2699 Information	
CVSS Score	5.0
CWE	Unknown
Vulnerability impact	
Confidentiality	NONE
Integrity	NONE
Availability	PARTIAL
Access methodology information	
Vector	NETWORK
Complexity	LOW
Authentication	NONE

Vulnerable configs

Apache Software Foundation Apache HTTP Server	Apache Software Foundation Apache HTTP Server 0.8.11	Apache Software Foundation Apache HTTP Server 0.8.14
Apache Software Foundation Apache HTTP Server 1.0.2	Apache Software Foundation Apache HTTP Server 1.0.3	Apache Software Foundation Apache HTTP Server 1.0.5
Apache Software Foundation Apache HTTP Server 1.1	Apache Software Foundation Apache HTTP Server 1.1.1	Apache Software Foundation Apache 1.2
Apache Software Foundation Apache HTTP Server 1.2.4	Apache Software Foundation Apache HTTP Server 1.2.5	Apache Software Foundation Apache HTTP Server 1.2.6
Apache Software Foundation Apache 1.29	Apache Software Foundation Apache HTTP Server 1.3	Apache Software Foundation Apache HTTP Server 1.3.0
Apache Software Foundation Apache HTTP Server 1.3.1	Apache Software Foundation Apache HTTP Server 1.3.1.1	Apache Software Foundation Apache HTTP Server 1.3.2
Apache Software Foundation Apache HTTP Server 1.3.3	Apache Software Foundation Apache HTTP Server 1.3.4	Apache Software Foundation Apache HTTP Server 1.3.5
Apache Software Foundation Apache HTTP Server 1.3.6	Apache Software Foundation Apache HTTP Server 1.3.7	Apache Software Foundation Apache HTTP Server 1.3.8
Apache Software Foundation Apache HTTP Server 1.3.9	Apache Software Foundation Apache 1.3.10	Apache Software Foundation Apache HTTP Server 1.3.11
Apache Software Foundation Apache HTTP Server 1.3.12	Apache Software Foundation Apache 1.3.13	Apache Software Foundation Apache HTTP Server 1.3.14
Apache Software Foundation Apache 1.3.15	Apache Software Foundation Apache 1.3.16	Apache Software Foundation Apache HTTP Server 1.3.17
Apache Software Foundation Apache HTTP Server 1.3.18	Apache Software Foundation Apache HTTP Server 1.3.19	Apache Software Foundation Apache HTTP Server 1.3.20
Apache Software Foundation Apache HTTP Server 1.3.22	Apache Software Foundation Apache HTTP Server 1.3.23	Apache Software Foundation Apache HTTP Server 1.3.24
Apache Software Foundation Apache HTTP Server 1.3.25	Apache Software Foundation Apache HTTP Server 1.3.26	Apache Software Foundation Apache HTTP Server 1.3.27
Apache Software Foundation Apache HTTP Server 1.3.28	Apache Software Foundation Apache HTTP Server 1.3.29	Apache Software Foundation Apache HTTP Server 1.3.30
Apache Software Foundation Apache HTTP Server 1.3.31	Apache Software Foundation Apache HTTP Server 1.3.32	Apache Software Foundation Apache HTTP Server 1.3.33
Apache Software Foundation Apache HTTP Server 1.3.34	Apache Software Foundation Apache HTTP Server 1.3.35	Apache Software Foundation Apache HTTP Server 1.3.36
Apache Software Foundation Apache HTTP Server 1.3.37	Apache Software Foundation Apache HTTP Server 1.3.38	Apache Software Foundation Apache HTTP Server 1.3.39
Apache Software Foundation Apache HTTP Server 1.3.65	Apache Software Foundation Apache HTTP Server 1.3.68	Apache Software Foundation Apache HTTP Server 1.4.0
Apache Software Foundation Apache HTTP Server 1.99	Apache Software Foundation Apache HTTP Server 2.0	Apache Software Foundation Apache HTTP Server 2.0.9a
Apache Software Foundation Apache HTTP Server 2.0.28	Apache Software Foundation Apache HTTP Server 2.0.32	Apache Software Foundation Apache HTTP Server 2.0.32 Beta
Apache Software Foundation Apache HTTP Server 2.0.34 Beta	Apache Software Foundation Apache HTTP Server 2.0.35	Apache Software Foundation Apache HTTP Server 2.0.36
Apache Software Foundation Apache HTTP Server 2.0.37	Apache Software Foundation Apache HTTP Server 2.0.38	Apache Software Foundation Apache HTTP Server 2.0.39
Apache Software Foundation Apache HTTP Server 2.0.40	Apache Software Foundation Apache HTTP Server 2.0.41	Apache Software Foundation Apache HTTP Server 2.0.42
Apache Software Foundation Apache HTTP Server 2.0.43	Apache Software Foundation Apache HTTP Server 2.0.44	Apache Software Foundation Apache HTTP Server 2.0.45
Apache Software Foundation Apache HTTP Server 2.0.46	Apache Software Foundation Apache HTTP Server 2.0.47	Apache Software Foundation Apache HTTP Server 2.0.48
Apache Software Foundation Apache HTTP Server 2.0.49	Apache Software Foundation Apache HTTP Server 2.0.50	Apache Software Foundation Apache HTTP Server 2.0.51

Apache Software Foundation Apache HTTP Server 2.0.52	Apache Software Foundation Apache HTTP Server 2.0.53	Apache Software Foundation Apache HTTP Server 2.0.54
Apache Software Foundation Apache HTTP Server 2.0.55	Apache Software Foundation Apache HTTP Server 2.0.56	Apache Software Foundation Apache HTTP Server 2.0.57
Apache Software Foundation Apache HTTP Server 2.0.58	Apache Software Foundation HTTP Server 2.0.59	Apache Software Foundation Apache HTTP Server 2.0.60 dev
Apache Software Foundation Apache HTTP Server 2.1	Apache Software Foundation Apache HTTP Server 2.1.1	Apache Software Foundation Apache HTTP Server 2.1.2
Apache Software Foundation Apache HTTP Server 2.1.3	Apache Software Foundation Apache HTTP Server 2.1.4	Apache Software Foundation Apache HTTP Server 2.1.5
Apache Software Foundation Apache HTTP Server 2.1.6	Apache Software Foundation Apache HTTP Server 2.1.7	Apache Software Foundation Apache HTTP Server 2.1.8
Apache Software Foundation Apache HTTP Server 2.1.9	Apache Software Foundation Apache HTTP Server 2.2	Apache Software Foundation Apache HTTP Server 2.2.0
Apache Software Foundation Apache HTTP Server 2.2.1	Apache Software Foundation Apache HTTP Server 2.2.2	Apache Software Foundation Apache HTTP Server 2.2.3
Apache Software Foundation Apache HTTP Server 2.2.4	Apache Software Foundation Apache HTTP Server 2.2.6	cpe:2.3:a:apache:http_server:2.2.7
Apache Software Foundation Apache HTTP Server 2.2.8	Apache Software Foundation Apache HTTP Server 2.2.9	Apache Software Foundation Apache HTTP Server 2.2.10
Apache Software Foundation Apache HTTP Server 2.2.11	Apache Software Foundation Apache HTTP Server 2.2.12	Apache Software Foundation Apache HTTP Server 2.2.13
cpe:2.3:a:apache:apr:0.9.7	cpe:2.3:a:apache:apr:0.9.17	cpe:2.3:a:apache:apr:0.9.18
cpe:2.3:a:apache:apr:1.2.1		cpe:2.3:a:apache:apr:1.3.8

References

http://marc.info/?l=bugtraq&m=133355494609819&w=2

http://securitytracker.com/id?1022988

http://www.apache.org/dist/httpd/CHANGES_2.2.14

http://www.mandriva.com/security/advisories?name=MDVSA-2013:150

http://www.oracle.com/technetwork/topics/security/cpuapr2013-1899555.html

http://www.securityfocus.com/bid/36596

https://exchange.xforce.ibmcloud.com/vulnerabilities/53666

https://issues.apache.org/bugzilla/show_bug.cgi?id=47645

Summary

The Apache HTTP Server 2.2.11 and earlier 2.2 versions does not properly handle Options=IncludesNOEXEC in the AllowOverride directive, which allows local users to gain privileges by configuring (1) Options Includes, (2) Options +Includes, or (3) Options +IncludesNOEXEC in a .htaccess file, and then inserting an exec element in a .shtml file.

CVE-2009-1195 Information	
CVSS Score	4.9
CWE	CWE-16
Vulnerability impact	
Confidentiality	NONE
Integrity	NONE
Availability	COMPLETE
Access methodology information	
Vector	LOCAL
Complexity	LOW
Authentication	NONE

Vulnerable configs

Apache Software Foundation Apache HTTP Server
Apache Software Foundation Apache HTTP Server 2.2 Apache Software Foundation Apache HTTP Server 2.2.0 Apache Software Foundation Apache HTTP Server 2.2.1
Apache Software Foundation Apache HTTP Server 2.2.2 cpe:2.3:a:apache:http_server:2.2.2:-:windows Apache Software Foundation Apache HTTP Server 2.2.3
cpe:2.3:a:apache:http_server:2.2.3:-:windows Apache Software Foundation Apache HTTP Server 2.2.4 Apache Software Foundation Apache HTTP Server 2.2.6
cpe:2.3:a:apache:http_server:2.2.7 Apache Software Foundation Apache HTTP Server 2.2.8 Apache Software Foundation Apache HTTP Server 2.2.9
Apache Software Foundation Apache HTTP Server 2.2.10 Apache Software Foundation Apache HTTP Server 2.2.11

References

http://lists.apple.com/archives/security-announce/2009/Nov/msg00000.html
http://lists.opensuse.org/opensuse-security-announce/2009-10/msg00006.html
http://marc.info/?l=apache-httpd-dev&m=124048996106302&w=2
http://marc.info/?l=bugtraq&m=129190899612998&w=2
http://security.gentoo.org/glsa/glsa-200907-04.xml
http://support.apple.com/kb/HT3937

http://svn.apache.org/viewvc?view=rev&revision=772997
http://wiki.rpath.com/Advisories:rPSA-2009-0142
http://www.debian.org/security/2009/dsa-1816
http://www.mandriva.com/security/advisories?name=MDVSA-2009:124
http://www.redhat.com/support/errata/RHSA-2009-1075.html
http://www.redhat.com/support/errata/RHSA-2009-1156.html
http://www.securityfocus.com/archive/1/507852/100/0/threaded
http://www.securityfocus.com/archive/1/507857/100/0/threaded
http://www.securityfocus.com/bid/35115
http://www.securitytracker.com/id?1022296
http://www.ubuntu.com/usn/usn-787-1
http://www.vupen.com/english/advisories/2009/1444
http://www.vupen.com/english/advisories/2009/3184
https://bugzilla.redhat.com/show_bug.cgi?id=489436
https://exchange.xforce.ibmcloud.com/vulnerabilities/50808
https://www.redhat.com/archives/fedora-package-announce/2009-August/msg01363.html

Summary

scoreboard.c in the Apache HTTP Server 2.2.21 and earlier might allow local users to cause a denial of service (daemon crash during shutdown) or possibly have unspecified other impact by modifying a certain type field within a scoreboard shared memory segment, leading to an invalid call to the free function.

CVE-2012-0031 Information	
CVSS Score	4.6
CWE	CWE-399
Vulnerability impact	
Confidentiality	PARTIAL
Integrity	PARTIAL
Availability	PARTIAL
Access methodology information	
Vector	LOCAL
Complexity	LOW
Authentication	NONE

Vulnerable configs

Apache Software Foundation Apache HTTP Server 1.0		
Apache Software Foundation Apache HTTP Server 1.0.2	Apache Software Foundation Apache HTTP Server 1.0.3	Apache Software Foundation Apache HTTP Server 1.0.5
Apache Software Foundation Apache HTTP Server 1.1	Apache Software Foundation Apache HTTP Server 1.1.1	Apache Software Foundation Apache 1.2
Apache Software Foundation Apache HTTP Server 1.2.4	Apache Software Foundation Apache HTTP Server 1.2.5	Apache Software Foundation Apache HTTP Server 1.2.6
Apache Software Foundation Apache 1.29	Apache Software Foundation Apache HTTP Server 1.3	Apache Software Foundation Apache HTTP Server 1.3.0
Apache Software Foundation Apache HTTP Server 1.3.1	Apache Software Foundation Apache HTTP Server 1.3.1.1	Apache Software Foundation Apache HTTP Server 1.3.2
Apache Software Foundation Apache HTTP Server 1.3.3	Apache Software Foundation Apache HTTP Server 1.3.4	Apache Software Foundation Apache HTTP Server 1.3.5
Apache Software Foundation Apache HTTP Server 1.3.6	Apache Software Foundation Apache HTTP Server 1.3.7	Apache Software Foundation Apache HTTP Server 1.3.8
Apache Software Foundation Apache HTTP Server 1.3.9	Apache Software Foundation Apache 1.3.10	Apache Software Foundation Apache HTTP Server 1.3.11
Apache Software Foundation Apache HTTP Server 1.3.12	Apache Software Foundation Apache 1.3.13	Apache Software Foundation Apache HTTP Server 1.3.14
Apache Software Foundation Apache 1.3.15	Apache Software Foundation Apache 1.3.16	Apache Software Foundation Apache HTTP Server 1.3.17
Apache Software Foundation Apache HTTP Server 1.3.18	Apache Software Foundation Apache HTTP Server 1.3.19	Apache Software Foundation Apache HTTP Server 1.3.20
Apache Software Foundation Apache HTTP Server 1.3.22	Apache Software Foundation Apache HTTP Server 1.3.23	Apache Software Foundation Apache HTTP Server 1.3.24
Apache Software Foundation Apache HTTP Server 1.3.25	Apache Software Foundation Apache HTTP Server 1.3.26	Apache Software Foundation Apache HTTP Server 1.3.27
Apache Software Foundation Apache HTTP Server 1.3.28	Apache Software Foundation Apache HTTP Server 1.3.29	Apache Software Foundation Apache HTTP Server 1.3.30
Apache Software Foundation Apache HTTP Server 1.3.31	Apache Software Foundation Apache HTTP Server 1.3.32	Apache Software Foundation Apache HTTP Server 1.3.33
Apache Software Foundation Apache HTTP Server 1.3.34	Apache Software Foundation Apache HTTP Server 1.3.35	Apache Software Foundation Apache HTTP Server 1.3.36
Apache Software Foundation Apache HTTP Server 1.3.37	Apache Software Foundation Apache HTTP Server 1.3.38	Apache Software Foundation Apache HTTP Server 1.3.39
Apache Software Foundation Apache HTTP Server 1.3.41	Apache Software Foundation Apache HTTP Server 1.3.42	Apache Software Foundation Apache HTTP Server 1.3.65
Apache Software Foundation Apache HTTP Server 1.3.68	Apache Software Foundation Apache HTTP Server 1.4.0	Apache Software Foundation Apache HTTP Server 1.99
Apache Software Foundation Apache HTTP Server 2.0	Apache Software Foundation Apache HTTP Server 2.0.9a	Apache Software Foundation Apache HTTP Server 2.0.28
Apache Software Foundation Apache HTTP Server 2.0.28 Beta	Apache Software Foundation Apache HTTP Server 2.0.32	Apache Software Foundation Apache HTTP Server 2.0.32 Beta
Apache Software Foundation Apache HTTP Server 2.0.34 Beta	Apache Software Foundation Apache HTTP Server 2.0.35	Apache Software Foundation Apache HTTP Server 2.0.36
Apache Software Foundation Apache HTTP Server 2.0.37	Apache Software Foundation Apache HTTP Server 2.0.38	Apache Software Foundation Apache HTTP Server 2.0.39
Apache Software Foundation Apache HTTP Server 2.0.40	Apache Software Foundation Apache HTTP Server 2.0.41	Apache Software Foundation Apache HTTP Server 2.0.42
Apache Software Foundation Apache HTTP Server 2.0.43	Apache Software Foundation Apache HTTP Server 2.0.44	Apache Software Foundation Apache HTTP Server 2.0.45
Apache Software Foundation Apache HTTP Server 2.0.46	Apache Software Foundation Apache HTTP Server 2.0.47	Apache Software Foundation Apache HTTP Server 2.0.48
Apache Software Foundation Apache HTTP Server 2.0.49	Apache Software Foundation Apache HTTP Server 2.0.50	Apache Software Foundation Apache HTTP Server 2.0.51
Apache Software Foundation Apache HTTP Server 2.0.52	Apache Software Foundation Apache HTTP Server 2.0.53	Apache Software Foundation Apache HTTP Server 2.0.54
Apache Software Foundation Apache HTTP Server 2.0.55	Apache Software Foundation Apache HTTP Server 2.0.56	Apache Software Foundation Apache HTTP Server 2.0.57

Apache Software Foundation Apache HTTP Server 2.0.58 Apache Software Foundation HTTP Server 2.0.59 Apache Software Foundation Apache HTTP Server 2.0.60 dev
Apache Software Foundation HTTP Server 2.0.61 Apache Software Foundation Apache HTTP Server 2.0.63 Apache Software Foundation Apache HTTP Server 2.1
Apache Software Foundation Apache HTTP Server 2.1.1 Apache Software Foundation Apache HTTP Server 2.1.2 Apache Software Foundation Apache HTTP Server 2.1.3
Apache Software Foundation Apache HTTP Server 2.1.4 Apache Software Foundation Apache HTTP Server 2.1.5 Apache Software Foundation Apache HTTP Server 2.1.6
Apache Software Foundation Apache HTTP Server 2.1.7 Apache Software Foundation Apache HTTP Server 2.1.8 Apache Software Foundation Apache HTTP Server 2.1.9
Apache Software Foundation Apache HTTP Server 2.2 Apache Software Foundation Apache HTTP Server 2.2.0 Apache Software Foundation Apache HTTP Server 2.2.1
Apache Software Foundation Apache HTTP Server 2.2.2 Apache Software Foundation Apache HTTP Server 2.2.3 Apache Software Foundation Apache HTTP Server 2.2.4
Apache Software Foundation Apache HTTP Server 2.2.6 Apache Software Foundation Apache HTTP Server 2.2.8 Apache Software Foundation Apache HTTP Server 2.2.9
Apache Software Foundation Apache HTTP Server 2.2.10 Apache Software Foundation Apache HTTP Server 2.2.11 Apache Software Foundation Apache HTTP Server 2.2.12
Apache Software Foundation Apache HTTP Server 2.2.13 Apache Software Foundation Apache HTTP Server 2.2.14 Apache Software Foundation Apache HTTP Server 2.2.15
Apache Software Foundation Apache HTTP Server 2.2.16 Apache Software Foundation Apache HTTP Server 2.2.17 Apache Software Foundation Apache HTTP Server 2.2.18
Apache Software Foundation Apache HTTP Server 2.2.19 Apache Software Foundation Apache HTTP Server 2.2.20 Apache HTTP Server 2.2.21

References

http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=c03360041
http://lists.apple.com/archives/security-announce/2012/Sep/msg00004.html
http://lists.opensuse.org/opensuse-security-announce/2012-02/msg00026.html
http://lists.opensuse.org/opensuse-security-announce/2012-03/msg00002.html
http://marc.info/?l=bugtraq&m=133294460209056&w=2
http://marc.info/?l=bugtraq&m=133494237717847&w=2
http://marc.info/?l=bugtraq&m=134987041210674&w=2
http://rhn.redhat.com/errata/RHSA-2012-0128.html
http://rhn.redhat.com/errata/RHSA-2012-0542.html
http://rhn.redhat.com/errata/RHSA-2012-0543.html
http://support.apple.com/kb/HT5501
http://svn.apache.org/viewvc?view=revision&revision=1230065
http://www.debian.org/security/2012/dsa-2405
http://www.halfdog.net/Security/2011/ApacheScoreboardInvalidFreeOnShutdown/
http://www.mandriva.com/security/advisories?name=MDVSA-2012:012
http://www.mandriva.com/security/advisories?name=MDVSA-2013:150
http://www.oracle.com/technetwork/topics/security/cpujul2012-392727.html
http://www.securityfocus.com/bid/51407
https://bugzilla.redhat.com/show_bug.cgi?id=773744

Summary

Integer overflow in the ap_pregsub function in server/util.c in the Apache HTTP Server 2.0.x through 2.0.64 and 2.2.x through 2.2.21, when the mod_setenvif module is enabled, allows local users to gain privileges via a .htaccess file with a crafted SetEnvIf directive, in conjunction with a crafted HTTP request header, leading to a heap-based buffer overflow.

CVE-2011-3607 Information	
CVSS Score	4.4
CWE	CWE-189
Vulnerability impact	
Confidentiality	PARTIAL
Integrity	PARTIAL
Availability	PARTIAL
Access methodology information	
Vector	LOCAL
Complexity	MEDIUM
Authentication	NONE

Vulnerable configs

Apache Software Foundation Apache HTTP Server 2.0 Apache Software Foundation Apache HTTP Server 2.0.9a Apache Software Foundation Apache HTTP Server 2.0.28 Apache Software Foundation Apache HTTP Server 2.0.28 Beta Apache Software Foundation Apache HTTP Server 2.0.32 Apache Software Foundation Apache HTTP Server 2.0.32 Beta Apache Software Foundation Apache HTTP Server 2.0.34 Beta Apache Software Foundation Apache HTTP Server 2.0.35 Apache Software Foundation Apache HTTP Server 2.0.36 Apache Software Foundation Apache HTTP Server 2.0.37 Apache Software Foundation Apache HTTP Server 2.0.38 Apache Software Foundation Apache HTTP Server 2.0.39 Apache Software Foundation Apache HTTP Server 2.0.40 Apache Software Foundation Apache HTTP Server 2.0.41 Apache Software Foundation Apache HTTP Server 2.0.42 Apache Software Foundation Apache HTTP Server 2.0.43 Apache Software Foundation Apache HTTP Server 2.0.44 Apache Software Foundation Apache HTTP Server 2.0.45 Apache Software Foundation Apache HTTP Server 2.0.46 Apache Software Foundation Apache HTTP Server 2.0.47 Apache Software Foundation Apache HTTP Server 2.0.48 Apache Software Foundation Apache HTTP Server 2.0.49 Apache Software Foundation Apache HTTP Server 2.0.50 Apache Software Foundation Apache HTTP Server 2.0.51 Apache Software Foundation Apache HTTP Server 2.0.52 Apache Software Foundation Apache HTTP Server 2.0.53 Apache Software Foundation Apache HTTP Server 2.0.54 Apache Software Foundation Apache HTTP Server 2.0.55 Apache Software Foundation Apache HTTP Server 2.0.56 Apache Software Foundation Apache HTTP Server 2.0.57 Apache Software Foundation Apache HTTP Server 2.0.58 Apache Software Foundation HTTP Server 2.0.59 Apache Software Foundation Apache HTTP Server 2.0.60 dev Apache Software Foundation HTTP Server 2.0.61 Apache Software Foundation Apache HTTP Server 2.0.63 Apache Software Foundation Apache HTTP Server 2.0.64 Apache Software Foundation Apache HTTP Server 2.2.0 Apache Software Foundation Apache HTTP Server 2.2.1 Apache Software Foundation Apache HTTP Server 2.2.2 Apache Software Foundation Apache HTTP Server 2.2.3 Apache Software Foundation Apache HTTP Server 2.2.4 Apache Software Foundation Apache HTTP Server 2.2.6 Apache Software Foundation Apache HTTP Server 2.2.8 Apache Software Foundation Apache HTTP Server 2.2.9 Apache Software Foundation Apache HTTP Server 2.2.10 Apache Software Foundation Apache HTTP Server 2.2.11 Apache Software Foundation Apache HTTP Server 2.2.12 Apache Software Foundation Apache HTTP Server 2.2.13 Apache Software Foundation Apache HTTP Server 2.2.14 Apache Software Foundation Apache HTTP Server 2.2.15 Apache Software Foundation Apache HTTP Server 2.2.16 Apache Software Foundation Apache HTTP Server 2.2.18 Apache Software Foundation Apache HTTP Server 2.2.19 Apache Software Foundation Apache HTTP Server 2.2.20 Apache HTTP Server 2.2.21

References

http://archives.neohapsis.com/archives/fulldisclosure/2011-11/0023.html

http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=c03360041
http://lists.apple.com/archives/security-announce/2012/Sep/msg00004.html
http://marc.info/?l=bugtraq&m=133294460209056&w=2
http://marc.info/?l=bugtraq&m=133494237717847&w=2
http://marc.info/?l=bugtraq&m=134987041210674&w=2
http://rhn.redhat.com/errata/RHSA-2012-0128.html
http://rhn.redhat.com/errata/RHSA-2012-0542.html
http://rhn.redhat.com/errata/RHSA-2012-0543.html
http://securitytracker.com/id?1026267
http://support.apple.com/kb/HT5501
http://www.debian.org/security/2012/dsa-2405
http://www.fujitsu.com/global/support/software/security/products-f/interstage-201303e.html
http://www.halfdog.net/Security/2011/ApacheModSetEnvIfIntegerOverflow/
http://www.halfdog.net/Security/2011/ApacheModSetEnvIfIntegerOverflow/DemoExploit.html
http://www.mandriva.com/security/advisories?name=MDVSA-2012:003
http://www.mandriva.com/security/advisories?name=MDVSA-2013:150
http://www.oracle.com/technetwork/topics/security/cpujan2015-1972971.html
http://www.oracle.com/technetwork/topics/security/cpujul2012-392727.html
http://www.securityfocus.com/bid/50494
https://bugs.launchpad.net/ubuntu/+source/apache2/+bug/811422
https://bugzilla.redhat.com/show_bug.cgi?id=750935
https://exchange.xforce.ibmcloud.com/vulnerabilities/71093

Summary

The mod_proxy module in the Apache HTTP Server 1.3.x through 1.3.42, 2.0.x through 2.0.64, and 2.2.x through 2.2.21, when the Revision 1179239 patch is in place, does not properly interact with use of (1) RewriteRule and (2) ProxyPassMatch pattern matches for configuration of a reverse proxy, which allows remote attackers to send requests to intranet servers via a malformed URI containing an @ (at sign) character and a : (colon) character in invalid positions. NOTE: this vulnerability exists because of an incomplete fix for CVE-2011-3368.

CVE-2011-4317 Information	
CVSS Score	4.3
CWE	CWE-20
Vulnerability impact	
Confidentiality	NONE
Integrity	PARTIAL
Availability	NONE
Access methodology information	
Vector	NETWORK
Complexity	MEDIUM
Authentication	NONE

Vulnerable configs

Apache Software Foundation Apache HTTP Server 1.3		Apache Software Foundation Apache HTTP Server 1.3.0
Apache Software Foundation Apache HTTP Server 1.3.1	Apache Software Foundation Apache HTTP Server 1.3.1.1	Apache Software Foundation Apache HTTP Server 1.3.2
Apache Software Foundation Apache HTTP Server 1.3.3	Apache Software Foundation Apache HTTP Server 1.3.4	Apache Software Foundation Apache HTTP Server 1.3.5
Apache Software Foundation Apache HTTP Server 1.3.6	Apache Software Foundation Apache HTTP Server 1.3.7	Apache Software Foundation Apache HTTP Server 1.3.8
Apache Software Foundation Apache HTTP Server 1.3.9	Apache Software Foundation Apache 1.3.10	Apache Software Foundation Apache HTTP Server 1.3.11
Apache Software Foundation Apache HTTP Server 1.3.12	Apache Software Foundation Apache 1.3.13	Apache Software Foundation Apache HTTP Server 1.3.14
Apache Software Foundation Apache 1.3.15	Apache Software Foundation Apache 1.3.16	Apache Software Foundation Apache HTTP Server 1.3.17
Apache Software Foundation Apache HTTP Server 1.3.18	Apache Software Foundation Apache HTTP Server 1.3.19	Apache Software Foundation Apache HTTP Server 1.3.20
Apache Software Foundation Apache HTTP Server 1.3.22	Apache Software Foundation Apache HTTP Server 1.3.23	Apache Software Foundation Apache HTTP Server 1.3.24
Apache Software Foundation Apache HTTP Server 1.3.25	Apache Software Foundation Apache HTTP Server 1.3.26	Apache Software Foundation Apache HTTP Server 1.3.27
Apache Software Foundation Apache HTTP Server 1.3.28	Apache Software Foundation Apache HTTP Server 1.3.29	Apache Software Foundation Apache HTTP Server 1.3.30
Apache Software Foundation Apache HTTP Server 1.3.31	Apache Software Foundation Apache HTTP Server 1.3.32	Apache Software Foundation Apache HTTP Server 1.3.33
Apache Software Foundation Apache HTTP Server 1.3.34	Apache Software Foundation Apache HTTP Server 1.3.35	Apache Software Foundation Apache HTTP Server 1.3.36
Apache Software Foundation Apache HTTP Server 1.3.37	Apache Software Foundation Apache HTTP Server 1.3.38	Apache Software Foundation Apache HTTP Server 1.3.39
Apache Software Foundation Apache HTTP Server 1.3.41	Apache Software Foundation Apache HTTP Server 1.3.42	Apache Software Foundation Apache HTTP Server 1.3.65
Apache Software Foundation Apache HTTP Server 1.3.68	Apache Software Foundation Apache HTTP Server 2.0	Apache Software Foundation Apache HTTP Server 2.0.9a
Apache Software Foundation Apache HTTP Server 2.0.28	Apache Software Foundation Apache HTTP Server 2.0.28 Beta	Apache Software Foundation Apache HTTP Server 2.0.32
Apache Software Foundation Apache HTTP Server 2.0.32 Beta	Apache Software Foundation Apache HTTP Server 2.0.34 Beta	Apache Software Foundation Apache HTTP Server 2.0.35
Apache Software Foundation Apache HTTP Server 2.0.36	Apache Software Foundation Apache HTTP Server 2.0.37	Apache Software Foundation Apache HTTP Server 2.0.38
Apache Software Foundation Apache HTTP Server 2.0.39	Apache Software Foundation Apache HTTP Server 2.0.40	Apache Software Foundation Apache HTTP Server 2.0.41
Apache Software Foundation Apache HTTP Server 2.0.42	Apache Software Foundation Apache HTTP Server 2.0.43	Apache Software Foundation Apache HTTP Server 2.0.44
Apache Software Foundation Apache HTTP Server 2.0.45	Apache Software Foundation Apache HTTP Server 2.0.46	Apache Software Foundation Apache HTTP Server 2.0.47
Apache Software Foundation Apache HTTP Server 2.0.48	Apache Software Foundation Apache HTTP Server 2.0.49	Apache Software Foundation Apache HTTP Server 2.0.50
Apache Software Foundation Apache HTTP Server 2.0.51	Apache Software Foundation Apache HTTP Server 2.0.52	Apache Software Foundation Apache HTTP Server 2.0.53

Apache Software Foundation Apache HTTP Server 2.0.54
Apache Software Foundation Apache HTTP Server 2.0.55
Apache Software Foundation Apache HTTP Server 2.0.56
Apache Software Foundation Apache HTTP Server 2.0.57
Apache Software Foundation Apache HTTP Server 2.0.58
Apache Software Foundation HTTP Server 2.0.59
Apache Software Foundation Apache HTTP Server 2.0.60 dev
Apache Software Foundation HTTP Server 2.0.61
Apache Software Foundation Apache HTTP Server 2.0.63
Apache Software Foundation Apache HTTP Server 2.0.64
Apache Software Foundation Apache HTTP Server 2.2.0
Apache Software Foundation Apache HTTP Server 2.2.1
Apache Software Foundation Apache HTTP Server 2.2.2
Apache Software Foundation Apache HTTP Server 2.2.3
Apache Software Foundation Apache HTTP Server 2.2.4
Apache Software Foundation Apache HTTP Server 2.2.6
Apache Software Foundation Apache HTTP Server 2.2.8
Apache Software Foundation Apache HTTP Server 2.2.9
Apache Software Foundation Apache HTTP Server 2.2.10
Apache Software Foundation Apache HTTP Server 2.2.11
Apache Software Foundation Apache HTTP Server 2.2.12
Apache Software Foundation Apache HTTP Server 2.2.13
Apache Software Foundation Apache HTTP Server 2.2.14
Apache Software Foundation Apache HTTP Server 2.2.15
Apache Software Foundation Apache HTTP Server 2.2.16
Apache Software Foundation Apache HTTP Server 2.2.18
Apache Software Foundation Apache HTTP Server 2.2.19
Apache Software Foundation Apache HTTP Server 2.2.20
Apache HTTP Server 2.2.21

References

http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=c03360041
http://kb.juniper.net/JSA10585
http://lists.apple.com/archives/security-announce/2012/Sep/msg00004.html
http://lists.opensuse.org/opensuse-updates/2013-02/msg00009.html
http://lists.opensuse.org/opensuse-updates/2013-02/msg00012.html
http://marc.info/?l=bugtraq&m=133294460209056&w=2
http://marc.info/?l=bugtraq&m=134987041210674&w=2
http://rhn.redhat.com/errata/RHSA-2012-0128.html
http://support.apple.com/kb/HT5501
http://thread.gmane.org/gmane.comp.apache.devel/46440
http://www.debian.org/security/2012/dsa-2405
http://www.mandriva.com/security/advisories?name=MDVSA-2012:003
http://www.mandriva.com/security/advisories?name=MDVSA-2013:150
http://www.oracle.com/technetwork/topics/security/cpujan2015-1972971.html
http://www.oracle.com/technetwork/topics/security/cpujul2012-392727.html
http://www.securitytracker.com/id?1026353
https://bugzilla.redhat.com/show_bug.cgi?id=756483
https://community.qualys.com/blogs/securitylabs/2011/11/23/apache-reverse-proxy-bypass-issue

Summary

The mod_proxy_ajp module in the Apache HTTP Server before 2.2.21, when used with mod_proxy_balancer in certain configurations, allows remote attackers to cause a denial of service (temporary "error state" in the backend server) via a malformed HTTP request.

CVE-2011-3348 Information	
CVSS Score	4.3
CWE	CWE-399
Vulnerability impact	
Confidentiality	NONE
Integrity	NONE
Availability	PARTIAL
Access methodology information	
Vector	NETWORK
Complexity	MEDIUM
Authentication	NONE

Vulnerable configs

Apache Software Foundation Apache HTTP Server 0.8.11		
Apache Software Foundation Apache HTTP Server 0.8.14	Apache Software Foundation Apache HTTP Server 1.0	Apache Software Foundation Apache HTTP Server 1.0.2
Apache Software Foundation Apache HTTP Server 1.0.3	Apache Software Foundation Apache HTTP Server 1.0.5	Apache Software Foundation Apache HTTP Server 1.1
Apache Software Foundation Apache HTTP Server 1.1.1	Apache Software Foundation Apache 1.2	Apache Software Foundation Apache HTTP Server 1.2.4
Apache Software Foundation Apache HTTP Server 1.2.5	Apache Software Foundation Apache HTTP Server 1.2.6	Apache Software Foundation Apache 1.29
Apache Software Foundation Apache HTTP Server 1.3	Apache Software Foundation Apache HTTP Server 1.3.0	Apache Software Foundation Apache HTTP Server 1.3.1
Apache Software Foundation Apache HTTP Server 1.3.1.1	Apache Software Foundation Apache HTTP Server 1.3.2	Apache Software Foundation Apache HTTP Server 1.3.3
Apache Software Foundation Apache HTTP Server 1.3.4	Apache Software Foundation Apache HTTP Server 1.3.5	Apache Software Foundation Apache HTTP Server 1.3.6
Apache Software Foundation Apache HTTP Server 1.3.7	Apache Software Foundation Apache HTTP Server 1.3.8	Apache Software Foundation Apache HTTP Server 1.3.9
Apache Software Foundation Apache 1.3.10	Apache Software Foundation Apache HTTP Server 1.3.11	Apache Software Foundation Apache HTTP Server 1.3.12
Apache Software Foundation Apache 1.3.13	Apache Software Foundation Apache HTTP Server 1.3.14	Apache Software Foundation Apache 1.3.15
Apache Software Foundation Apache 1.3.16	Apache Software Foundation Apache HTTP Server 1.3.17	Apache Software Foundation Apache HTTP Server 1.3.18
Apache Software Foundation Apache HTTP Server 1.3.19	Apache Software Foundation Apache HTTP Server 1.3.20	Apache Software Foundation Apache HTTP Server 1.3.22
Apache Software Foundation Apache HTTP Server 1.3.23	Apache Software Foundation Apache HTTP Server 1.3.24	Apache Software Foundation Apache HTTP Server 1.3.25
Apache Software Foundation Apache HTTP Server 1.3.26	Apache Software Foundation Apache HTTP Server 1.3.27	Apache Software Foundation Apache HTTP Server 1.3.28
Apache Software Foundation Apache HTTP Server 1.3.29	Apache Software Foundation Apache HTTP Server 1.3.30	Apache Software Foundation Apache HTTP Server 1.3.31
Apache Software Foundation Apache HTTP Server 1.3.32	Apache Software Foundation Apache HTTP Server 1.3.33	Apache Software Foundation Apache HTTP Server 1.3.34
Apache Software Foundation Apache HTTP Server 1.3.35	Apache Software Foundation Apache HTTP Server 1.3.36	Apache Software Foundation Apache HTTP Server 1.3.37
Apache Software Foundation Apache HTTP Server 1.3.38	Apache Software Foundation Apache HTTP Server 1.3.39	Apache Software Foundation Apache HTTP Server 1.3.41
Apache Software Foundation Apache HTTP Server 1.3.42	Apache Software Foundation Apache HTTP Server 1.3.65	Apache Software Foundation Apache HTTP Server 1.3.68
Apache Software Foundation Apache HTTP Server 1.4.0	Apache Software Foundation Apache HTTP Server 1.99	Apache Software Foundation Apache HTTP Server 2.0
Apache Software Foundation Apache HTTP Server 2.0.9a	Apache Software Foundation Apache HTTP Server 2.0.28	Apache Software Foundation Apache HTTP Server 2.0.28 Beta
Apache Software Foundation Apache HTTP Server 2.0.32	Apache Software Foundation Apache HTTP Server 2.0.32 Beta	Apache Software Foundation Apache HTTP Server 2.0.34 Beta
Apache Software Foundation Apache HTTP Server 2.0.35	Apache Software Foundation Apache HTTP Server 2.0.36	Apache Software Foundation Apache HTTP Server 2.0.37
Apache Software Foundation Apache HTTP Server 2.0.38	Apache Software Foundation Apache HTTP Server 2.0.39	Apache Software Foundation Apache HTTP Server 2.0.40
Apache Software Foundation Apache HTTP Server 2.0.41	Apache Software Foundation Apache HTTP Server 2.0.42	Apache Software Foundation Apache HTTP Server 2.0.43
Apache Software Foundation Apache HTTP Server 2.0.44	Apache Software Foundation Apache HTTP Server 2.0.45	Apache Software Foundation Apache HTTP Server 2.0.46
Apache Software Foundation Apache HTTP Server 2.0.47	Apache Software Foundation Apache HTTP Server 2.0.48	Apache Software Foundation Apache HTTP Server 2.0.49
Apache Software Foundation Apache HTTP Server 2.0.50	Apache Software Foundation Apache HTTP Server 2.0.51	Apache Software Foundation Apache HTTP Server 2.0.52
Apache Software Foundation Apache HTTP Server 2.0.53	Apache Software Foundation Apache HTTP Server 2.0.54	Apache Software Foundation Apache HTTP Server 2.0.55
Apache Software Foundation Apache HTTP Server 2.0.56	Apache Software Foundation Apache HTTP Server 2.0.57	Apache Software Foundation Apache HTTP Server 2.0.58
Apache Software Foundation HTTP Server 2.0.59	Apache Software Foundation Apache HTTP Server 2.0.60 dev	Apache Software Foundation HTTP Server 2.0.61

Apache Software Foundation Apache HTTP Server 2.0.63	Apache Software Foundation Apache HTTP Server 2.1	Apache Software Foundation Apache HTTP Server 2.1.1
Apache Software Foundation Apache HTTP Server 2.1.2	Apache Software Foundation Apache HTTP Server 2.1.3	Apache Software Foundation Apache HTTP Server 2.1.4
Apache Software Foundation Apache HTTP Server 2.1.5	Apache Software Foundation Apache HTTP Server 2.1.6	Apache Software Foundation Apache HTTP Server 2.1.7
Apache Software Foundation Apache HTTP Server 2.1.8	Apache Software Foundation Apache HTTP Server 2.1.9	Apache Software Foundation Apache HTTP Server 2.2
Apache Software Foundation Apache HTTP Server 2.2.0	Apache Software Foundation Apache HTTP Server 2.2.1	Apache Software Foundation Apache HTTP Server 2.2.2
Apache Software Foundation Apache HTTP Server 2.2.3	Apache Software Foundation Apache HTTP Server 2.2.4	Apache Software Foundation Apache HTTP Server 2.2.6
Apache Software Foundation Apache HTTP Server 2.2.8	Apache Software Foundation Apache HTTP Server 2.2.9	Apache Software Foundation Apache HTTP Server 2.2.10
Apache Software Foundation Apache HTTP Server 2.2.11	Apache Software Foundation Apache HTTP Server 2.2.12	Apache Software Foundation Apache HTTP Server 2.2.13
Apache Software Foundation Apache HTTP Server 2.2.14	Apache Software Foundation Apache HTTP Server 2.2.15	Apache Software Foundation Apache HTTP Server 2.2.16
Apache Software Foundation Apache HTTP Server 2.2.17	Apache Software Foundation Apache HTTP Server 2.2.18	Apache Software Foundation Apache HTTP Server 2.2.20

References

http://community.jboss.org/message/625307

http://httpd.apache.org/security/vulnerabilities_22.html##2.2.21

http://lists.apple.com/archives/security-announce/2012/Feb/msg00000.html

http://marc.info/?l=bugtraq&m=131731002122529&w=2

http://marc.info/?l=bugtraq&m=132033751509019&w=2

http://rhn.redhat.com/errata/RHSA-2012-0542.html

http://rhn.redhat.com/errata/RHSA-2012-0543.html

http://support.apple.com/kb/HT5130

http://www.apache.org/dist/httpd/Announcement2.2.html

http://www.mandriva.com/security/advisories?name=MDVSA-2011:168

http://www.oracle.com/technetwork/topics/security/cpujuly2013-1899826.html

http://www.redhat.com/support/errata/RHSA-2011-1391.html

http://www.securityfocus.com/bid/49616

http://www.securitytracker.com/id?1026054

https://exchange.xforce.ibmcloud.com/vulnerabilities/69804

Summary

Stack consumption vulnerability in the fnmatch implementation in apr_fnmatch.c in the Apache Portable Runtime (APR) library before 1.4.3 and the Apache HTTP Server before 2.2.18, and in fnmatch.c in libc in NetBSD 5.1, OpenBSD 4.8, FreeBSD, Apple Mac OS X 10.6, Oracle Solaris 10, and Android, allows context-dependent attackers to cause a denial of service (CPU and memory consumption) via *? sequences in the first argument, as demonstrated by attacks against mod_autoindex in httpd.

CVE-2011-0419 Information	
CVSS Score	4.3
CWE	CWE-399
Vulnerability impact	
Confidentiality	NONE
Integrity	NONE
Availability	PARTIAL
Access methodology information	
Vector	NETWORK
Complexity	MEDIUM
Authentication	NONE

Vulnerable configs

cpe:2.3:a:apache:portable_runtime:0.9.1	cpe:2.3:a:apache:portable_runtime:0.9.2	cpe:2.3:a:apache:portable_runtime:0.9.2-dev
cpe:2.3:a:apache:portable_runtime:0.9.3	cpe:2.3:a:apache:portable_runtime:0.9.3-dev	cpe:2.3:a:apache:portable_runtime:0.9.4
cpe:2.3:a:apache:portable_runtime:0.9.5	cpe:2.3:a:apache:portable_runtime:0.9.6	cpe:2.3:a:apache:portable_runtime:0.9.7
cpe:2.3:a:apache:portable_runtime:0.9.7-dev	cpe:2.3:a:apache:portable_runtime:0.9.8	cpe:2.3:a:apache:portable_runtime:0.9.9
cpe:2.3:a:apache:portable_runtime:0.9.16-dev	cpe:2.3:a:apache:portable_runtime:1.3.0	cpe:2.3:a:apache:portable_runtime:1.3.1
cpe:2.3:a:apache:portable_runtime:1.3.2	cpe:2.3:a:apache:portable_runtime:1.3.3	cpe:2.3:a:apache:portable_runtime:1.3.4
cpe:2.3:a:apache:portable_runtime:1.3.4-dev	cpe:2.3:a:apache:portable_runtime:1.3.5	cpe:2.3:a:apache:portable_runtime:1.3.6
cpe:2.3:a:apache:portable_runtime:1.3.6-dev	cpe:2.3:a:apache:portable_runtime:1.3.7	cpe:2.3:a:apache:portable_runtime:1.3.8
cpe:2.3:a:apache:portable_runtime:1.3.9	cpe:2.3:a:apache:portable_runtime:1.3.10	cpe:2.3:a:apache:portable_runtime:1.3.11
cpe:2.3:a:apache:portable_runtime:1.3.12	cpe:2.3:a:apache:portable_runtime:1.3.13	cpe:2.3:a:apache:portable_runtime:1.4.0
cpe:2.3:a:apache:portable_runtime:1.4.1	cpe:2.3:a:apache:portable_runtime:1.4.2	Apache Software Foundation Apache HTTP Server 0.8.11
Apache Software Foundation Apache HTTP Server 0.8.14	Apache Software Foundation Apache HTTP Server 1.0	Apache Software Foundation Apache HTTP Server 1.0.2
Apache Software Foundation Apache HTTP Server 1.0.3	Apache Software Foundation Apache HTTP Server 1.0.5	Apache Software Foundation Apache HTTP Server 1.1
Apache Software Foundation Apache HTTP Server 1.1.1	Apache Software Foundation Apache 1.2	Apache Software Foundation Apache HTTP Server 1.2.4
Apache Software Foundation Apache HTTP Server 1.2.5	Apache Software Foundation Apache HTTP Server 1.2.6	Apache Software Foundation Apache 1.29
Apache Software Foundation Apache HTTP Server 1.3	Apache Software Foundation Apache HTTP Server 1.3.0	Apache Software Foundation Apache HTTP Server 1.3.1
Apache Software Foundation Apache HTTP Server 1.3.1.1	Apache Software Foundation Apache HTTP Server 1.3.2	Apache Software Foundation Apache HTTP Server 1.3.3
Apache Software Foundation Apache HTTP Server 1.3.4	Apache Software Foundation Apache HTTP Server 1.3.5	Apache Software Foundation Apache HTTP Server 1.3.6
Apache Software Foundation Apache HTTP Server 1.3.7	Apache Software Foundation Apache HTTP Server 1.3.8	Apache Software Foundation Apache HTTP Server 1.3.9
Apache Software Foundation Apache 1.3.10	Apache Software Foundation Apache HTTP Server 1.3.11	Apache Software Foundation Apache HTTP Server 1.3.12
Apache Software Foundation Apache 1.3.13	Apache Software Foundation Apache HTTP Server 1.3.14	Apache Software Foundation Apache 1.3.15
Apache Software Foundation Apache 1.3.16	Apache Software Foundation Apache HTTP Server 1.3.17	Apache Software Foundation Apache HTTP Server 1.3.18
Apache Software Foundation Apache HTTP Server 1.3.19	Apache Software Foundation Apache HTTP Server 1.3.20	Apache Software Foundation Apache HTTP Server 1.3.22
Apache Software Foundation Apache HTTP Server 1.3.23	Apache Software Foundation Apache HTTP Server 1.3.24	Apache Software Foundation Apache HTTP Server 1.3.25

Apache Software Foundation Apache HTTP Server 1.3.26	Apache Software Foundation Apache HTTP Server 1.3.27	Apache Software Foundation Apache HTTP Server 1.3.28
Apache Software Foundation Apache HTTP Server 1.3.29	Apache Software Foundation Apache HTTP Server 1.3.30	Apache Software Foundation Apache HTTP Server 1.3.31
Apache Software Foundation Apache HTTP Server 1.3.32	Apache Software Foundation Apache HTTP Server 1.3.33	Apache Software Foundation Apache HTTP Server 1.3.34
Apache Software Foundation Apache HTTP Server 1.3.35	Apache Software Foundation Apache HTTP Server 1.3.36	Apache Software Foundation Apache HTTP Server 1.3.37
Apache Software Foundation Apache HTTP Server 1.3.38	Apache Software Foundation Apache HTTP Server 1.3.39	Apache Software Foundation Apache HTTP Server 1.3.41
Apache Software Foundation Apache HTTP Server 1.3.42	Apache Software Foundation Apache HTTP Server 1.3.65	Apache Software Foundation Apache HTTP Server 1.3.68
Apache Software Foundation Apache HTTP Server 1.4.0	Apache Software Foundation Apache HTTP Server 1.99	Apache Software Foundation Apache HTTP Server 2.0
Apache Software Foundation Apache HTTP Server 2.0.9a	Apache Software Foundation Apache HTTP Server 2.0.28	Apache Software Foundation Apache HTTP Server 2.0.28 Beta
Apache Software Foundation Apache HTTP Server 2.0.32	Apache Software Foundation Apache HTTP Server 2.0.32 Beta	Apache Software Foundation Apache HTTP Server 2.0.34 Beta
Apache Software Foundation Apache HTTP Server 2.0.35	Apache Software Foundation Apache HTTP Server 2.0.36	Apache Software Foundation Apache HTTP Server 2.0.37
Apache Software Foundation Apache HTTP Server 2.0.38	Apache Software Foundation Apache HTTP Server 2.0.39	Apache Software Foundation Apache HTTP Server 2.0.40
Apache Software Foundation Apache HTTP Server 2.0.41	Apache Software Foundation Apache HTTP Server 2.0.42	Apache Software Foundation Apache HTTP Server 2.0.43
Apache Software Foundation Apache HTTP Server 2.0.44	Apache Software Foundation Apache HTTP Server 2.0.45	Apache Software Foundation Apache HTTP Server 2.0.46
Apache Software Foundation Apache HTTP Server 2.0.47	Apache Software Foundation Apache HTTP Server 2.0.48	Apache Software Foundation Apache HTTP Server 2.0.49
Apache Software Foundation Apache HTTP Server 2.0.50	Apache Software Foundation Apache HTTP Server 2.0.51	Apache Software Foundation Apache HTTP Server 2.0.52
Apache Software Foundation Apache HTTP Server 2.0.53	Apache Software Foundation Apache HTTP Server 2.0.54	Apache Software Foundation Apache HTTP Server 2.0.55
Apache Software Foundation Apache HTTP Server 2.0.56	Apache Software Foundation Apache HTTP Server 2.0.57	Apache Software Foundation Apache HTTP Server 2.0.58
Apache Software Foundation HTTP Server 2.0.59	Apache Software Foundation Apache HTTP Server 2.0.60 dev	Apache Software Foundation HTTP Server 2.0.61
Apache Software Foundation Apache HTTP Server 2.0.63	Apache Software Foundation Apache HTTP Server 2.1	Apache Software Foundation Apache HTTP Server 2.1.1
Apache Software Foundation Apache HTTP Server 2.1.2	Apache Software Foundation Apache HTTP Server 2.1.3	Apache Software Foundation Apache HTTP Server 2.1.4
Apache Software Foundation Apache HTTP Server 2.1.5	Apache Software Foundation Apache HTTP Server 2.1.6	Apache Software Foundation Apache HTTP Server 2.1.7
Apache Software Foundation Apache HTTP Server 2.1.8	Apache Software Foundation Apache HTTP Server 2.1.9	Apache Software Foundation Apache HTTP Server 2.2
Apache Software Foundation Apache HTTP Server 2.2.0	Apache Software Foundation Apache HTTP Server 2.2.1	Apache Software Foundation Apache HTTP Server 2.2.2
Apache Software Foundation Apache HTTP Server 2.2.3	Apache Software Foundation Apache HTTP Server 2.2.4	Apache Software Foundation Apache HTTP Server 2.2.6
Apache Software Foundation Apache HTTP Server 2.2.8	Apache Software Foundation Apache HTTP Server 2.2.9	Apache Software Foundation Apache HTTP Server 2.2.10
Apache Software Foundation Apache HTTP Server 2.2.11	Apache Software Foundation Apache HTTP Server 2.2.12	Apache Software Foundation Apache HTTP Server 2.2.13
Apache Software Foundation Apache HTTP Server 2.2.14	Apache Software Foundation Apache HTTP Server 2.2.15	Apache Software Foundation Apache HTTP Server 2.2.16
Apache Software Foundation Apache HTTP Server 2.2.17	Apple Mac OS X 10.6.0	FreeBSD
Google Android Operating System	NetBSD 5.1	OpenBSD 4.8
Oracle Solaris 10		

References

http://cvsweb.netbsd.org/bsdweb.cgi/src/lib/libc/gen/fnmatch.c##rev1.22

http://cxib.net/stuff/apache.fnmatch.phps

http://cxib.net/stuff/apr_fnmatch.txts

http://httpd.apache.org/security/vulnerabilities_22.html

http://lists.apple.com/archives/Security-announce/2011//Oct/msg00003.html

http://lists.opensuse.org/opensuse-security-announce/2011-11/msg00011.html

http://marc.info/?l=bugtraq&m=131551295528105&w=2

http://marc.info/?l=bugtraq&m=131731002122529&w=2

http://marc.info/?l=bugtraq&m=132033751509019&w=2

http://marc.info/?l=bugtraq&m=134987041210674&w=2

http://secunia.com/advisories/48308

http://securityreason.com/achievement_securityalert/98

http://securityreason.com/securityalert/8246

http://securitytracker.com/id?1025527

http://support.apple.com/kb/HT5002

http://svn.apache.org/viewvc/apr/apr/branches/1.4.x/strings/apr_fnmatch.c?r1=731029&r2=1098902

http://svn.apache.org/viewvc?view=revision&revision=1098188

http://svn.apache.org/viewvc?view=revision&revision=1098799

http://www.apache.org/dist/apr/Announcement1.x.html

http://www.apache.org/dist/apr/CHANGES-APR-1.4

http://www.apache.org/dist/httpd/Announcement2.2.html
http://www.debian.org/security/2011/dsa-2237
http://www.mail-archive.com/dev@apr.apache.org/msg23960.html
http://www.mail-archive.com/dev@apr.apache.org/msg23961.html
http://www.mail-archive.com/dev@apr.apache.org/msg23976.html
http://www.mandriva.com/security/advisories?name=MDVSA-2011:084
http://www.mandriva.com/security/advisories?name=MDVSA-2013:150
http://www.openbsd.org/cgi-bin/cvsweb/src/lib/libc/gen/fnmatch.c##rev1.15
http://www.oracle.com/technetwork/topics/security/cpujul2012-392727.html
http://www.oracle.com/technetwork/topics/security/cpujuly2013-1899826.html
http://www.redhat.com/support/errata/RHSA-2011-0507.html
http://www.redhat.com/support/errata/RHSA-2011-0896.html
http://www.redhat.com/support/errata/RHSA-2011-0897.html
https://bugzilla.redhat.com/show_bug.cgi?id=703390

Summary

Multiple cross-site scripting (XSS) vulnerabilities in the balancer_handler function in the manager interface in mod_proxy_balancer.c in the mod_proxy_balancer module in the Apache HTTP Server 2.2.x before 2.2.24-dev and 2.4.x before 2.4.4 allow remote attackers to inject arbitrary web script or HTML via a crafted string.

CVE-2012-4558 Information	
CVSS Score	4.3
CWE	CWE-79
Vulnerability impact	
Confidentiality	NONE
Integrity	PARTIAL
Availability	NONE
Access methodology information	
Vector	NETWORK
Complexity	MEDIUM
Authentication	NONE

Vulnerable configs

Apache Software Foundation Apache HTTP Server 2.2
Apache Software Foundation Apache HTTP Server 2.2.0
Apache Software Foundation Apache HTTP Server 2.2.1
Apache Software Foundation Apache HTTP Server 2.2.2
Apache Software Foundation Apache HTTP Server 2.2.3
Apache Software Foundation Apache HTTP Server 2.2.4
Apache Software Foundation Apache HTTP Server 2.2.6
Apache Software Foundation Apache HTTP Server 2.2.8
Apache Software Foundation Apache HTTP Server 2.2.9
Apache Software Foundation Apache HTTP Server 2.2.10
Apache Software Foundation Apache HTTP Server 2.2.11
Apache Software Foundation Apache HTTP Server 2.2.12
Apache Software Foundation Apache HTTP Server 2.2.13
Apache Software Foundation Apache HTTP Server 2.2.14
Apache Software Foundation Apache HTTP Server 2.2.15
Apache Software Foundation Apache HTTP Server 2.2.16
Apache Software Foundation Apache HTTP Server 2.2.17
Apache Software Foundation Apache HTTP Server 2.2.18
Apache Software Foundation Apache HTTP Server 2.2.19
Apache Software Foundation Apache HTTP Server 2.2.20
Apache HTTP Server 2.2.21
Apache Software Foundation Apache HTTP Server 2.2.22
Apache Software Foundation Apache HTTP Server 2.2.23
Apache Software Foundation Apache HTTP Server 2.4.1
Apache Software Foundation Apache HTTP Server 2.4.2
Apache Software Foundation Apache HTTP Server 2.4.0
Apache Software Foundation Apache HTTP Server 2.4.3

References

http://httpd.apache.org/security/vulnerabilities_22.html
http://httpd.apache.org/security/vulnerabilities_24.html
http://lists.apple.com/archives/security-announce/2013/Sep/msg00002.html
http://lists.fedoraproject.org/pipermail/package-announce/2013-April/101196.html

http://marc.info/?l=bugtraq&m=136612293908376&w=2
http://rhn.redhat.com/errata/RHSA-2013-0815.html
http://rhn.redhat.com/errata/RHSA-2013-1207.html
http://rhn.redhat.com/errata/RHSA-2013-1208.html
http://rhn.redhat.com/errata/RHSA-2013-1209.html
http://support.apple.com/kb/HT5880
http://svn.apache.org/viewvc/httpd/httpd/trunk/modules/proxy/mod_proxy_balancer.c?r1=1404653&r2=1
http://www.debian.org/security/2013/dsa-2637
http://www.oracle.com/technetwork/topics/security/cpujan2014-1972949.html
http://www.securityfocus.com/bid/58165
http://www.securityfocus.com/bid/64758

Summary

protocol.c in the Apache HTTP Server 2.2.x through 2.2.21 does not properly restrict header information during construction of Bad Request (aka 400) error documents, which allows remote attackers to obtain the values of HTTPOnly cookies via vectors involving a (1) long or (2) malformed header in conjunction with crafted web script.

CVE-2012-0053 Information	
CVSS Score	4.3
CWE	CWE-264
Vulnerability impact	
Confidentiality	PARTIAL
Integrity	NONE
Availability	NONE
Access methodology information	
Vector	NETWORK
Complexity	MEDIUM
Authentication	NONE

Vulnerable configs

Apache Software Foundation Apache HTTP Server 2.2
Apache Software Foundation Apache HTTP Server 2.2.0
Apache Software Foundation Apache HTTP Server 2.2.1
Apache Software Foundation Apache HTTP Server 2.2.2
Apache Software Foundation Apache HTTP Server 2.2.3
Apache Software Foundation Apache HTTP Server 2.2.4
Apache Software Foundation Apache HTTP Server 2.2.6
Apache Software Foundation Apache HTTP Server 2.2.8
Apache Software Foundation Apache HTTP Server 2.2.9
Apache Software Foundation Apache HTTP Server 2.2.10
Apache Software Foundation Apache HTTP Server 2.2.11
Apache Software Foundation Apache HTTP Server 2.2.12
Apache Software Foundation Apache HTTP Server 2.2.13
Apache Software Foundation Apache HTTP Server 2.2.14
Apache Software Foundation Apache HTTP Server 2.2.15
Apache Software Foundation Apache HTTP Server 2.2.16
Apache Software Foundation Apache HTTP Server 2.2.17
Apache Software Foundation Apache HTTP Server 2.2.18
Apache Software Foundation Apache HTTP Server 2.2.19
Apache Software Foundation Apache HTTP Server 2.2.20
Apache HTTP Server 2.2.21

References

http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=c03360041
http://httpd.apache.org/security/vulnerabilities_22.html
http://kb.juniper.net/JSA10585
http://lists.apple.com/archives/security-announce/2012/Sep/msg00004.html
http://lists.opensuse.org/opensuse-security-announce/2012-02/msg00026.html

http://lists.opensuse.org/opensuse-security-announce/2012-03/msg00002.html
http://marc.info/?l=bugtraq&m=133294460209056&w=2
http://marc.info/?l=bugtraq&m=133494237717847&w=2
http://marc.info/?l=bugtraq&m=133951357207000&w=2
http://marc.info/?l=bugtraq&m=136441204617335&w=2
http://rhn.redhat.com/errata/RHSA-2012-0128.html
http://rhn.redhat.com/errata/RHSA-2012-0542.html
http://rhn.redhat.com/errata/RHSA-2012-0543.html
http://support.apple.com/kb/HT5501
http://svn.apache.org/viewvc?view=revision&revision=1235454
http://www.debian.org/security/2012/dsa-2405
http://www.mandriva.com/security/advisories?name=MDVSA-2012:012
http://www.mandriva.com/security/advisories?name=MDVSA-2013:150
http://www.oracle.com/technetwork/topics/security/cpujan2015-1972971.html
http://www.oracle.com/technetwork/topics/security/cpujul2012-392727.html
http://www.securityfocus.com/bid/51706
https://bugzilla.redhat.com/show_bug.cgi?id=785069

Summary

The mod_proxy module in the Apache HTTP Server 2.0.x through 2.0.64 and 2.2.x before 2.2.18, when the Revision 1179239 patch is in place, does not properly interact with use of (1) RewriteRule and (2) ProxyPassMatch pattern matches for configuration of a reverse proxy, which allows remote attackers to send requests to intranet servers by using the HTTP/0.9 protocol with a malformed URI containing an initial @ (at sign) character. NOTE: this vulnerability exists because of an incomplete fix for CVE-2011-3368.

CVE-2011-3639 Information	
CVSS Score	4.3
CWE	CWE-20
Vulnerability impact	
Confidentiality	NONE
Integrity	PARTIAL
Availability	NONE
Access methodology information	
Vector	NETWORK
Complexity	MEDIUM
Authentication	NONE

Vulnerable configs

cpe:2.3:a:apache:http_server:2.0.11		cpe:2.3:a:apache:http_server:2.0.12
cpe:2.3:a:apache:http_server:2.0.13	cpe:2.3:a:apache:http_server:2.0.14	cpe:2.3:a:apache:http_server:2.0.15
cpe:2.3:a:apache:http_server:2.0.16	cpe:2.3:a:apache:http_server:2.0.17	cpe:2.3:a:apache:http_server:2.0.18
cpe:2.3:a:apache:http_server:2.0.19	cpe:2.3:a:apache:http_server:2.0.20	cpe:2.3:a:apache:http_server:2.0.21
cpe:2.3:a:apache:http_server:2.0.22	cpe:2.3:a:apache:http_server:2.0.23	cpe:2.3:a:apache:http_server:2.0.24
cpe:2.3:a:apache:http_server:2.0.25	cpe:2.3:a:apache:http_server:2.0.26	cpe:2.3:a:apache:http_server:2.0.27
Apache Software Foundation Apache HTTP Server 2.0.28	cpe:2.3:a:apache:http_server:2.0.29	cpe:2.3:a:apache:http_server:2.0.30
cpe:2.3:a:apache:http_server:2.0.31	Apache Software Foundation Apache HTTP Server 2.0.32	cpe:2.3:a:apache:http_server:2.0.33
cpe:2.3:a:apache:http_server:2.0.34	Apache Software Foundation Apache HTTP Server 2.0.35	Apache Software Foundation Apache HTTP Server 2.0.36
Apache Software Foundation Apache HTTP Server 2.0.37	Apache Software Foundation Apache HTTP Server 2.0.38	Apache Software Foundation Apache HTTP Server 2.0.39
Apache Software Foundation Apache HTTP Server 2.0.40	Apache Software Foundation Apache HTTP Server 2.0.41	Apache Software Foundation Apache HTTP Server 2.0.42
Apache Software Foundation Apache HTTP Server 2.0.43	Apache Software Foundation Apache HTTP Server 2.0.44	Apache Software Foundation Apache HTTP Server 2.0.45
Apache Software Foundation Apache HTTP Server 2.0.46	Apache Software Foundation Apache HTTP Server 2.0.47	Apache Software Foundation Apache HTTP Server 2.0.48
Apache Software Foundation Apache HTTP Server 2.0.49	Apache Software Foundation Apache HTTP Server 2.0.50	Apache Software Foundation Apache HTTP Server 2.0.51
Apache Software Foundation Apache HTTP Server 2.0.52	Apache Software Foundation Apache HTTP Server 2.0.53	Apache Software Foundation Apache HTTP Server 2.0.54
Apache Software Foundation Apache HTTP Server 2.0.55	Apache Software Foundation Apache HTTP Server 2.0.56	Apache Software Foundation Apache HTTP Server 2.0.57
Apache Software Foundation Apache HTTP Server 2.0.58	Apache Software Foundation HTTP Server 2.0.59	Apache Software Foundation HTTP Server 2.0.61
Apache Software Foundation Apache HTTP Server 2.0.63	Apache Software Foundation Apache HTTP Server 2.2.0	Apache Software Foundation Apache HTTP Server 2.2.1
Apache Software Foundation Apache HTTP Server 2.2.2	Apache Software Foundation Apache HTTP Server 2.2.3	Apache Software Foundation Apache HTTP Server 2.2.4
Apache Software Foundation Apache HTTP Server 2.2.6	Apache Software Foundation Apache HTTP Server 2.2.8	Apache Software Foundation Apache HTTP Server 2.2.9
Apache Software Foundation Apache HTTP Server 2.2.10	Apache Software Foundation Apache HTTP Server 2.2.11	Apache Software Foundation Apache HTTP Server 2.2.12
Apache Software Foundation Apache HTTP Server 2.2.13	Apache Software Foundation Apache HTTP Server 2.2.14	Apache Software Foundation Apache HTTP Server 2.2.15
Apache Software Foundation Apache HTTP Server 2.2.16	Apache Software Foundation Apache HTTP Server 2.2.17	cpe:2.3:a:apache:http_server2.0a1
cpe:2.3:a:apache:http_server2.0a2	cpe:2.3:a:apache:http_server2.0a3	cpe:2.3:a:apache:http_server2.0a4

cpe:2.3:a:apache:http_server2.0a5 cpe:2.3:a:apache:http_server2.0a6 cpe:2.3:a:apache:http_server2.0a7
cpe:2.3:a:apache:http_server2.0a8 cpe:2.3:a:apache:http_server2.0a9

References

http://rhn.redhat.com/errata/RHSA-2012-0128.html

http://svn.apache.org/viewvc?view=revision&revision=1188745

http://www.debian.org/security/2012/dsa-2405

https://bugzilla.redhat.com/show_bug.cgi?id=752080

Summary

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.

CVE-2008-2939 Information	
CVSS Score	4.3
CWE	CWE-79
Vulnerability impact	
Confidentiality	NONE
Integrity	PARTIAL
Availability	NONE
Access methodology information	
Vector	NETWORK
Complexity	MEDIUM
Authentication	NONE

Vulnerable configs

Apache Software Foundation Apache HTTP Server
Apache Software Foundation Apache HTTP Server 2.0.63
Apache Software Foundation Apache HTTP Server 2.2.0
Apache Software Foundation Apache HTTP Server 2.2.1
Apache Software Foundation Apache HTTP Server 2.2.2
Apache Software Foundation Apache HTTP Server 2.2.3
Apache Software Foundation Apache HTTP Server 2.2.4
Apache Software Foundation Apache HTTP Server 2.2.6
Apache Software Foundation Apache HTTP Server 2.2.8
Apache Software Foundation Apache HTTP Server 2.2.9
Apple Mac OS X 10.5.6
Canonical Ubuntu Linux 6.06 LTS (Long-Term Support)
Canonical Ubuntu Linux 7.10
Canonical Ubuntu Linux 8.04 LTS (Long-Term Support)
OpenSUSE 10.2
OpenSUSE 10.3
OpenSUSE 11.0

References

http://lists.apple.com/archives/security-announce/2009/May/msg00002.html
http://lists.opensuse.org/opensuse-security-announce/2008-11/msg00000.html
http://marc.info/?l=bugtraq&m=123376588623823&w=2
http://marc.info/?l=bugtraq&m=125631037611762&w=2
http://rhn.redhat.com/errata/RHSA-2008-0967.html
http://sunsolve.sun.com/search/document.do?assetkey=1-26-247666-1

http://support.apple.com/kb/HT3549
http://svn.apache.org/viewvc?view=rev&revision=682868
http://svn.apache.org/viewvc?view=rev&revision=682870
http://svn.apache.org/viewvc?view=rev&revision=682871
http://wiki.rpath.com/Advisories:rPSA-2008-0327
http://wiki.rpath.com/wiki/Advisories:rPSA-2008-0328
http://www-1.ibm.com/support/docview.wss?uid=swg1PK70197
http://www-1.ibm.com/support/docview.wss?uid=swg1PK70937
http://www.kb.cert.org/vuls/id/663763
http://www.mandriva.com/security/advisories?name=MDVSA-2008:194
http://www.mandriva.com/security/advisories?name=MDVSA-2008:195
http://www.mandriva.com/security/advisories?name=MDVSA-2009:124
http://www.rapid7.com/advisories/R7-0033
http://www.redhat.com/support/errata/RHSA-2008-0966.html
http://www.securityfocus.com/archive/1/495180/100/0/threaded
http://www.securityfocus.com/archive/1/498566/100/0/threaded
http://www.securityfocus.com/archive/1/498567/100/0/threaded
http://www.securityfocus.com/bid/30560
http://www.securitytracker.com/id?1020635
http://www.ubuntu.com/usn/USN-731-1
http://www.us-cert.gov/cas/techalerts/TA09-133A.html
http://www.vupen.com/english/advisories/2008/2315
http://www.vupen.com/english/advisories/2008/2461
http://www.vupen.com/english/advisories/2009/0320
http://www.vupen.com/english/advisories/2009/1297
https://exchange.xforce.ibmcloud.com/vulnerabilities/44223

Summary

mod_dav.c in the Apache HTTP Server before 2.2.25 does 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 Information	
CVSS Score	4.3
CWE	CWE-264
Vulnerability impact	
Confidentiality	NONE
Integrity	NONE
Availability	PARTIAL
Access methodology information	
Vector	NETWORK
Complexity	MEDIUM
Authentication	NONE

Vulnerable configs

Apache Software Foundation Apache HTTP Server 2.2.24
Apache Software Foundation Apache HTTP Server 2.2.1
Apache Software Foundation Apache HTTP Server 2.2.0
Apache Software Foundation Apache HTTP Server 2.2.10
Apache Software Foundation Apache HTTP Server 2.2.22
Apache Software Foundation Apache HTTP Server 2.2.15
Apache Software Foundation Apache HTTP Server 2.2.4
Apache Software Foundation Apache HTTP Server 2.2.13
Apache Software Foundation Apache HTTP Server 2.2.6
Apache Software Foundation Apache HTTP Server 2.2.11
Apache Software Foundation Apache HTTP Server 2.2.8
Apache Software Foundation Apache HTTP Server 2.2.23
Apache HTTP Server 2.2.21
Apache Software Foundation Apache HTTP Server 2.2.17
Apache Software Foundation Apache HTTP Server 2.2.3
Apache Software Foundation Apache HTTP Server 2.2.19
Apache Software Foundation Apache HTTP Server 2.2.12
Apache Software Foundation Apache HTTP Server 2.2.9
Apache Software Foundation Apache HTTP Server 2.2.20
Apache Software Foundation Apache HTTP Server 2.2.16
Apache Software Foundation Apache HTTP Server 2.2.2
Apache Software Foundation Apache HTTP Server 2.2.18
Apache Software Foundation Apache HTTP Server 2.2.14

References

http://lists.opensuse.org/opensuse-updates/2013-08/msg00026.html
http://lists.opensuse.org/opensuse-updates/2013-08/msg00029.html
http://lists.opensuse.org/opensuse-updates/2013-08/msg00030.html
http://rhn.redhat.com/errata/RHSA-2013-1156.html
http://rhn.redhat.com/errata/RHSA-2013-1207.html

http://rhn.redhat.com/errata/RHSA-2013-1208.html
http://rhn.redhat.com/errata/RHSA-2013-1209.html
http://support.apple.com/kb/HT6150
http://svn.apache.org/viewvc/httpd/httpd/trunk/modules/dav/main/mod_dav.c?r1=1482522&r2=1485668
http://svn.apache.org/viewvc/httpd/httpd/trunk/modules/dav/main/mod_dav.c?view=log
http://tools.cisco.com/security/center/content/CiscoSecurityNotice/CVE-2013-1896
http://www-01.ibm.com/support/docview.wss?uid=swg21644047
http://www.apache.org/dist/httpd/Announcement2.2.html
http://www.securityfocus.com/bid/61129
http://www.ubuntu.com/usn/USN-1903-1
https://h20566.www2.hp.com/portal/site/hpsc/template.PAGE/public/kb/docDisplay/?spf_p.tpst=kbDocD
navigationalState\%3DdocId\%253Demr_na-c03922406-1\%257CdocLocale\%253D\%257CcalledBy\%253
https://httpd.apache.org/security/vulnerabilities_24.html

Summary

Possible CRLF injection allowing HTTP response splitting attacks for sites which use mod_userdir. This issue was mitigated by changes made in 2.4.25 and 2.2.32 which prohibit CR or LF injection into the "Location" or other outbound header key or value. Fixed in Apache HTTP Server 2.4.25 (Affected 2.4.1-2.4.23). Fixed in Apache HTTP Server 2.2.32 (Affected 2.2.0-2.2.31).

CVE-2016-4975 Information	
CVSS Score	4.3
CWE	CWE-93

Vulnerable configs

Apache Software Foundation Apache HTTP Server 2.2.0
Apache Software Foundation Apache HTTP Server 2.2.2
Apache Software Foundation Apache HTTP Server 2.2.3
Apache Software Foundation Apache HTTP Server 2.2.4
Apache Software Foundation Apache HTTP Server 2.2.6
Apache Software Foundation Apache HTTP Server 2.2.8
Apache Software Foundation Apache HTTP Server 2.2.9
Apache Software Foundation Apache HTTP Server 2.2.10
Apache Software Foundation Apache HTTP Server 2.2.11
Apache Software Foundation Apache HTTP Server 2.2.12
Apache Software Foundation Apache HTTP Server 2.2.13
Apache Software Foundation Apache HTTP Server 2.2.14
Apache Software Foundation Apache HTTP Server 2.2.15
Apache Software Foundation Apache HTTP Server 2.2.16
Apache Software Foundation Apache HTTP Server 2.2.17
Apache Software Foundation Apache HTTP Server 2.2.18
Apache Software Foundation Apache HTTP Server 2.2.19
Apache Software Foundation Apache HTTP Server 2.2.20
Apache HTTP Server 2.2.21
Apache Software Foundation Apache HTTP Server 2.2.22
Apache Software Foundation Apache HTTP Server 2.2.23
Apache Software Foundation Apache HTTP Server 2.2.24
Apache Software Foundation Apache HTTP Server 2.2.25
Apache Software Foundation Apache HTTP Server 2.2.26
Apache Software Foundation Apache HTTP Server 2.2.27
Apache Software Foundation Apache HTTP Server 2.2.29
Apache Software Foundation Apache HTTP Server 2.2.31
Apache Software Foundation Apache HTTP Server 2.4.1
Apache Software Foundation Apache HTTP Server 2.4.2
Apache Software Foundation Apache HTTP Server 2.4.3
Apache Software Foundation Apache HTTP Server 2.4.4
Apache Software Foundation Apache HTTP Server 2.4.6
Apache Software Foundation Apache HTTP Server 2.4.7
Apache Software Foundation Apache HTTP Server 2.4.9
Apache Software Foundation Apache HTTP Server 2.4.10
Apache Software Foundation Apache HTTP Server 2.4.12
Apache Software Foundation Apache HTTP Server 2.4.16
Apache Software Foundation Apache HTTP Server 2.4.17
Apache Software Foundation Apache HTTP Server 2.4.18
Apache Software Foundation HTTP Server 2.4.20
Apache Software Foundation HTTP Server 2.4.23

References

http://www.securityfocus.com/bid/105093
https://httpd.apache.org/security/vulnerabilities_22.html##CVE-2016-4975
https://httpd.apache.org/security/vulnerabilities_24.html##CVE-2016-4975
https://security.netapp.com/advisory/ntap-20180926-0006/
https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbux03908en_us

Summary

Multiple cross-site scripting (XSS) vulnerabilities in the Apache HTTP Server 2.2.x before 2.2.24-dev and 2.4.x before 2.4.4 allow remote attackers to inject arbitrary web script or HTML via vectors involving hostnames and URIs in the (1) mod_imagemap, (2) mod_info, (3) mod_ldap, (4) mod_proxy_ftp, and (5) mod_status modules.

CVE-2012-3499 Information	
CVSS Score	4.3
CWE	CWE-79
Vulnerability impact	
Confidentiality	NONE
Integrity	PARTIAL
Availability	NONE
Access methodology information	
Vector	NETWORK
Complexity	MEDIUM
Authentication	NONE

Vulnerable configs

Apache Software Foundation Apache HTTP Server 2.2
Apache Software Foundation Apache HTTP Server 2.2.0
Apache Software Foundation Apache HTTP Server 2.2.1
Apache Software Foundation Apache HTTP Server 2.2.2
Apache Software Foundation Apache HTTP Server 2.2.3
Apache Software Foundation Apache HTTP Server 2.2.4
Apache Software Foundation Apache HTTP Server 2.2.6
Apache Software Foundation Apache HTTP Server 2.2.8
Apache Software Foundation Apache HTTP Server 2.2.9
Apache Software Foundation Apache HTTP Server 2.2.10
Apache Software Foundation Apache HTTP Server 2.2.11
Apache Software Foundation Apache HTTP Server 2.2.12
Apache Software Foundation Apache HTTP Server 2.2.13
Apache Software Foundation Apache HTTP Server 2.2.14
Apache Software Foundation Apache HTTP Server 2.2.15
Apache Software Foundation Apache HTTP Server 2.2.16
Apache Software Foundation Apache HTTP Server 2.2.17
Apache Software Foundation Apache HTTP Server 2.2.18
Apache Software Foundation Apache HTTP Server 2.2.19
Apache Software Foundation Apache HTTP Server 2.2.20
Apache HTTP Server 2.2.21
Apache Software Foundation Apache HTTP Server 2.2.22
Apache Software Foundation Apache HTTP Server 2.2.23
Apache Software Foundation Apache HTTP Server 2.4.1
Apache Software Foundation Apache HTTP Server 2.4.2
Apache Software Foundation Apache HTTP Server 2.4.0
Apache Software Foundation Apache HTTP Server 2.4.3

References

http://httpd.apache.org/security/vulnerabilities_22.html
http://httpd.apache.org/security/vulnerabilities_24.html
http://lists.apple.com/archives/security-announce/2013/Sep/msg00002.html
http://lists.fedoraproject.org/pipermail/package-announce/2013-April/101196.html

http://marc.info/?l=bugtraq&m=136612293908376&w=2
http://rhn.redhat.com/errata/RHSA-2013-0815.html
http://rhn.redhat.com/errata/RHSA-2013-1207.html
http://rhn.redhat.com/errata/RHSA-2013-1208.html
http://rhn.redhat.com/errata/RHSA-2013-1209.html
http://support.apple.com/kb/HT5880
http://svn.apache.org/viewvc/httpd/httpd/trunk/modules/generators/mod_info.c?r1=1225799&r2=141373
http://svn.apache.org/viewvc/httpd/httpd/trunk/modules/generators/mod_status.c?r1=1389564&r2=1413
http://svn.apache.org/viewvc/httpd/httpd/trunk/modules/ldap/util_ldap_cache_mgr.c?r1=1209766&r2=14
http://svn.apache.org/viewvc/httpd/httpd/trunk/modules/mappers/mod_imagemap.c?r1=1398480&r2=14
http://svn.apache.org/viewvc/httpd/httpd/trunk/modules/proxy/mod_proxy_ftp.c?r1=1404625&r2=141373
http://www.debian.org/security/2013/dsa-2637
http://www.fujitsu.com/global/support/software/security/products-f/interstage-201303e.html
http://www.oracle.com/technetwork/topics/security/cpujan2014-1972949.html
http://www.securityfocus.com/bid/58165
http://www.securityfocus.com/bid/64758

Summary

The ap_read_request function in server/protocol.c in the Apache HTTP Server 2.2.x before 2.2.15, when a multithreaded MPM is used, does not properly handle headers in subrequests in certain circumstances involving a parent request that has a body, which might allow remote attackers to obtain sensitive information via a crafted request that triggers access to memory locations associated with an earlier request.

CVE-2010-0434 Information	
CVSS Score	4.3
CWE	CWE-200
Vulnerability impact	
Confidentiality	PARTIAL
Integrity	NONE
Availability	NONE
Access methodology information	
Vector	NETWORK
Complexity	MEDIUM
Authentication	NONE

Vulnerable configs

Apache Software Foundation Apache HTTP Server
Apache Software Foundation Apache HTTP Server 2.2
Apache Software Foundation Apache HTTP Server 2.2.0
Apache Software Foundation Apache HTTP Server 2.2.1
Apache Software Foundation Apache HTTP Server 2.2.2
Apache Software Foundation Apache HTTP Server 2.2.3
Apache Software Foundation Apache HTTP Server 2.2.4
Apache Software Foundation Apache HTTP Server 2.2.6
Apache Software Foundation Apache HTTP Server 2.2.8
Apache Software Foundation Apache HTTP Server 2.2.9
Apache Software Foundation Apache HTTP Server 2.2.11
Apache Software Foundation Apache HTTP Server 2.2.12
Apache Software Foundation Apache HTTP Server 2.2.13
Apache Software Foundation Apache HTTP Server 2.2.14

References

http://httpd.apache.org/security/vulnerabilities_22.html
http://lists.apple.com/archives/security-announce/2010//Nov/msg00000.html
http://lists.fedoraproject.org/pipermail/package-announce/2010-April/039957.html
http://lists.fedoraproject.org/pipermail/package-announce/2010-May/040652.html
http://lists.opensuse.org/opensuse-security-announce/2010-04/msg00006.html

http://lists.vmware.com/pipermail/security-announce/2010/000105.html
http://marc.info/?l=bugtraq&m=127557640302499&w=2
http://support.apple.com/kb/HT4435
http://svn.apache.org/viewvc/httpd/httpd/branches/2.2.x/server/protocol.c?r1=917617&r2=917867&pathr
http://svn.apache.org/viewvc?view=revision&revision=917867
http://svn.apache.org/viewvc?view=revision&revision=918427
http://www-01.ibm.com/support/docview.wss?uid=swg1PM08939
http://www-01.ibm.com/support/docview.wss?uid=swg1PM12247
http://www-01.ibm.com/support/docview.wss?uid=swg1PM15829
http://www.debian.org/security/2010/dsa-2035
http://www.oracle.com/technetwork/topics/security/cpujuly2013-1899826.html
http://www.redhat.com/support/errata/RHSA-2010-0168.html
http://www.redhat.com/support/errata/RHSA-2010-0175.html
http://www.securityfocus.com/bid/38494
http://www.vmware.com/security/advisories/VMSA-2010-0014.html
http://www.vupen.com/english/advisories/2010/0911
http://www.vupen.com/english/advisories/2010/0994
http://www.vupen.com/english/advisories/2010/1001
http://www.vupen.com/english/advisories/2010/1057
http://www.vupen.com/english/advisories/2010/1411
https://bugzilla.redhat.com/show_bug.cgi?id=570171
https://exchange.xforce.ibmcloud.com/vulnerabilities/56625
https://issues.apache.org/bugzilla/show_bug.cgi?id=48359

Summary

Apache HTTP Server mod_cluster before version httpd 2.4.23 is vulnerable to an Improper Input Validation in the protocol parsing logic in the load balancer resulting in a Segmentation Fault in the serving httpd process.

CVE-2016-8612 Information	
CVSS Score	3.3
CWE	CWE-20

Vulnerable configs

Apache Software Foundation Apache HTTP Server
Apache Software Foundation Apache HTTP Server 0.8.11
Apache Software Foundation Apache HTTP Server 0.8.14
Apache Software Foundation Apache HTTP Server 1.0
Apache Software Foundation Apache HTTP Server 1.0.2
Apache Software Foundation Apache HTTP Server 1.0.3
Apache Software Foundation Apache HTTP Server 1.0.5
Apache Software Foundation Apache HTTP Server 1.1
Apache Software Foundation Apache HTTP Server 1.1.1
Apache Software Foundation Apache 1.2
Apache Software Foundation Apache HTTP Server 1.2.4
Apache Software Foundation Apache HTTP Server 1.2.5
Apache Software Foundation Apache HTTP Server 1.2.6
Apache Software Foundation Apache 1.29
Apache Software Foundation Apache HTTP Server 1.3
Apache Software Foundation Apache HTTP Server 1.3.0
Apache Software Foundation Apache HTTP Server 1.3.1
Apache Software Foundation Apache HTTP Server 1.3.1.1
Apache Software Foundation Apache HTTP Server 1.3.2
Apache Software Foundation Apache HTTP Server 1.3.3
Apache Software Foundation Apache HTTP Server 1.3.4
Apache Software Foundation Apache HTTP Server 1.3.5
Apache Software Foundation Apache HTTP Server 1.3.6
Apache Software Foundation Apache HTTP Server 1.3.7
Apache Software Foundation Apache HTTP Server 1.3.8
Apache Software Foundation Apache HTTP Server 1.3.9
Apache Software Foundation Apache 1.3.10
Apache Software Foundation Apache HTTP Server 1.3.11
Apache Software Foundation Apache HTTP Server 1.3.12
Apache Software Foundation Apache 1.3.13
Apache Software Foundation Apache HTTP Server 1.3.14
Apache Software Foundation Apache 1.3.15
Apache Software Foundation Apache 1.3.16
Apache Software Foundation Apache HTTP Server 1.3.17
Apache Software Foundation Apache HTTP Server 1.3.18
Apache Software Foundation Apache HTTP Server 1.3.19
Apache Software Foundation Apache HTTP Server 1.3.20
Apache Software Foundation Apache HTTP Server 1.3.22
Apache Software Foundation Apache HTTP Server 1.3.23
Apache Software Foundation Apache HTTP Server 1.3.24
Apache Software Foundation Apache HTTP Server 1.3.25
Apache Software Foundation Apache HTTP Server 1.3.26
Apache Software Foundation Apache HTTP Server 1.3.27
Apache Software Foundation Apache HTTP Server 1.3.28
Apache Software Foundation Apache HTTP Server 1.3.29
Apache Software Foundation Apache HTTP Server 1.3.30
Apache Software Foundation Apache HTTP Server 1.3.31
Apache Software Foundation Apache HTTP Server 1.3.32
Apache Software Foundation Apache HTTP Server 1.3.33
Apache Software Foundation Apache HTTP Server 1.3.34
Apache Software Foundation Apache HTTP Server 1.3.35
Apache Software Foundation Apache HTTP Server 1.3.36
Apache Software Foundation Apache HTTP Server 1.3.37
Apache Software Foundation Apache HTTP Server 1.3.38
Apache Software Foundation Apache HTTP Server 1.3.39
Apache Software Foundation Apache HTTP Server 1.3.41
Apache Software Foundation Apache HTTP Server 1.3.42
Apache Software Foundation Apache HTTP Server 1.3.65
Apache Software Foundation Apache HTTP Server 1.3.68
Apache Software Foundation Apache HTTP Server 1.4.0
Apache Software Foundation Apache HTTP Server 1.99
Apache Software Foundation Apache HTTP Server 2.0
Apache Software Foundation Apache HTTP Server 2.0.0
Apache Software Foundation Apache HTTP Server 2.0.9a
Apache Software Foundation Apache HTTP Server 2.0.28
Apache Software Foundation Apache HTTP Server 2.0.28 Beta
Apache Software Foundation Apache HTTP Server 2.0.32
Apache Software Foundation Apache HTTP Server 2.0.32 Beta
Apache Software Foundation Apache HTTP Server 2.0.34 Beta
Apache Software Foundation Apache HTTP Server 2.0.35
Apache Software Foundation Apache HTTP Server 2.0.36
Apache Software Foundation Apache HTTP Server 2.0.37
Apache Software Foundation Apache HTTP Server 2.0.38
Apache Software Foundation Apache HTTP Server 2.0.39
Apache Software Foundation Apache HTTP Server 2.0.40
Apache Software Foundation Apache HTTP Server 2.0.41
Apache Software Foundation Apache HTTP Server 2.0.42
Apache Software Foundation Apache HTTP Server 2.0.43
Apache Software Foundation Apache HTTP Server 2.0.44
Apache Software Foundation Apache HTTP Server 2.0.45
Apache Software Foundation Apache HTTP Server 2.0.46
Apache Software Foundation Apache HTTP Server 2.0.47
Apache Software Foundation Apache HTTP Server 2.0.48
Apache Software Foundation Apache HTTP Server 2.0.49
Apache Software Foundation Apache HTTP Server 2.0.50
Apache Software Foundation Apache HTTP Server 2.0.51
Apache Software Foundation Apache HTTP Server 2.0.52
Apache Software Foundation Apache HTTP Server 2.0.53
Apache Software Foundation Apache HTTP Server 2.0.54
Apache Software Foundation Apache HTTP Server 2.0.55
Apache Software Foundation Apache HTTP Server 2.0.56
Apache Software Foundation Apache HTTP Server 2.0.57
Apache Software Foundation Apache HTTP Server 2.0.58
Apache Software Foundation HTTP Server 2.0.59
Apache Software Foundation Apache HTTP Server 2.0.60 dev
Apache Software Foundation HTTP Server 2.0.61
Apache Software Foundation Apache HTTP Server 2.0.63
Apache Software Foundation Apache HTTP Server 2.0.64
Apache Software Foundation Apache HTTP Server 2.0.65
Apache Software Foundation Apache HTTP Server 2.1
Apache Software Foundation Apache HTTP Server 2.1.0
Apache Software Foundation Apache HTTP Server 2.1.1
Apache Software Foundation Apache HTTP Server 2.1.2
Apache Software Foundation Apache HTTP Server 2.1.3
Apache Software Foundation Apache HTTP Server 2.1.4
Apache Software Foundation Apache HTTP Server 2.1.5
Apache Software Foundation Apache HTTP Server 2.1.6
Apache Software Foundation Apache HTTP Server 2.1.7
Apache Software Foundation Apache HTTP Server 2.1.8
Apache Software Foundation Apache HTTP Server 2.1.9
Apache Software Foundation Apache HTTP Server 2.2
Apache Software Foundation Apache HTTP Server 2.2.0
Apache Software Foundation Apache HTTP Server 2.2.1
Apache Software Foundation Apache HTTP Server 2.2.2
Apache Software Foundation Apache HTTP Server 2.2.3
Apache Software Foundation Apache HTTP Server 2.2.4
Apache Software Foundation Apache HTTP Server
Apache Software Foundation Apache HTTP Server 2.2.6
Apache Software Foundation Apache HTTP Server 2.2.8
Apache Software Foundation Apache HTTP Server 2.2.9
Apache Software Foundation Apache HTTP Server 2.2.10
Apache Software Foundation Apache HTTP Server 2.2.11
Apache Software Foundation Apache HTTP Server 2.2.12
Apache Software Foundation Apache HTTP Server 2.2.13
Apache Software Foundation Apache HTTP Server 2.2.14
Apache Software Foundation Apache HTTP Server 2.2.15
Apache Software Foundation Apache HTTP Server 2.2.16
Apache Software Foundation Apache HTTP Server 2.2.17
Apache Software Foundation Apache HTTP Server 2.2.18
Apache Software Foundation Apache HTTP Server 2.2.19
Apache Software Foundation Apache HTTP Server 2.2.20
Apache HTTP Server 2.2.21
Apache Software Foundation Apache HTTP Server 2.2.22
Apache Software Foundation Apache HTTP Server 2.2.23
Apache Software Foundation Apache HTTP Server 2.2.24
Apache Software Foundation Apache HTTP Server 2.2.25
Apache Software Foundation Apache HTTP Server 2.2.26
Apache Software Foundation Apache HTTP Server 2.2.27
Apache Software Foundation Apache HTTP Server 2.2.29
Apache Software Foundation Apache HTTP Server 2.2.31
Apache Software Foundation Apache HTTP Server 2.2.32
Apache Software Foundation Apache HTTP Server 2.2.33
Apache Software Foundation Apache HTTP Server 2.2.34
Apache Software Foundation Apache HTTP Server 2.3.0
Apache Software Foundation Apache HTTP Server 2.3.1
Apache Software Foundation Apache HTTP Server 2.3.2
Apache Software Foundation Apache HTTP Server 2.3.3
Apache Software Foundation Apache HTTP Server 2.3.4
Apache Software Foundation Apache HTTP Server 2.3.5
Apache Software Foundation Apache HTTP Server 2.3.6
Apache Software Foundation Apache HTTP Server 2.3.7
Apache Software Foundation Apache HTTP Server 2.3.8
Apache Software Foundation Apache HTTP Server 2.3.9
Apache Software Foundation Apache HTTP Server 2.3.10
Apache Software Foundation Apache HTTP Server 2.3.11
Apache Software Foundation Apache HTTP Server 2.3.12
Apache Software Foundation Apache HTTP Server 2.3.13
Apache Software Foundation Apache HTTP Server 2.3.14
Apache Software Foundation Apache HTTP Server 2.3.15
Apache Software Foundation Apache HTTP Server 2.3.16
Apache Software Foundation Apache HTTP Server 2.4.0
Apache Software Foundation Apache HTTP Server 2.4.1
Apache Software Foundation Apache HTTP Server 2.4.2
Apache Software Foundation Apache HTTP Server 2.4.3
Apache Software Foundation Apache HTTP Server 2.4.4
Apache Software Foundation Apache HTTP Server 2.4.6
Apache Software Foundation Apache HTTP Server 2.4.7
Apache Software Foundation Apache HTTP Server 2.4.8
Apache Software Foundation Apache HTTP Server 2.4.9
Apache Software Foundation Apache HTTP Server 2.4.10
Apache Software Foundation Apache HTTP Server 2.4.12
Apache Software Foundation Apache HTTP Server 2.4.14
Apache Software Foundation Apache HTTP Server 2.4.16
Apache Software Foundation Apache HTTP Server 2.4.17
Apache Software Foundation Apache HTTP Server 2.4.18
Apache Software Foundation HTTP Server 2.4.19
Apache Software Foundation HTTP Server 2.4.20
Apache Software Foundation Apache HTTP Server 2.4.21
Apache Software Foundation Apache HTTP Server 2.4.22
cpe:2.3:o:redhat:enterprise_linux:6.0
Red Hat Enterprise Linux (RHEL) 7.0 (7)

References

http://rhn.redhat.com/errata/RHSA-2016-2957.html
http://www.securityfocus.com/bid/94939
https://access.redhat.com/errata/RHSA-2017:0193
https://access.redhat.com/errata/RHSA-2017:0194
https://bugzilla.redhat.com/show_bug.cgi?id=1387605
https://security.netapp.com/advisory/ntap-20180601-0005/

Summary

Multiple cross-site scripting (XSS) vulnerabilities in the make_variant_list function in mod_negotiation.c in the mod_negotiation module in the Apache HTTP Server 2.4.x before 2.4.3, when the MultiViews option is enabled, allow remote attackers to inject arbitrary web script or HTML via a crafted filename that is not properly handled during construction of a variant list.

CVE-2012-2687 Information	
CVSS Score	2.6
CWE	CWE-79
Vulnerability impact	
Confidentiality	NONE
Integrity	PARTIAL
Availability	NONE
Access methodology information	
Vector	NETWORK
Complexity	HIGH
Authentication	NONE

Vulnerable configs

Apache Software Foundation Apache HTTP Server 2.4.1
Apache Software Foundation Apache HTTP Server 2.4.2
Apache Software Foundation Apache HTTP Server 2.4.0
Apache Software Foundation Apache HTTP Server 2.2.22
Apache Software Foundation Apache HTTP Server 2.2.23
Apache Software Foundation Apache HTTP Server 2.2.19
Apache Software Foundation Apache HTTP Server 2.2.1
Apache Software Foundation Apache HTTP Server 2.2.16
Apache Software Foundation Apache HTTP Server 2.2.15
Apache Software Foundation Apache HTTP Server 2.2.6
Apache HTTP Server 2.2.21
Apache Software Foundation Apache HTTP Server 2.2.12
Apache Software Foundation Apache HTTP Server 2.2.2
Apache Software Foundation Apache HTTP Server 2.2.4
Apache Software Foundation Apache HTTP Server 2.2.17
Apache Software Foundation Apache HTTP Server 2.2.0
Apache Software Foundation Apache HTTP Server 2.2.18
Apache Software Foundation Apache HTTP Server 2.2.11
Apache Software Foundation Apache HTTP Server 2.2.9
Apache Software Foundation Apache HTTP Server 2.2.13
Apache Software Foundation Apache HTTP Server 2.2.10
Apache Software Foundation Apache HTTP Server 2.2.8
Apache Software Foundation Apache HTTP Server 2.2.3
Apache Software Foundation Apache HTTP Server 2.2.20
Apache Software Foundation Apache HTTP Server 2.2.14

References

http://httpd.apache.org/security/vulnerabilities_24.html
http://lists.apple.com/archives/security-announce/2013/Sep/msg00002.html
http://lists.opensuse.org/opensuse-updates/2013-02/msg00009.html
http://lists.opensuse.org/opensuse-updates/2013-02/msg00011.html

http://lists.opensuse.org/opensuse-updates/2013-02/msg00012.html
http://mail-archives.apache.org/mod_mbox/www-announce/201208.mbox/\%3C0BFFEA9B-801B-4BAA-9534-56F640268E30@apache.org\%3E
http://marc.info/?l=bugtraq&m=136612293908376&w=2
http://rhn.redhat.com/errata/RHSA-2012-1591.html
http://rhn.redhat.com/errata/RHSA-2012-1592.html
http://rhn.redhat.com/errata/RHSA-2012-1594.html
http://rhn.redhat.com/errata/RHSA-2013-0130.html
http://support.apple.com/kb/HT5880
http://www-01.ibm.com/support/docview.wss?uid=nas2a2b50a0ca011b37c86257a96003c9a4f
http://www.apache.org/dist/httpd/CHANGES_2.4.3
http://www.fujitsu.com/global/support/software/security/products-f/interstage-201303e.html
http://www.oracle.com/technetwork/topics/security/cpujuly2013-1899826.html
http://www.securityfocus.com/bid/55131
http://www.ubuntu.com/usn/USN-1627-1
http://www.xerox.com/download/security/security-bulletin/16287-4d6b7b0c81f7b/cert_XRX13-003_v1.0.pdf

Summary

The ap_pregsub function in server/util.c in the Apache HTTP Server 2.0.x through 2.0.64 and 2.2.x through 2.2.21, when the mod_setenvif module is enabled, does not restrict the size of values of environment variables, which allows local users to cause a denial of service (memory consumption or NULL pointer dereference) via a .htaccess file with a crafted SetEnvIf directive, in conjunction with a crafted HTTP request header, related to (1) the "len +=" statement and (2) the apr_pcalloc function call, a different vulnerability than CVE-2011-3607.

CVE-2011-4415 Information	
CVSS Score	1.2
CWE	CWE-20
Vulnerability impact	
Confidentiality	NONE
Integrity	NONE
Availability	PARTIAL
Access methodology information	
Vector	LOCAL
Complexity	HIGH
Authentication	NONE

Vulnerable configs

Apache Software Foundation HTTP Server 2.0.61 Apache Software Foundation Apache HTTP Server 2.0.58 Apache Software Foundation Apache HTTP Server 2.0.55
Apache Software Foundation Apache HTTP Server 2.0.54 Apache Software Foundation Apache HTTP Server 2.0.57 Apache Software Foundation Apache HTTP Server 2.0.56
Apache Software Foundation Apache HTTP Server 2.0.51 Apache Software Foundation Apache HTTP Server 2.0.50 Apache Software Foundation Apache HTTP Server 2.0.53
Apache Software Foundation Apache HTTP Server 2.0.52 Apache Software Foundation Apache HTTP Server 2.0.47 Apache Software Foundation Apache HTTP Server 2.0.46
Apache Software Foundation Apache HTTP Server 2.0.49 Apache Software Foundation Apache HTTP Server 2.0.48 Apache Software Foundation Apache HTTP Server 2.0.43
Apache Software Foundation Apache HTTP Server 2.0.42 Apache Software Foundation Apache HTTP Server 2.0.45 Apache Software Foundation Apache HTTP Server 2.0.44
Apache Software Foundation HTTP Server 2.0.59 Apache Software Foundation Apache HTTP Server 2.0.63 Apache Software Foundation Apache HTTP Server 2.0.9a
Apache Software Foundation Apache HTTP Server 2.0.60 dev Apache Software Foundation Apache HTTP Server 2.0 Apache Software Foundation Apache HTTP Server 2.0.28 Beta
Apache Software Foundation Apache HTTP Server 2.0.28 Apache Software Foundation Apache HTTP Server 2.0.32 Beta Apache Software Foundation Apache HTTP Server 2.0.32
Apache Software Foundation Apache HTTP Server 2.0.35 Apache Software Foundation Apache HTTP Server 2.0.34 Beta Apache Software Foundation Apache HTTP Server 2.0.37
Apache Software Foundation Apache HTTP Server 2.0.36 Apache Software Foundation Apache HTTP Server 2.0.39 Apache Software Foundation Apache HTTP Server 2.0.38
Apache Software Foundation Apache HTTP Server 2.0.41 Apache Software Foundation Apache HTTP Server 2.0.40 Apache Software Foundation Apache HTTP Server 2.0.64
Apache Software Foundation Apache HTTP Server 2.2.1 Apache Software Foundation Apache HTTP Server 2.2.6 Apache Software Foundation Apache HTTP Server 2.2.11
Apache Software Foundation Apache HTTP Server 2.2.9 Apache Software Foundation Apache HTTP Server 2.2.10 Apache Software Foundation Apache HTTP Server 2.2.8
Apache Software Foundation Apache HTTP Server 2.2.13 Apache Software Foundation Apache HTTP Server 2.2.3 Apache Software Foundation Apache HTTP Server 2.2.12
Apache Software Foundation Apache HTTP Server 2.2.0 Apache Software Foundation Apache HTTP Server 2.2.16 Apache Software Foundation Apache HTTP Server 2.2.15
Apache Software Foundation Apache HTTP Server 2.2.2 Apache Software Foundation Apache HTTP Server 2.2.4 Apache Software Foundation Apache HTTP Server 2.2.18
Apache Software Foundation Apache HTTP Server 2.2.14 Apache Software Foundation Apache HTTP Server 2.2.19 Apache Software Foundation Apache HTTP Server 2.2.20
Apache HTTP Server 2.2.21

References

http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=c03360041
http://www.gossamer-threads.com/lists/apache/dev/403775
http://www.halfdog.net/Security/2011/ApacheModSetEnvIfIntegerOverflow/
http://www.halfdog.net/Security/2011/ApacheModSetEnvIfIntegerOverflow/DemoExploit.html

Summary

modules/arch/win32/mod_isapi.c in mod_isapi in the Apache HTTP Server 2.0.37 through 2.0.63, 2.2.0 through 2.2.14, and 2.3.x before 2.3.7, when running on Windows, does not ensure that request processing is complete before calling isapi_unload for an ISAPI .dll module, which allows remote attackers to execute arbitrary code via unspecified vectors related to a crafted request, a reset packet, and "orphaned callback pointers."

CVE-2010-0425 Information	
CVSS Score	10.0
CWE	Unknown
Vulnerability impact	
Confidentiality	COMPLETE
Integrity	COMPLETE
Availability	COMPLETE
Access methodology information	
Vector	NETWORK
Complexity	LOW
Authentication	NONE

Vulnerable configs

Apache Software Foundation Apache HTTP Server 2.3.0		Apache Software Foundation Apache HTTP Server 2.3.1
Apache Software Foundation Apache HTTP Server 2.3.2	Apache Software Foundation Apache HTTP Server 2.3.3	Apache Software Foundation Apache HTTP Server 2.3.4
Apache Software Foundation Apache HTTP Server 2.3.5	Apache Software Foundation Apache HTTP Server 2.3.6	Microsoft Windows
Apache Software Foundation Apache HTTP Server 2.0.9a	Apache Software Foundation Apache HTTP Server 2.0.28	Apache Software Foundation Apache HTTP Server 2.0.28 Beta
Apache Software Foundation Apache HTTP Server 2.0.32	Apache Software Foundation Apache HTTP Server 2.0.32 Beta	Apache Software Foundation Apache HTTP Server 2.0.34 Beta
Apache Software Foundation Apache HTTP Server 2.0.35	Apache Software Foundation Apache HTTP Server 2.0.36	Apache Software Foundation Apache HTTP Server 2.0.37
Apache Software Foundation Apache HTTP Server 2.0.38	Apache Software Foundation Apache HTTP Server 2.0.39	Apache Software Foundation Apache HTTP Server 2.0.40
Apache Software Foundation Apache HTTP Server 2.0.41	Apache Software Foundation Apache HTTP Server 2.0.42	Apache Software Foundation Apache HTTP Server 2.0.43
Apache Software Foundation Apache HTTP Server 2.0.44	Apache Software Foundation Apache HTTP Server 2.0.45	Apache Software Foundation Apache HTTP Server 2.0.46
Apache Software Foundation Apache HTTP Server 2.0.47	Apache Software Foundation Apache HTTP Server 2.0.48	Apache Software Foundation Apache HTTP Server 2.0.49
Apache Software Foundation Apache HTTP Server 2.0.50	Apache Software Foundation Apache HTTP Server 2.0.51	Apache Software Foundation Apache HTTP Server 2.0.52
Apache Software Foundation Apache HTTP Server 2.0.53	Apache Software Foundation Apache HTTP Server 2.0.54	Apache Software Foundation Apache HTTP Server 2.0.55
Apache Software Foundation Apache HTTP Server 2.0.56	Apache Software Foundation Apache HTTP Server 2.0.57	Apache Software Foundation Apache HTTP Server 2.0.58
Apache Software Foundation HTTP Server 2.0.59	Apache Software Foundation Apache HTTP Server 2.0.60 dev	Apache Software Foundation HTTP Server 2.0.61
Apache Software Foundation Apache HTTP Server 2.0.63	Microsoft Windows	Apache Software Foundation Apache HTTP Server
Apache Software Foundation Apache HTTP Server 2.2.0	Apache Software Foundation Apache HTTP Server 2.2.1	Apache Software Foundation Apache HTTP Server 2.2.2
Apache Software Foundation Apache HTTP Server 2.2.3	Apache Software Foundation Apache HTTP Server 2.2.4	Apache Software Foundation Apache HTTP Server 2.2.6
cpe:2.3:a:apache:http_server:2.2.7	Apache Software Foundation Apache HTTP Server 2.2.8	Apache Software Foundation Apache HTTP Server 2.2.9
Apache Software Foundation Apache HTTP Server 2.2.10	Apache Software Foundation Apache HTTP Server 2.2.11	Apache Software Foundation Apache HTTP Server 2.2.12
Apache Software Foundation Apache HTTP Server 2.2.13	Apache Software Foundation Apache HTTP Server 2.2.14	Microsoft Windows

References

http://httpd.apache.org/security/vulnerabilities_20.html
http://httpd.apache.org/security/vulnerabilities_22.html
http://lists.vmware.com/pipermail/security-announce/2010/000105.html
http://svn.apache.org/viewvc/httpd/httpd/trunk/CHANGES?r1=917870&r2=917869&pathrev=917870
http://svn.apache.org/viewvc/httpd/httpd/trunk/modules/arch/win32/mod_isapi.c?r1=917870&r2=917869
http://svn.apache.org/viewvc?view=revision&revision=917870
http://www-01.ibm.com/support/docview.wss?uid=swg1PM09447
http://www-01.ibm.com/support/docview.wss?uid=swg1PM12247
http://www.kb.cert.org/vuls/id/280613
http://www.oracle.com/technetwork/topics/security/cpujuly2013-1899826.html
http://www.securityfocus.com/bid/38494
http://www.securitytracker.com/id?1023701
http://www.senseofsecurity.com.au/advisories/SOS-10-002
http://www.vmware.com/security/advisories/VMSA-2010-0014.html
http://www.vupen.com/english/advisories/2010/0634
http://www.vupen.com/english/advisories/2010/0994
https://exchange.xforce.ibmcloud.com/vulnerabilities/56624

Summary

The byterange filter in the Apache HTTP Server 1.3.x, 2.0.x through 2.0.64, and 2.2.x through 2.2.19 allows remote attackers to cause a denial of service (memory and CPU consumption) via a Range header that expresses multiple overlapping ranges, as exploited in the wild in August 2011, a different vulnerability than CVE-2007-0086.

CVE-2011-3192 Information	
CVSS Score	7.8
CWE	CWE-399
Vulnerability impact	
Confidentiality	NONE
Integrity	NONE
Availability	COMPLETE
Access methodology information	
Vector	NETWORK
Complexity	LOW
Authentication	NONE

Vulnerable configs

Apache Software Foundation Apache HTTP Server 1.3 Apache Software Foundation Apache HTTP Server 1.3.0 Apache Software Foundation Apache HTTP Server 1.3.1
Apache Software Foundation Apache HTTP Server 1.3.1.1 Apache Software Foundation Apache HTTP Server 1.3.2 Apache Software Foundation Apache HTTP Server 1.3.3
Apache Software Foundation Apache HTTP Server 1.3.4 Apache Software Foundation Apache HTTP Server 1.3.5 Apache Software Foundation Apache HTTP Server 1.3.6
Apache Software Foundation Apache HTTP Server 1.3.7 Apache Software Foundation Apache HTTP Server 1.3.8 Apache Software Foundation Apache HTTP Server 1.3.9
Apache Software Foundation Apache 1.3.10 Apache Software Foundation Apache HTTP Server 1.3.11 Apache Software Foundation Apache HTTP Server 1.3.12
Apache Software Foundation Apache 1.3.13 Apache Software Foundation Apache HTTP Server 1.3.14 Apache Software Foundation Apache 1.3.15
Apache Software Foundation Apache 1.3.16 Apache Software Foundation Apache HTTP Server 1.3.17 Apache Software Foundation Apache HTTP Server 1.3.18
Apache Software Foundation Apache HTTP Server 1.3.19 Apache Software Foundation Apache HTTP Server 1.3.20 Apache Software Foundation Apache HTTP Server 1.3.22
Apache Software Foundation Apache HTTP Server 1.3.23 Apache Software Foundation Apache HTTP Server 1.3.24 Apache Software Foundation Apache HTTP Server 1.3.25
Apache Software Foundation Apache HTTP Server 1.3.26 Apache Software Foundation Apache HTTP Server 1.3.27 Apache Software Foundation Apache HTTP Server 1.3.28
Apache Software Foundation Apache HTTP Server 1.3.29 Apache Software Foundation Apache HTTP Server 1.3.30 Apache Software Foundation Apache HTTP Server 1.3.31
Apache Software Foundation Apache HTTP Server 1.3.32 Apache Software Foundation Apache HTTP Server 1.3.33 Apache Software Foundation Apache HTTP Server 1.3.34
Apache Software Foundation Apache HTTP Server 1.3.35 Apache Software Foundation Apache HTTP Server 1.3.36 Apache Software Foundation Apache HTTP Server 1.3.37
Apache Software Foundation Apache HTTP Server 1.3.38 Apache Software Foundation Apache HTTP Server 1.3.39 Apache Software Foundation Apache HTTP Server 1.3.41
Apache Software Foundation Apache HTTP Server 1.3.42 Apache Software Foundation Apache HTTP Server 1.3.65 Apache Software Foundation Apache HTTP Server 1.3.68
Apache Software Foundation Apache HTTP Server 2.0 Apache Software Foundation Apache HTTP Server 2.0.9a Apache Software Foundation Apache HTTP Server 2.0.28
Apache Software Foundation Apache HTTP Server 2.0.28 Beta Apache Software Foundation Apache HTTP Server 2.0.32 Apache Software Foundation Apache HTTP Server 2.0.32 Beta
Apache Software Foundation Apache HTTP Server 2.0.34 Beta Apache Software Foundation Apache HTTP Server 2.0.35 Apache Software Foundation Apache HTTP Server 2.0.36
Apache Software Foundation Apache HTTP Server 2.0.37 Apache Software Foundation Apache HTTP Server 2.0.38 Apache Software Foundation Apache HTTP Server 2.0.39
Apache Software Foundation Apache HTTP Server 2.0.40 Apache Software Foundation Apache HTTP Server 2.0.41 Apache Software Foundation Apache HTTP Server 2.0.42
Apache Software Foundation Apache HTTP Server 2.0.43 Apache Software Foundation Apache HTTP Server 2.0.44 Apache Software Foundation Apache HTTP Server 2.0.45
Apache Software Foundation Apache HTTP Server 2.0.46 Apache Software Foundation Apache HTTP Server 2.0.47 Apache Software Foundation Apache HTTP Server 2.0.48
Apache Software Foundation Apache HTTP Server 2.0.49 Apache Software Foundation Apache HTTP Server 2.0.50 Apache Software Foundation Apache HTTP Server 2.0.51
Apache Software Foundation Apache HTTP Server 2.0.52 Apache Software Foundation Apache HTTP Server 2.0.53 Apache Software Foundation Apache HTTP Server 2.0.54
Apache Software Foundation Apache HTTP Server 2.0.55 Apache Software Foundation Apache HTTP Server 2.0.56 Apache Software Foundation Apache HTTP Server 2.0.57
Apache Software Foundation Apache HTTP Server 2.0.58 Apache Software Foundation HTTP Server 2.0.59 Apache Software Foundation Apache HTTP Server 2.0.60 dev
Apache Software Foundation HTTP Server 2.0.61 Apache Software Foundation Apache HTTP Server 2.0.63 Apache Software Foundation Apache HTTP Server 2.0.64
Apache Software Foundation Apache HTTP Server 2.2.0 Apache Software Foundation Apache HTTP Server 2.2.1 Apache Software Foundation Apache HTTP Server 2.2.2
Apache Software Foundation Apache HTTP Server 2.2.3 Apache Software Foundation Apache HTTP Server 2.2.4 Apache Software Foundation Apache HTTP Server 2.2.6

Apache Software Foundation Apache HTTP Server 2.2.8
Apache Software Foundation Apache HTTP Server 2.2.9
Apache Software Foundation Apache HTTP Server 2.2.10
Apache Software Foundation Apache HTTP Server 2.2.11
Apache Software Foundation Apache HTTP Server 2.2.12
Apache Software Foundation Apache HTTP Server 2.2.13
Apache Software Foundation Apache HTTP Server 2.2.14
Apache Software Foundation Apache HTTP Server 2.2.15
Apache Software Foundation Apache HTTP Server 2.2.16
Apache Software Foundation Apache HTTP Server 2.2.18
Apache Software Foundation Apache HTTP Server 2.2.19

References

http://archives.neohapsis.com/archives/fulldisclosure/2011-08/0285.html
http://blogs.oracle.com/security/entry/security_alert_for_cve_2011
http://lists.apple.com/archives/Security-announce/2011//Oct/msg00003.html
http://lists.opensuse.org/opensuse-security-announce/2011-09/msg00006.html
http://lists.opensuse.org/opensuse-security-announce/2011-09/msg00009.html
http://lists.opensuse.org/opensuse-security-announce/2011-09/msg00010.html
http://lists.opensuse.org/opensuse-security-announce/2011-09/msg00011.html
http://lists.opensuse.org/opensuse-security-announce/2011-11/msg00008.html
http://lists.opensuse.org/opensuse-security-announce/2011-11/msg00011.html
http://mail-archives.apache.org/mod_mbox/httpd-announce/201108.mbox/\%3c20110824161640.122D38
http://mail-archives.apache.org/mod_mbox/httpd-dev/201108.mbox/\%3cCAAPSnn2PO-d-C4nQt_TES2RRWiZr7urefhTKPWBC1b+K1Dqc7g@mail.gmail.com\%3e
http://marc.info/?l=bugtraq&m=131551295528105&w=2
http://marc.info/?l=bugtraq&m=131731002122529&w=2
http://marc.info/?l=bugtraq&m=132033751509019&w=2
http://marc.info/?l=bugtraq&m=133477473521382&w=2
http://marc.info/?l=bugtraq&m=133951357207000&w=2
http://marc.info/?l=bugtraq&m=134987041210674&w=2
http://seclists.org/fulldisclosure/2011/Aug/175
http://securitytracker.com/id?1025960
http://support.apple.com/kb/HT5002
http://www.apache.org/dist/httpd/Announcement2.2.html
http://www.cisco.com/en/US/products/products_security_advisory09186a0080b90d73.shtml
http://www.exploit-db.com/exploits/17696
http://www.gossamer-threads.com/lists/apache/dev/401638
http://www.kb.cert.org/vuls/id/405811
http://www.mandriva.com/security/advisories?name=MDVSA-2011:130
http://www.mandriva.com/security/advisories?name=MDVSA-2013:150
http://www.oracle.com/technetwork/topics/security/alert-cve-2011-3192-485304.html
http://www.oracle.com/technetwork/topics/security/cpujan2012-366304.html

http://www.oracle.com/technetwork/topics/security/cpujul2012-392727.html
http://www.oracle.com/technetwork/topics/security/cpuoct2011-330135.html
http://www.redhat.com/support/errata/RHSA-2011-1245.html
http://www.redhat.com/support/errata/RHSA-2011-1294.html
http://www.redhat.com/support/errata/RHSA-2011-1300.html
http://www.redhat.com/support/errata/RHSA-2011-1329.html
http://www.redhat.com/support/errata/RHSA-2011-1330.html
http://www.redhat.com/support/errata/RHSA-2011-1369.html
http://www.securityfocus.com/bid/49303
http://www.ubuntu.com/usn/USN-1199-1
https://bugzilla.redhat.com/show_bug.cgi?id=732928
https://exchange.xforce.ibmcloud.com/vulnerabilities/69396
https://help.ecostruxureit.com/display/public/UADCE725/Security+fixes+in+StruxureWare+Data+Center+
https://issues.apache.org/bugzilla/show_bug.cgi?id=51714

Summary

mod_session_dbd.c in the mod_session_dbd module in the Apache HTTP Server before 2.4.5 proceeds with save operations for a session without considering the dirty flag and the requirement for a new session ID, which has unspecified impact and remote attack vectors.

CVE-2013-2249 Information	
CVSS Score	7.5
CWE	Vulnerability impact
Confidentiality	PARTIAL
Integrity	PARTIAL
Availability	PARTIAL
Access methodology information	
Vector	NETWORK
Complexity	LOW
Authentication	NONE

Vulnerable configs

Apache Software Foundation Apache HTTP Server 1.3.35
Apache Software Foundation Apache HTTP Server 1.3.20 | Apache Software Foundation Apache HTTP Server 1.3.34 | Apache Software Foundation Apache HTTP Server 1.3.36
Apache Software Foundation Apache HTTP Server 2.1.1 | Apache Software Foundation Apache HTTP Server 2.1.2 | Apache Software Foundation Apache HTTP Server 1.3.39
Apache Software Foundation HTTP Server 2.0.61 | Apache Software Foundation Apache HTTP Server 2.0.58 | Apache Software Foundation Apache HTTP Server 2.1
Apache Software Foundation Apache HTTP Server 2.0.55 | Apache Software Foundation Apache HTTP Server 2.0.54 | Apache Software Foundation Apache HTTP Server 2.0.57
Apache Software Foundation Apache HTTP Server 2.0.56 | Apache Software Foundation Apache HTTP Server 2.0.51 | Apache Software Foundation Apache HTTP Server 2.0.50
Apache Software Foundation Apache HTTP Server 2.0.53 | Apache Software Foundation Apache HTTP Server 2.0.52 | Apache Software Foundation Apache HTTP Server 2.0.47
Apache Software Foundation Apache HTTP Server 2.0.46 | Apache Software Foundation Apache HTTP Server 2.0.49 | Apache Software Foundation Apache HTTP Server 2.0.48
Apache Software Foundation Apache HTTP Server 2.0.43 | Apache Software Foundation Apache HTTP Server 1.3.19 | Apache Software Foundation Apache HTTP Server 2.0.42
Apache Software Foundation Apache HTTP Server 1.3.18 | Apache Software Foundation Apache HTTP Server 2.0.45 | Apache Software Foundation Apache HTTP Server 1.3.17
Apache Software Foundation Apache HTTP Server 2.0.44 | Apache Software Foundation Apache HTTP Server 1.3.14 | Apache Software Foundation Apache HTTP Server 1.3.41
Apache Software Foundation Apache HTTP Server 1.3.0 | Apache Software Foundation Apache HTTP Server 1.3.38 | Apache Software Foundation Apache HTTP Server 2.0.63
Apache Software Foundation Apache HTTP Server 1.3.24 | Apache Software Foundation Apache HTTP Server 1.3.25 | Apache Software Foundation Apache HTTP Server 1.3.22
Apache Software Foundation Apache HTTP Server 1.3.23 | Apache Software Foundation Apache HTTP Server 2.0.64 | Apache Software Foundation Apache HTTP Server 1.3.27
Apache Software Foundation Apache HTTP Server 1.3.26 | Apache Software Foundation Apache HTTP Server 1.3.42 | Apache Software Foundation Apache HTTP Server 1.3.2
Apache Software Foundation Apache 1.3.10 | Apache Software Foundation Apache 1.29 | Apache Software Foundation Apache 1.2
Apache Software Foundation Apache 1.3.16 | Apache Software Foundation Apache 1.3.15 | Apache Software Foundation Apache 1.3.13
Apache Software Foundation Apache HTTP Server 1.3.37 | Apache Software Foundation HTTP Server 2.0.59 | Apache Software Foundation Apache HTTP Server 2.0.9a
Apache Software Foundation Apache HTTP Server 2.0.60 dev | Apache Software Foundation Apache HTTP Server 1.0 | Apache Software Foundation Apache HTTP Server 0.8.14
Apache Software Foundation Apache HTTP Server 0.8.11 | Apache Software Foundation Apache HTTP Server 1.1 | Apache Software Foundation Apache HTTP Server 1.0.5
Apache Software Foundation Apache HTTP Server 1.0.3 | Apache Software Foundation Apache HTTP Server 1.0.2 | Apache Software Foundation Apache HTTP Server 1.1.1
Apache Software Foundation Apache HTTP Server 1.2.5 | Apache Software Foundation Apache HTTP Server 1.3.65 | Apache Software Foundation Apache HTTP Server 1.3.1
Apache Software Foundation Apache HTTP Server 1.3.11 | Apache Software Foundation Apache HTTP Server 1.99 | Apache Software Foundation Apache HTTP Server 1.3.12
Apache Software Foundation Apache HTTP Server 1.3.68 | Apache Software Foundation Apache HTTP Server 1.3.28 | Apache Software Foundation Apache HTTP Server 1.3.29
Apache Software Foundation Apache HTTP Server 1.3.3 | Apache Software Foundation Apache HTTP Server 1.3.30 | Apache Software Foundation Apache HTTP Server 1.3.31
Apache Software Foundation Apache HTTP Server 1.3 | Apache Software Foundation Apache HTTP Server 1.3.32 | Apache Software Foundation Apache HTTP Server 1.2.4
Apache Software Foundation Apache HTTP Server 1.3.33 | Apache Software Foundation Apache HTTP Server 1.3.1.1 | Apache Software Foundation Apache HTTP Server 1.3.4
Apache Software Foundation Apache HTTP Server 1.2.6 | Apache Software Foundation Apache HTTP Server 1.3.5 | Apache Software Foundation Apache HTTP Server 1.4.0
Apache Software Foundation Apache HTTP Server 1.3.6 | Apache Software Foundation Apache HTTP Server 1.3.8 | Apache Software Foundation Apache HTTP Server 1.3.7
Apache Software Foundation Apache HTTP Server 2.0 | Apache Software Foundation Apache HTTP Server 1.3.9 | Apache Software Foundation Apache HTTP Server 2.0.28 Beta
Apache Software Foundation Apache HTTP Server 2.0.28 | Apache Software Foundation Apache HTTP Server 2.0.32 Beta | Apache Software Foundation Apache HTTP Server 2.0.32
Apache Software Foundation Apache HTTP Server 2.0.35 | Apache Software Foundation Apache HTTP Server 2.0.34 Beta | Apache Software Foundation Apache HTTP Server 2.0.37
Apache Software Foundation Apache HTTP Server 2.0.36 | Apache Software Foundation Apache HTTP Server 2.0.39 | Apache Software Foundation Apache HTTP Server 2.0.38
Apache Software Foundation Apache HTTP Server 2.0.41 | Apache Software Foundation Apache HTTP Server 2.0.40 | Apache Software Foundation Apache HTTP Server 2.1.5
Apache Software Foundation Apache HTTP Server 2.1.6 | Apache Software Foundation Apache HTTP Server 2.2 | Apache Software Foundation Apache HTTP Server 2.2.1
Apache Software Foundation Apache HTTP Server 2.1.3 | Apache Software Foundation Apache HTTP Server 2.2.6 | Apache Software Foundation Apache HTTP Server 2.1.4

Apache Software Foundation Apache HTTP Server 2.2.11
Apache Software Foundation Apache HTTP Server 2.2.9
Apache Software Foundation Apache HTTP Server 2.2.10
Apache Software Foundation Apache HTTP Server 2.2.8
Apache Software Foundation Apache HTTP Server 2.2.13
Apache Software Foundation Apache HTTP Server 2.3.0
Apache Software Foundation Apache HTTP Server 2.2.19
Apache Software Foundation Apache HTTP Server 2.3.4
Apache Software Foundation Apache HTTP Server 2.3.3
Apache Software Foundation Apache HTTP Server 2.3.5
Apache Software Foundation Apache HTTP Server 2.2.20
Apache Software Foundation Apache HTTP Server 2.2.16
Apache Software Foundation Apache HTTP Server 2.3.6
Apache Software Foundation Apache HTTP Server 2.2.15
Apache Software Foundation Apache HTTP Server 2.2.18
Apache Software Foundation Apache HTTP Server 2.2.14
Apache Software Foundation Apache HTTP Server 2.2.22
Apache Software Foundation Apache HTTP Server 2.2.23
Apache Software Foundation Apache HTTP Server 2.4.3
Apache Software Foundation Apache HTTP Server 2.3.2
Apache Software Foundation Apache HTTP Server 2.3.1
Apache Software Foundation Apache HTTP Server 2.2.3
Apache Software Foundation Apache HTTP Server 2.2.25
Apache Software Foundation Apache HTTP Server 2.2.24
Apache Software Foundation Apache HTTP Server 2.1.7
Apache Software Foundation Apache HTTP Server 2.1.8
Apache Software Foundation Apache HTTP Server 2.2.12
Apache Software Foundation Apache HTTP Server 2.2.0
Apache Software Foundation Apache HTTP Server 2.4.2
Apache Software Foundation Apache HTTP Server 2.3.16
Apache Software Foundation Apache HTTP Server 2.4.0
Apache Software Foundation Apache HTTP Server 2.3.14
Apache Software Foundation Apache HTTP Server 2.3.15
Apache Software Foundation Apache HTTP Server 2.3.12
Apache Software Foundation Apache HTTP Server 2.3.13
Apache Software Foundation Apache HTTP Server 2.3.10
Apache Software Foundation Apache HTTP Server 2.3.11
Apache Software Foundation Apache HTTP Server 2.3.8
Apache HTTP Server 2.2.21
Apache Software Foundation Apache HTTP Server 2.3.9
Apache Software Foundation Apache HTTP Server 2.2.2
Apache Software Foundation Apache HTTP Server 2.1.9
Apache Software Foundation Apache HTTP Server 2.3.7
Apache Software Foundation Apache HTTP Server 2.2.4
Apache Software Foundation Apache HTTP Server 2.2.17
Apache Software Foundation Apache HTTP Server 2.4.1
Apache Software Foundation Apache HTTP Server 2.4.4
Juniper JUNOS Space 15.1 R1

References

http://kb.juniper.net/InfoCenter/index?page=content&id=JSA10698

http://svn.apache.org/viewvc/httpd/httpd/trunk/modules/session/mod_session_dbd.c?r1=1409170&r2=14

http://tools.cisco.com/security/center/content/CiscoSecurityNotice/CVE-2013-2249

http://www.apache.org/dist/httpd/CHANGES_2.4.6

https://httpd.apache.org/security/vulnerabilities_24.html

Summary

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.

CVE-2017-7679 Information	
CVSS Score	7.5
CWE	CWE-119

Vulnerable configs

Apache Software Foundation Apache HTTP Server 2.2.0
Apache Software Foundation Apache HTTP Server 2.2.1
Apache Software Foundation Apache HTTP Server 2.2.2
Apache Software Foundation Apache HTTP Server 2.2.3
Apache Software Foundation Apache HTTP Server 2.2.4
Apache Software Foundation Apache HTTP Server
Apache Software Foundation Apache HTTP Server 2.2.6
Apache Software Foundation Apache HTTP Server 2.2.8
Apache Software Foundation Apache HTTP Server 2.2.9
Apache Software Foundation Apache HTTP Server 2.2.10
Apache Software Foundation Apache HTTP Server 2.2.11
Apache Software Foundation Apache HTTP Server 2.2.12
Apache Software Foundation Apache HTTP Server 2.2.13
Apache Software Foundation Apache HTTP Server 2.2.14
Apache Software Foundation Apache HTTP Server 2.2.15
Apache Software Foundation Apache HTTP Server 2.2.16
Apache Software Foundation Apache HTTP Server 2.2.17
Apache Software Foundation Apache HTTP Server 2.2.18
Apache Software Foundation Apache HTTP Server 2.2.19
Apache Software Foundation Apache HTTP Server 2.2.20
Apache Software Foundation Apache HTTP Server 2.2.21
Apache Software Foundation Apache HTTP Server 2.2.22
Apache Software Foundation Apache HTTP Server 2.2.23
Apache Software Foundation Apache HTTP Server 2.2.24
Apache Software Foundation Apache HTTP Server 2.2.25
Apache Software Foundation Apache HTTP Server 2.2.26
Apache Software Foundation Apache HTTP Server 2.2.27
Apache Software Foundation Apache HTTP Server 2.2.29
Apache Software Foundation Apache HTTP Server 2.2.31
Apache Software Foundation Apache HTTP Server 2.2.32
Apache Software Foundation Apache HTTP Server 2.4.0
Apache Software Foundation Apache HTTP Server 2.4.1
Apache Software Foundation Apache HTTP Server 2.4.2
Apache Software Foundation Apache HTTP Server 2.4.3
Apache Software Foundation Apache HTTP Server 2.4.4
Apache Software Foundation Apache HTTP Server 2.4.6
Apache Software Foundation Apache HTTP Server 2.4.7
Apache Software Foundation Apache HTTP Server 2.4.8
Apache Software Foundation Apache HTTP Server 2.4.9
Apache Software Foundation Apache HTTP Server 2.4.10
Apache Software Foundation Apache HTTP Server 2.4.12
Apache Software Foundation Apache HTTP Server 2.4.14
Apache Software Foundation Apache HTTP Server 2.4.16
Apache Software Foundation Apache HTTP Server 2.4.17
Apache Software Foundation Apache HTTP Server 2.4.18
Apache Software Foundation HTTP Server 2.4.19
Apache Software Foundation HTTP Server 2.4.20
Apache Software Foundation Apache HTTP Server 2.4.21
Apache Software Foundation Apache HTTP Server 2.4.22
Apache Software Foundation HTTP Server 2.4.23
Apache Software Foundation HTTP Server 2.4.24
Apache Software Foundation Apache HTTP Server 2.4.25

References

http://www.debian.org/security/2017/dsa-3896
http://www.oracle.com/technetwork/security-advisory/cpuoct2017-3236626.html
http://www.securityfocus.com/bid/99170
http://www.securitytracker.com/id/1038711
https://access.redhat.com/errata/RHSA-2017:2478
https://access.redhat.com/errata/RHSA-2017:2479
https://access.redhat.com/errata/RHSA-2017:2483
https://access.redhat.com/errata/RHSA-2017:3193
https://access.redhat.com/errata/RHSA-2017:3194
https://access.redhat.com/errata/RHSA-2017:3195
https://access.redhat.com/errata/RHSA-2017:3475
https://access.redhat.com/errata/RHSA-2017:3476
https://access.redhat.com/errata/RHSA-2017:3477
https://github.com/gottburgm/Exploits/tree/master/CVE-2017-7679
https://lists.apache.org/thread.html/f4515e580dfb6eeca589a5cdebd4c4c709ce632b12924f343c3b7751@\%3

https://security.gentoo.org/glsa/201710-32
https://security.netapp.com/advisory/ntap-20180601-0002/
https://support.apple.com/HT208221
https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf03821en_us
https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbux03908en_us
https://www.nomachine.com/SU08O00185

Summary

The stream_reqbody_cl function in mod_proxy_http.c in the mod_proxy module in the Apache HTTP Server before 2.3.3, when a reverse proxy is configured, does not properly handle an amount of streamed data that exceeds the Content-Length value, which allows remote attackers to cause a denial of service (CPU consumption) via crafted requests.

CVE-2009-1890 Information	
CVSS Score	7.1
CWE	CWE-189
Vulnerability impact	
Confidentiality	NONE
Integrity	NONE
Availability	COMPLETE
Access methodology information	
Vector	NETWORK
Complexity	MEDIUM
Authentication	NONE

Vulnerable configs

cpe:2.3:a:apache:http_server:-:win32		Apache Software Foundation Apache HTTP Server
Apache Software Foundation Apache HTTP Server 0.8.11	Apache Software Foundation Apache HTTP Server 0.8.14	Apache Software Foundation Apache HTTP Server 1.0
Apache Software Foundation Apache HTTP Server 1.0.2	Apache Software Foundation Apache HTTP Server 1.0.3	Apache Software Foundation Apache HTTP Server 1.0.5
Apache Software Foundation Apache HTTP Server 1.1	Apache Software Foundation Apache HTTP Server 1.1.1	Apache Software Foundation Apache 1.2
Apache Software Foundation Apache HTTP Server 1.2.4	Apache Software Foundation Apache HTTP Server 1.2.5	Apache Software Foundation Apache HTTP Server 1.2.6
Apache Software Foundation Apache 1.29	Apache Software Foundation Apache HTTP Server 1.3	Apache Software Foundation Apache HTTP Server 1.3.0
Apache Software Foundation Apache HTTP Server 1.3.1	Apache Software Foundation Apache HTTP Server 1.3.1.1	Apache Software Foundation Apache HTTP Server 1.3.2
Apache Software Foundation Apache HTTP Server 1.3.3	Apache Software Foundation Apache HTTP Server 1.3.4	Apache Software Foundation Apache HTTP Server 1.3.5
Apache Software Foundation Apache HTTP Server 1.3.6	cpe:2.3:a:apache:http_server:1.3.6:-:win32	Apache Software Foundation Apache HTTP Server 1.3.7
cpe:2.3:a:apache:http_server:1.3.7:-:dev	Apache Software Foundation Apache HTTP Server 1.3.8	Apache Software Foundation Apache HTTP Server 1.3.9
cpe:2.3:a:apache:http_server:1.3.9:-:win32	Apache Software Foundation Apache 1.3.10	Apache Software Foundation Apache HTTP Server 1.3.11
cpe:2.3:a:apache:http_server:1.3.11:-:win32	Apache Software Foundation Apache HTTP Server 1.3.12	cpe:2.3:a:apache:http_server:1.3.12:-:win32
Apache Software Foundation Apache 1.3.13	cpe:2.3:a:apache:http_server:1.3.13:-:win32	Apache Software Foundation Apache HTTP Server 1.3.14
cpe:2.3:a:apache:http_server:1.3.14:-:mac_os	cpe:2.3:a:apache:http_server:1.3.14:-:win32	Apache Software Foundation Apache 1.3.15
cpe:2.3:a:apache:http_server:1.3.15:-:win32	Apache Software Foundation Apache 1.3.16	cpe:2.3:a:apache:http_server:1.3.16:-:win32
Apache Software Foundation Apache HTTP Server 1.3.17	cpe:2.3:a:apache:http_server:1.3.17:-:win32	Apache Software Foundation Apache HTTP Server 1.3.18
cpe:2.3:a:apache:http_server:1.3.18:-:win32	Apache Software Foundation Apache HTTP Server 1.3.19	cpe:2.3:a:apache:http_server:1.3.19:-:win32
Apache Software Foundation Apache HTTP Server 1.3.20	cpe:2.3:a:apache:http_server:1.3.20:-:win32	Apache Software Foundation Apache HTTP Server 1.3.22
cpe:2.3:a:apache:http_server:1.3.22:-:win32	Apache Software Foundation Apache HTTP Server 1.3.23	cpe:2.3:a:apache:http_server:1.3.23:-:win32
Apache Software Foundation Apache HTTP Server 1.3.24	cpe:2.3:a:apache:http_server:1.3.24:-:win32	Apache Software Foundation Apache HTTP Server 1.3.25
cpe:2.3:a:apache:http_server:1.3.25:-:win32	Apache Software Foundation Apache HTTP Server 1.3.26	cpe:2.3:a:apache:http_server:1.3.26:-:win32
Apache Software Foundation Apache HTTP Server 1.3.27	Apache Software Foundation Apache HTTP Server 1.3.28	Apache Software Foundation Apache HTTP Server 1.3.29
Apache Software Foundation Apache HTTP Server 1.3.30	Apache Software Foundation Apache HTTP Server 1.3.31	Apache Software Foundation Apache HTTP Server 1.3.32
Apache Software Foundation Apache HTTP Server 1.3.33	Apache Software Foundation Apache HTTP Server 1.3.34	Apache Software Foundation Apache HTTP Server 1.3.35
Apache Software Foundation Apache HTTP Server 1.3.36	Apache Software Foundation Apache HTTP Server 1.3.37	Apache Software Foundation Apache HTTP Server 1.3.38
Apache Software Foundation Apache HTTP Server 1.3.39	Apache Software Foundation Apache HTTP Server 1.3.65	Apache Software Foundation Apache HTTP Server 1.3.68
Apache Software Foundation Apache HTTP Server 1.4.0	Apache Software Foundation Apache HTTP Server 1.99	Apache Software Foundation Apache HTTP Server 2.0
Apache Software Foundation Apache HTTP Server 2.0.9a	Apache Software Foundation Apache HTTP Server 2.0.28	Apache Software Foundation Apache HTTP Server 2.0.28 Beta
cpe:2.3:a:apache:http_server:2.0.28:beta:win32	Apache Software Foundation Apache HTTP Server 2.0.32	Apache Software Foundation Apache HTTP Server 2.0.32 Beta
cpe:2.3:a:apache:http_server:2.0.32:beta:win32	Apache Software Foundation Apache HTTP Server 2.0.34 Beta	cpe:2.3:a:apache:http_server:2.0.34:beta:win32

Apache Software Foundation Apache HTTP Server 2.0.35 Apache Software Foundation Apache HTTP Server 2.0.36 Apache Software Foundation Apache HTTP Server 2.0.37
Apache Software Foundation Apache HTTP Server 2.0.38 Apache Software Foundation Apache HTTP Server 2.0.39 Apache Software Foundation Apache HTTP Server 2.0.40
Apache Software Foundation Apache HTTP Server 2.0.41 Apache Software Foundation Apache HTTP Server 2.0.42 Apache Software Foundation Apache HTTP Server 2.0.43
Apache Software Foundation Apache HTTP Server 2.0.44 Apache Software Foundation Apache HTTP Server 2.0.45 Apache Software Foundation Apache HTTP Server 2.0.46
cpe:2.3:a:apache:http_server:2.0.46:-:win32 Apache Software Foundation Apache HTTP Server 2.0.47 Apache Software Foundation Apache HTTP Server 2.0.48
Apache Software Foundation Apache HTTP Server 2.0.49 Apache Software Foundation Apache HTTP Server 2.0.50 Apache Software Foundation Apache HTTP Server 2.0.51
Apache Software Foundation Apache HTTP Server 2.0.52 Apache Software Foundation Apache HTTP Server 2.0.53 Apache Software Foundation Apache HTTP Server 2.0.54
Apache Software Foundation Apache HTTP Server 2.0.55 Apache Software Foundation Apache HTTP Server 2.0.56 Apache Software Foundation Apache HTTP Server 2.0.57
Apache Software Foundation Apache HTTP Server 2.0.58 cpe:2.3:a:apache:http_server:2.0.58:-:win32 Apache Software Foundation HTTP Server 2.0.59
Apache Software Foundation Apache HTTP Server 2.0.60 dev Apache Software Foundation HTTP Server 2.0.61 Apache Software Foundation Apache HTTP Server 2.1
Apache Software Foundation Apache HTTP Server 2.1.1 Apache Software Foundation Apache HTTP Server 2.1.2 Apache Software Foundation Apache HTTP Server 2.1.3
Apache Software Foundation Apache HTTP Server 2.1.4 Apache Software Foundation Apache HTTP Server 2.1.5 Apache Software Foundation Apache HTTP Server 2.1.6
Apache Software Foundation Apache HTTP Server 2.1.7 Apache Software Foundation Apache HTTP Server 2.1.8 Apache Software Foundation Apache HTTP Server 2.1.9
Apache Software Foundation Apache HTTP Server 2.2 Apache Software Foundation Apache HTTP Server 2.2.0 Apache Software Foundation Apache HTTP Server 2.2.1
Apache Software Foundation Apache HTTP Server 2.2.2 cpe:2.3:a:apache:http_server:2.2.2:-:windows Apache Software Foundation Apache HTTP Server 2.2.3
cpe:2.3:a:apache:http_server:2.2.3:-:windows Apache Software Foundation Apache HTTP Server 2.2.4 Apache Software Foundation Apache HTTP Server 2.2.6
cpe:2.3:a:apache:http_server:2.2.7 Apache Software Foundation Apache HTTP Server 2.2.8 Apache Software Foundation Apache HTTP Server 2.2.9
Apache Software Foundation Apache HTTP Server 2.2.10 Apache Software Foundation Apache HTTP Server 2.2.11 Apache Software Foundation Apache HTTP Server 2.3.0
Apache Software Foundation Apache HTTP Server 2.3.1 Apache Software Foundation Apache HTTP Server 2.3.2

References

http://lists.apple.com/archives/security-announce/2009/Nov/msg00000.html
http://lists.opensuse.org/opensuse-security-announce/2009-10/msg00006.html
http://marc.info/?l=bugtraq&m=129190899612998&w=2
http://security.gentoo.org/glsa/glsa-200907-04.xml
http://support.apple.com/kb/HT3937
http://svn.apache.org/viewvc/httpd/httpd/trunk/CHANGES?r1=790587&r2=790586&pathrev=790587
http://svn.apache.org/viewvc/httpd/httpd/trunk/CHANGES?revision=790587
http://svn.apache.org/viewvc/httpd/httpd/trunk/modules/proxy/mod_proxy_http.c?r1=790587&r2=790586
http://svn.apache.org/viewvc?view=rev&revision=790587
http://wiki.rpath.com/Advisories:rPSA-2009-0142
http://www-01.ibm.com/support/docview.wss?uid=swg1PK91259
http://www-01.ibm.com/support/docview.wss?uid=swg1PK99480
http://www.debian.org/security/2009/dsa-1834
http://www.mandriva.com/security/advisories?name=MDVSA-2009:149
http://www.mandriva.com/security/advisories?name=MDVSA-2013:150
http://www.oracle.com/technetwork/topics/security/cpuapr2013-1899555.html
http://www.redhat.com/support/errata/RHSA-2009-1156.html
http://www.securityfocus.com/archive/1/507852/100/0/threaded
http://www.securityfocus.com/archive/1/507857/100/0/threaded
http://www.securityfocus.com/bid/35565
http://www.securitytracker.com/id?1022509
http://www.ubuntu.com/usn/USN-802-1
http://www.vupen.com/english/advisories/2009/3184
https://rhn.redhat.com/errata/RHSA-2009-1148.html

https://www.redhat.com/archives/fedora-package-announce/2009-August/msg01363.html

Summary

The mod_deflate module in Apache httpd 2.2.11 and earlier compresses large files until completion even after the associated network connection is closed, which allows remote attackers to cause a denial of service (CPU consumption).

CVE-2009-1891 Information	
CVSS Score	7.1
CWE	CWE-399
Vulnerability impact	
Confidentiality	NONE
Integrity	NONE
Availability	COMPLETE
Access methodology information	
Vector	NETWORK
Complexity	MEDIUM
Authentication	NONE

Vulnerable configs

Apache Software Foundation Apache HTTP Server
Apache Software Foundation Apache HTTP Server 0.8.11 Apache Software Foundation Apache HTTP Server 0.8.14 Apache Software Foundation Apache HTTP Server 1.0.2
Apache Software Foundation Apache HTTP Server 1.0.3 Apache Software Foundation Apache HTTP Server 1.0.5 Apache Software Foundation Apache HTTP Server 1.1
Apache Software Foundation Apache HTTP Server 1.1.1 Apache Software Foundation Apache 1.2 Apache Software Foundation Apache HTTP Server 1.2.4
Apache Software Foundation Apache 1.29 Apache Software Foundation Apache HTTP Server 1.3.3 Apache Software Foundation Apache HTTP Server 1.3.6
Apache Software Foundation Apache HTTP Server 1.3.7 Apache Software Foundation Apache HTTP Server 1.3.9 Apache Software Foundation Apache 1.3.13
Apache Software Foundation Apache HTTP Server 1.3.14 Apache Software Foundation Apache HTTP Server 1.3.18 Apache Software Foundation Apache HTTP Server 1.3.19
Apache Software Foundation Apache HTTP Server 1.3.20 Apache Software Foundation Apache HTTP Server 1.3.22 Apache Software Foundation Apache HTTP Server 1.3.23
Apache Software Foundation Apache HTTP Server 1.3.27 Apache Software Foundation Apache HTTP Server 1.3.29 Apache Software Foundation Apache HTTP Server 1.3.31
Apache Software Foundation Apache HTTP Server 1.3.33 Apache Software Foundation Apache HTTP Server 1.3.38 Apache Software Foundation Apache HTTP Server 1.99
Apache Software Foundation Apache HTTP Server 2.0.9a Apache Software Foundation Apache HTTP Server 2.0.28 Apache Software Foundation Apache HTTP Server 2.0.34 Beta
Apache Software Foundation Apache HTTP Server 2.0.38 Apache Software Foundation Apache HTTP Server 2.0.39 Apache Software Foundation Apache HTTP Server 2.0.40
Apache Software Foundation Apache HTTP Server 2.0.41 Apache Software Foundation Apache HTTP Server 2.0.42 Apache Software Foundation Apache HTTP Server 2.0.45
Apache Software Foundation Apache HTTP Server 2.0.46 Apache Software Foundation Apache HTTP Server 2.0.47 Apache Software Foundation Apache HTTP Server 2.0.48
Apache Software Foundation Apache HTTP Server 2.0.49 Apache Software Foundation Apache HTTP Server 2.0.50 Apache Software Foundation Apache HTTP Server 2.0.51
Apache Software Foundation Apache HTTP Server 2.0.52 Apache Software Foundation Apache HTTP Server 2.0.53 Apache Software Foundation Apache HTTP Server 2.0.54
Apache Software Foundation Apache HTTP Server 2.0.55 Apache Software Foundation Apache HTTP Server 2.0.56 Apache Software Foundation Apache HTTP Server 2.0.57
Apache Software Foundation Apache HTTP Server 2.0.58 Apache Software Foundation HTTP Server 2.0.59 Apache Software Foundation Apache HTTP Server 2.0.60 dev
Apache Software Foundation HTTP Server 2.0.61 Apache Software Foundation Apache HTTP Server 2.1 Apache Software Foundation Apache HTTP Server 2.1.1
Apache Software Foundation Apache HTTP Server 2.1.2 Apache Software Foundation Apache HTTP Server 2.1.3 Apache Software Foundation Apache HTTP Server 2.1.4
Apache Software Foundation Apache HTTP Server 2.1.5 Apache Software Foundation Apache HTTP Server 2.1.6 Apache Software Foundation Apache HTTP Server 2.1.7
Apache Software Foundation Apache HTTP Server 2.1.8 Apache Software Foundation Apache HTTP Server 2.1.9 Apache Software Foundation Apache HTTP Server 2.2
Apache Software Foundation Apache HTTP Server 2.2.0 Apache Software Foundation Apache HTTP Server 2.2.1 Apache Software Foundation Apache HTTP Server 2.2.2
Apache Software Foundation Apache HTTP Server 2.2.3 Apache Software Foundation Apache HTTP Server 2.2.4 Apache Software Foundation Apache HTTP Server 2.2.6
cpe:2.3:a:apache:http_server:2.2.7 Apache Software Foundation Apache HTTP Server 2.2.8 Apache Software Foundation Apache HTTP Server 2.2.9
Apache Software Foundation Apache HTTP Server 2.2.10 Apache Software Foundation Apache HTTP Server 2.2.11

References

http://bugs.debian.org/cgi-bin/bugreport.cgi?bug=534712
http://lists.apple.com/archives/security-announce/2009/Nov/msg00000.html
http://lists.opensuse.org/opensuse-security-announce/2009-10/msg00006.html
http://marc.info/?l=apache-httpd-dev&m=124621326524824&w=2
http://marc.info/?l=apache-httpd-dev&m=124661528519546&w=2
http://marc.info/?l=bugtraq&m=129190899612998&w=2
http://marc.info/?l=bugtraq&m=130497311408250&w=2
http://security.gentoo.org/glsa/glsa-200907-04.xml
http://support.apple.com/kb/HT3937
http://wiki.rpath.com/Advisories:rPSA-2009-0142
http://wiki.rpath.com/wiki/Advisories:rPSA-2009-0142
http://www-01.ibm.com/support/docview.wss?uid=swg1PK91361
http://www-01.ibm.com/support/docview.wss?uid=swg1PK99480
http://www.debian.org/security/2009/dsa-1834
http://www.mandriva.com/security/advisories?name=MDVSA-2009:149
http://www.redhat.com/support/errata/RHSA-2009-1156.html
http://www.securityfocus.com/archive/1/507857/100/0/threaded
http://www.securitytracker.com/id?1022529
http://www.ubuntu.com/usn/USN-802-1
http://www.vupen.com/english/advisories/2009/1841
http://www.vupen.com/english/advisories/2009/3184
https://bugzilla.redhat.com/show_bug.cgi?id=509125
https://rhn.redhat.com/errata/RHSA-2009-1148.html
https://www.redhat.com/archives/fedora-package-announce/2009-August/msg01363.html

Summary

envvars (aka envvars-std) in the Apache HTTP Server before 2.4.2 places a zero-length directory name in the LD_LIBRARY_PATH, which allows local users to gain privileges via a Trojan horse DSO in the current working directory during execution of apachectl.

CVE-2012-0883 Information	
CVSS Score	6.9
CWE	CWE-264
Vulnerability impact	
Confidentiality	COMPLETE
Integrity	COMPLETE
Availability	COMPLETE
Access methodology information	
Vector	LOCAL
Complexity	MEDIUM
Authentication	NONE

Vulnerable configs

Apache Software Foundation Apache HTTP Server 0.8.11
Apache Software Foundation Apache HTTP Server 0.8.14 Apache Software Foundation Apache HTTP Server 1.0 Apache Software Foundation Apache HTTP Server 1.0.2
Apache Software Foundation Apache HTTP Server 1.0.3 Apache Software Foundation Apache HTTP Server 1.0.5 Apache Software Foundation Apache HTTP Server 1.1
Apache Software Foundation Apache HTTP Server 1.1.1 Apache Software Foundation Apache 1.2 Apache Software Foundation Apache HTTP Server 1.2.4
Apache Software Foundation Apache HTTP Server 1.2.5 Apache Software Foundation Apache HTTP Server 1.2.6 Apache Software Foundation Apache 1.29
Apache Software Foundation Apache HTTP Server 1.3 Apache Software Foundation Apache HTTP Server 1.3.0 Apache Software Foundation Apache HTTP Server 1.3.1
Apache Software Foundation Apache HTTP Server 1.3.1.1 Apache Software Foundation Apache HTTP Server 1.3.2 Apache Software Foundation Apache HTTP Server 1.3.3
Apache Software Foundation Apache HTTP Server 1.3.4 Apache Software Foundation Apache HTTP Server 1.3.5 Apache Software Foundation Apache HTTP Server 1.3.6
Apache Software Foundation Apache HTTP Server 1.3.7 Apache Software Foundation Apache HTTP Server 1.3.8 Apache Software Foundation Apache HTTP Server 1.3.9
Apache Software Foundation Apache 1.3.10 Apache Software Foundation Apache HTTP Server 1.3.11 Apache Software Foundation Apache HTTP Server 1.3.12
Apache Software Foundation Apache 1.3.13 Apache Software Foundation Apache HTTP Server 1.3.14 Apache Software Foundation Apache 1.3.15
Apache Software Foundation Apache 1.3.16 Apache Software Foundation Apache HTTP Server 1.3.17 Apache Software Foundation Apache HTTP Server 1.3.18
Apache Software Foundation Apache HTTP Server 1.3.19 Apache Software Foundation Apache HTTP Server 1.3.20 Apache Software Foundation Apache HTTP Server 1.3.22
Apache Software Foundation Apache HTTP Server 1.3.23 Apache Software Foundation Apache HTTP Server 1.3.24 Apache Software Foundation Apache HTTP Server 1.3.25
Apache Software Foundation Apache HTTP Server 1.3.26 Apache Software Foundation Apache HTTP Server 1.3.27 Apache Software Foundation Apache HTTP Server 1.3.28
Apache Software Foundation Apache HTTP Server 1.3.29 Apache Software Foundation Apache HTTP Server 1.3.30 Apache Software Foundation Apache HTTP Server 1.3.31
Apache Software Foundation Apache HTTP Server 1.3.32 Apache Software Foundation Apache HTTP Server 1.3.33 Apache Software Foundation Apache HTTP Server 1.3.34
Apache Software Foundation Apache HTTP Server 1.3.35 Apache Software Foundation Apache HTTP Server 1.3.36 Apache Software Foundation Apache HTTP Server 1.3.37
Apache Software Foundation Apache HTTP Server 1.3.38 Apache Software Foundation Apache HTTP Server 1.3.39 Apache Software Foundation Apache HTTP Server 1.3.41
Apache Software Foundation Apache HTTP Server 1.3.42 Apache Software Foundation Apache HTTP Server 1.3.65 Apache Software Foundation Apache HTTP Server 1.3.68
Apache Software Foundation Apache HTTP Server 1.4.0 Apache Software Foundation Apache HTTP Server 1.99 Apache Software Foundation Apache HTTP Server 2.0
Apache Software Foundation Apache HTTP Server 2.0.9a Apache Software Foundation Apache HTTP Server 2.0.28 Apache Software Foundation Apache HTTP Server 2.0.28 Beta
Apache Software Foundation Apache HTTP Server 2.0.32 Apache Software Foundation Apache HTTP Server 2.0.32 Beta Apache Software Foundation Apache HTTP Server 2.0.34 Beta
Apache Software Foundation Apache HTTP Server 2.0.35 Apache Software Foundation Apache HTTP Server 2.0.36 Apache Software Foundation Apache HTTP Server 2.0.37
Apache Software Foundation Apache HTTP Server 2.0.38 Apache Software Foundation Apache HTTP Server 2.0.39 Apache Software Foundation Apache HTTP Server 2.0.40
Apache Software Foundation Apache HTTP Server 2.0.41 Apache Software Foundation Apache HTTP Server 2.0.42 Apache Software Foundation Apache HTTP Server 2.0.43
Apache Software Foundation Apache HTTP Server 2.0.44 Apache Software Foundation Apache HTTP Server 2.0.45 Apache Software Foundation Apache HTTP Server 2.0.46
Apache Software Foundation Apache HTTP Server 2.0.47 Apache Software Foundation Apache HTTP Server 2.0.48 Apache Software Foundation Apache HTTP Server 2.0.49
Apache Software Foundation Apache HTTP Server 2.0.50 Apache Software Foundation Apache HTTP Server 2.0.51 Apache Software Foundation Apache HTTP Server 2.0.52
Apache Software Foundation Apache HTTP Server 2.0.53 Apache Software Foundation Apache HTTP Server 2.0.54 Apache Software Foundation Apache HTTP Server 2.0.55
Apache Software Foundation Apache HTTP Server 2.0.56 Apache Software Foundation Apache HTTP Server 2.0.57 Apache Software Foundation Apache HTTP Server 2.0.58
Apache Software Foundation HTTP Server 2.0.59 Apache Software Foundation Apache HTTP Server 2.0.60 dev Apache Software Foundation HTTP Server 2.0.61

Apache Software Foundation Apache HTTP Server 2.0.63	Apache Software Foundation Apache HTTP Server 2.1	Apache Software Foundation Apache HTTP Server 2.1.1
Apache Software Foundation Apache HTTP Server 2.1.2	Apache Software Foundation Apache HTTP Server 2.1.3	Apache Software Foundation Apache HTTP Server 2.1.4
Apache Software Foundation Apache HTTP Server 2.1.5	Apache Software Foundation Apache HTTP Server 2.1.6	Apache Software Foundation Apache HTTP Server 2.1.7
Apache Software Foundation Apache HTTP Server 2.1.8	Apache Software Foundation Apache HTTP Server 2.1.9	Apache Software Foundation Apache HTTP Server 2.2
Apache Software Foundation Apache HTTP Server 2.2.0	Apache Software Foundation Apache HTTP Server 2.2.1	Apache Software Foundation Apache HTTP Server 2.2.2
Apache Software Foundation Apache HTTP Server 2.2.3	Apache Software Foundation Apache HTTP Server 2.2.4	Apache Software Foundation Apache HTTP Server 2.2.6
Apache Software Foundation Apache HTTP Server 2.2.8	Apache Software Foundation Apache HTTP Server 2.2.9	Apache Software Foundation Apache HTTP Server 2.2.10
Apache Software Foundation Apache HTTP Server 2.2.11	Apache Software Foundation Apache HTTP Server 2.2.12	Apache Software Foundation Apache HTTP Server 2.2.13
Apache Software Foundation Apache HTTP Server 2.2.14	Apache Software Foundation Apache HTTP Server 2.2.15	Apache Software Foundation Apache HTTP Server 2.2.16
Apache Software Foundation Apache HTTP Server 2.2.17	Apache Software Foundation Apache HTTP Server 2.2.18	Apache Software Foundation Apache HTTP Server 2.2.19
Apache Software Foundation Apache HTTP Server 2.2.20	Apache HTTP Server 2.2.21	Apache Software Foundation Apache HTTP Server 2.3.0
Apache Software Foundation Apache HTTP Server 2.3.1	Apache Software Foundation Apache HTTP Server 2.3.2	Apache Software Foundation Apache HTTP Server 2.3.3
Apache Software Foundation Apache HTTP Server 2.3.4	Apache Software Foundation Apache HTTP Server 2.3.5	Apache Software Foundation Apache HTTP Server 2.3.6
Apache Software Foundation Apache HTTP Server 2.3.7	Apache Software Foundation Apache HTTP Server 2.3.8	Apache Software Foundation Apache HTTP Server 2.3.9
Apache Software Foundation Apache HTTP Server 2.3.10	Apache Software Foundation Apache HTTP Server 2.3.11	Apache Software Foundation Apache HTTP Server 2.3.12
Apache Software Foundation Apache HTTP Server 2.3.13	Apache Software Foundation Apache HTTP Server 2.3.14	Apache Software Foundation Apache HTTP Server 2.3.15
Apache Software Foundation Apache HTTP Server 2.3.16	Apache Software Foundation Apache HTTP Server 2.4.0	Apache Software Foundation Apache HTTP Server 2.4.1

References

http://article.gmane.org/gmane.comp.apache.devel/48158

http://lists.apple.com/archives/security-announce/2013/Sep/msg00002.html

http://lists.opensuse.org/opensuse-updates/2013-02/msg00009.html

http://lists.opensuse.org/opensuse-updates/2013-02/msg00012.html

http://marc.info/?l=bugtraq&m=134012830914727&w=2

http://support.apple.com/kb/HT5880

http://svn.apache.org/viewvc?view=revision&revision=1296428

http://www.apache.org/dist/httpd/Announcement2.4.html

http://www.apachelounge.com/Changelog-2.4.html

http://www.securityfocus.com/bid/53046

http://www.securitytracker.com/id?1026932

http://www.xerox.com/download/security/security-bulletin/16287-4d6b7b0c81f7b/cert_XRX13-003_v1.0.pdf

https://exchange.xforce.ibmcloud.com/vulnerabilities/74901

https://h20564.www2.hp.com/portal/site/hpsc/public/kb/docDisplay?docId=emr_na-c03839862

https://httpd.apache.org/security/vulnerabilities_24.html

Summary

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 Information	
CVSS Score	5.1
CWE	CWE-310
Vulnerability impact	
Confidentiality	PARTIAL
Integrity	PARTIAL
Availability	PARTIAL
Access methodology information	
Vector	NETWORK
Complexity	HIGH
Authentication	NONE

Vulnerable configs

Apache Software Foundation Apache HTTP Server 2.2.24
Apache Software Foundation Apache HTTP Server 2.2.22
Apache Software Foundation Apache HTTP Server 2.2.23
Apache Software Foundation Apache HTTP Server 2.2.19
Apache Software Foundation Apache HTTP Server 2.2
Apache Software Foundation Apache HTTP Server 2.2.1
Apache Software Foundation Apache HTTP Server 2.2.16
Apache Software Foundation Apache HTTP Server 2.2.15
Apache Software Foundation Apache HTTP Server 2.2.6
Apache HTTP Server 2.2.21
Apache Software Foundation Apache HTTP Server 2.2.12
Apache Software Foundation Apache HTTP Server 2.2.2
Apache Software Foundation Apache HTTP Server 2.2.4
Apache Software Foundation Apache HTTP Server 2.2.17
Apache Software Foundation Apache HTTP Server 2.2.0
Apache Software Foundation Apache HTTP Server 2.2.11
Apache Software Foundation Apache HTTP Server 2.2.18
Apache Software Foundation Apache HTTP Server 2.2.9
Apache Software Foundation Apache HTTP Server 2.2.13
Apache Software Foundation Apache HTTP Server 2.2.10
Apache Software Foundation Apache HTTP Server 2.2.8
Apache Software Foundation Apache HTTP Server 2.2.3
Apache Software Foundation Apache HTTP Server 2.2.20
Apache Software Foundation Apache HTTP Server 2.2.14

References

http://lists.opensuse.org/opensuse-updates/2013-08/msg00026.html
http://lists.opensuse.org/opensuse-updates/2013-08/msg00029.html
http://lists.opensuse.org/opensuse-updates/2013-08/msg00030.html
http://people.apache.org/~jorton/mod_rewrite-CVE-2013-1862.patch
http://rhn.redhat.com/errata/RHSA-2013-0815.html

http://rhn.redhat.com/errata/RHSA-2013-1207.html
http://rhn.redhat.com/errata/RHSA-2013-1208.html
http://rhn.redhat.com/errata/RHSA-2013-1209.html
http://support.apple.com/kb/HT6150
http://svn.apache.org/viewvc?view=revision&revision=r1469311
http://tools.cisco.com/security/center/content/CiscoSecurityNotice/CVE-2013-1862
http://www-01.ibm.com/support/docview.wss?uid=swg21644047
http://www.fujitsu.com/global/support/software/security/products-f/interstage-201303e.html
http://www.mandriva.com/security/advisories?name=MDVSA-2013:174
http://www.oracle.com/technetwork/topics/security/cpujan2014-1972949.html
http://www.securityfocus.com/bid/59826
http://www.securityfocus.com/bid/64758
http://www.ubuntu.com/usn/USN-1903-1
https://bugzilla.redhat.com/show_bug.cgi?id=953729
https://h20566.www2.hp.com/portal/site/hpsc/template.PAGE/public/kb/docDisplay/?spf_p.tpst=kbDocD
navigationalState\%3DdocId\%253Demr_na-c03922406-1\%257CdocLocale\%253D\%257CcalledBy\%253

Summary

The mod_cgid module in the Apache HTTP Server before 2.4.10 does not have a timeout mechanism, which allows remote attackers to cause a denial of service (process hang) via a request to a CGI script that does not read from its stdin file descriptor.

CVE-2014-0231 Information	
CVSS Score	5.0
CWE	CWE-399
Vulnerability impact	
Confidentiality	NONE
Integrity	NONE
Availability	PARTIAL
Access methodology information	
Vector	NETWORK
Complexity	LOW
Authentication	NONE

Vulnerable configs

Apache Software Foundation Apache HTTP Server
Apache Software Foundation Apache HTTP Server 2.2.0
Apache Software Foundation Apache HTTP Server 2.2.2
Apache Software Foundation Apache HTTP Server 2.2.3
Apache Software Foundation Apache HTTP Server 2.2.4
Apache Software Foundation Apache HTTP Server 2.2.6
Apache Software Foundation Apache HTTP Server 2.2.8
Apache Software Foundation Apache HTTP Server 2.2.9
Apache Software Foundation Apache HTTP Server 2.2.10
Apache Software Foundation Apache HTTP Server 2.2.11
Apache Software Foundation Apache HTTP Server 2.2.12
Apache Software Foundation Apache HTTP Server 2.2.13
Apache Software Foundation Apache HTTP Server 2.2.14
Apache Software Foundation Apache HTTP Server 2.2.15
Apache Software Foundation Apache HTTP Server 2.2.16
Apache Software Foundation Apache HTTP Server 2.2.17
Apache Software Foundation Apache HTTP Server 2.2.18
Apache Software Foundation Apache HTTP Server 2.2.19
Apache Software Foundation Apache HTTP Server 2.2.20
Apache HTTP Server 2.2.21
Apache Software Foundation Apache HTTP Server 2.2.22
Apache Software Foundation Apache HTTP Server 2.2.23
Apache Software Foundation Apache HTTP Server 2.2.24
Apache Software Foundation Apache HTTP Server 2.2.25
Apache Software Foundation Apache HTTP Server 2.2.26
Apache Software Foundation Apache HTTP Server 2.2.27
Apache Software Foundation Apache HTTP Server 2.4.1
Apache Software Foundation Apache HTTP Server 2.4.2
Apache Software Foundation Apache HTTP Server 2.4.3
Apache Software Foundation Apache HTTP Server 2.4.4
Apache Software Foundation Apache HTTP Server 2.4.6
Apache Software Foundation Apache HTTP Server 2.4.7
Apache Software Foundation Apache HTTP Server 2.4.8
Apache Software Foundation Apache HTTP Server 2.4.9

References

http://advisories.mageia.org/MGASA-2014-0304.html
http://advisories.mageia.org/MGASA-2014-0305.html
http://httpd.apache.org/security/vulnerabilities_24.html
http://lists.apple.com/archives/security-announce/2015/Apr/msg00001.html
http://marc.info/?l=bugtraq&m=143403519711434&w=2

http://marc.info/?l=bugtraq&m=143748090628601&w=2
http://marc.info/?l=bugtraq&m=144050155601375&w=2
http://marc.info/?l=bugtraq&m=144493176821532&w=2
http://packetstormsecurity.com/files/130769/RSA-Digital-Certificate-Solution-XSS-Denial-Of-Service.html
http://rhn.redhat.com/errata/RHSA-2014-1019.html
http://rhn.redhat.com/errata/RHSA-2014-1020.html
http://rhn.redhat.com/errata/RHSA-2014-1021.html
http://svn.apache.org/repos/asf/httpd/httpd/branches/2.2.x/CHANGES
http://svn.apache.org/viewvc/httpd/httpd/trunk/modules/generators/mod_cgid.c
http://svn.apache.org/viewvc/httpd/httpd/trunk/modules/generators/mod_cgid.c?r1=1482522&r2=153512
http://svn.apache.org/viewvc/httpd/httpd/trunk/modules/generators/mod_cgid.c?r1=1565711&r2=161050
http://www.debian.org/security/2014/dsa-2989
http://www.mandriva.com/security/advisories?name=MDVSA-2014:142
http://www.oracle.com/technetwork/topics/security/cpujan2015-1972971.html
http://www.securityfocus.com/bid/68742
https://bugzilla.redhat.com/show_bug.cgi?id=1120596
https://h20564.www2.hpe.com/portal/site/hpsc/public/kb/docDisplay?docId=emr_na-c04832246
https://puppet.com/security/cve/cve-2014-0231
https://security.gentoo.org/glsa/201504-03
https://support.apple.com/HT204659

Summary

The dav_xml_get_cdata function in main/util.c in the mod_dav module in the Apache HTTP Server before 2.4.8 does not properly remove whitespace characters from CDATA sections, which allows remote attackers to cause a denial of service (daemon crash) via a crafted DAV WRITE request.

CVE-2013-6438 Information	
CVSS Score	5.0
CWE	CWE-20
Vulnerability impact	
Confidentiality	NONE
Integrity	NONE
Availability	PARTIAL
Access methodology information	
Vector	NETWORK
Complexity	LOW
Authentication	NONE

Vulnerable configs

Apache Software Foundation Apache HTTP Server 2.0		Apache Software Foundation Apache HTTP Server 2.0.9a
Apache Software Foundation Apache HTTP Server 2.0.28	Apache Software Foundation Apache HTTP Server 2.0.28 Beta	Apache Software Foundation Apache HTTP Server 2.0.32
Apache Software Foundation Apache HTTP Server 2.0.32 Beta	Apache Software Foundation Apache HTTP Server 2.0.34 Beta	Apache Software Foundation Apache HTTP Server 2.0.35
Apache Software Foundation Apache HTTP Server 2.0.36	Apache Software Foundation Apache HTTP Server 2.0.37	Apache Software Foundation Apache HTTP Server 2.0.38
Apache Software Foundation Apache HTTP Server 2.0.39	Apache Software Foundation Apache HTTP Server 2.0.40	Apache Software Foundation Apache HTTP Server 2.0.41
Apache Software Foundation Apache HTTP Server 2.0.42	Apache Software Foundation Apache HTTP Server 2.0.43	Apache Software Foundation Apache HTTP Server 2.0.44
Apache Software Foundation Apache HTTP Server 2.0.45	Apache Software Foundation Apache HTTP Server 2.0.46	Apache Software Foundation Apache HTTP Server 2.0.47
Apache Software Foundation Apache HTTP Server 2.0.48	Apache Software Foundation Apache HTTP Server 2.0.49	Apache Software Foundation Apache HTTP Server 2.0.50
Apache Software Foundation Apache HTTP Server 2.0.51	Apache Software Foundation Apache HTTP Server 2.0.52	Apache Software Foundation Apache HTTP Server 2.0.53
Apache Software Foundation Apache HTTP Server 2.0.54	Apache Software Foundation Apache HTTP Server 2.0.55	Apache Software Foundation Apache HTTP Server 2.0.56
Apache Software Foundation Apache HTTP Server 2.0.57	Apache Software Foundation Apache HTTP Server 2.0.58	Apache Software Foundation HTTP Server 2.0.59
Apache Software Foundation Apache HTTP Server 2.0.60 dev	Apache Software Foundation HTTP Server 2.0.61	Apache Software Foundation Apache HTTP Server 2.0.63
Apache Software Foundation Apache HTTP Server 2.0.64	Apache Software Foundation Apache HTTP Server 2.1	Apache Software Foundation Apache HTTP Server 2.1.1
Apache Software Foundation Apache HTTP Server 2.1.2	Apache Software Foundation Apache HTTP Server 2.1.3	Apache Software Foundation Apache HTTP Server 2.1.4
Apache Software Foundation Apache HTTP Server 2.1.5	Apache Software Foundation Apache HTTP Server 2.1.6	Apache Software Foundation Apache HTTP Server 2.1.7
Apache Software Foundation Apache HTTP Server 2.1.8	Apache Software Foundation Apache HTTP Server 2.1.9	Apache Software Foundation Apache HTTP Server 2.2
Apache Software Foundation Apache HTTP Server 2.2.0	Apache Software Foundation Apache HTTP Server 2.2.1	Apache Software Foundation Apache HTTP Server 2.2.2
Apache Software Foundation Apache HTTP Server 2.2.3	Apache Software Foundation Apache HTTP Server 2.2.4	Apache Software Foundation Apache HTTP Server 2.2.6
Apache Software Foundation Apache HTTP Server 2.2.8	Apache Software Foundation Apache HTTP Server 2.2.9	Apache Software Foundation Apache HTTP Server 2.2.10
Apache Software Foundation Apache HTTP Server 2.2.11	Apache Software Foundation Apache HTTP Server 2.2.12	Apache Software Foundation Apache HTTP Server 2.2.13
Apache Software Foundation Apache HTTP Server 2.2.14	Apache Software Foundation Apache HTTP Server 2.2.15	Apache Software Foundation Apache HTTP Server 2.2.16
Apache Software Foundation Apache HTTP Server 2.2.17	Apache Software Foundation Apache HTTP Server 2.2.18	Apache Software Foundation Apache HTTP Server 2.2.19
Apache Software Foundation Apache HTTP Server 2.2.20	Apache HTTP Server 2.2.21	Apache Software Foundation Apache HTTP Server 2.2.22
Apache Software Foundation Apache HTTP Server 2.2.23	Apache Software Foundation Apache HTTP Server 2.2.24	Apache Software Foundation Apache HTTP Server 2.2.25
Apache Software Foundation Apache HTTP Server 2.3.0	Apache Software Foundation Apache HTTP Server 2.3.1	Apache Software Foundation Apache HTTP Server 2.3.2
Apache Software Foundation Apache HTTP Server 2.3.3	Apache Software Foundation Apache HTTP Server 2.3.4	Apache Software Foundation Apache HTTP Server 2.3.5
Apache Software Foundation Apache HTTP Server 2.3.6	Apache Software Foundation Apache HTTP Server 2.3.7	Apache Software Foundation Apache HTTP Server 2.3.8
Apache Software Foundation Apache HTTP Server 2.3.9	Apache Software Foundation Apache HTTP Server 2.3.10	Apache Software Foundation Apache HTTP Server 2.3.11
Apache Software Foundation Apache HTTP Server 2.3.12	Apache Software Foundation Apache HTTP Server 2.3.13	Apache Software Foundation Apache HTTP Server 2.3.14
Apache Software Foundation Apache HTTP Server 2.3.15	Apache Software Foundation Apache HTTP Server 2.3.16	Apache Software Foundation Apache HTTP Server 2.4.0

Apache Software Foundation Apache HTTP Server 2.4.1 Apache Software Foundation Apache HTTP Server 2.4.2 Apache Software Foundation Apache HTTP Server 2.4.3
Apache Software Foundation Apache HTTP Server 2.4.4 Apache Software Foundation Apache HTTP Server 2.4.6 Apache Software Foundation Apache HTTP Server 2.4.7

References

http://advisories.mageia.org/MGASA-2014-0135.html
http://archives.neohapsis.com/archives/bugtraq/2014-10/0101.html
http://kb.juniper.net/InfoCenter/index?page=content&id=JSA10698
http://lists.apple.com/archives/security-announce/2015/Apr/msg00001.html
http://marc.info/?l=bugtraq&m=141017844705317&w=2
http://marc.info/?l=bugtraq&m=141390017113542&w=2
http://seclists.org/fulldisclosure/2014/Dec/23
http://security.gentoo.org/glsa/glsa-201408-12.xml
http://svn.apache.org/repos/asf/httpd/httpd/branches/2.2.x/CHANGES
http://svn.apache.org/viewvc/httpd/httpd/trunk/modules/dav/main/util.c
http://svn.apache.org/viewvc/httpd/httpd/trunk/modules/dav/main/util.c?r1=1528718&r2=1556428&diff_
http://www-01.ibm.com/support/docview.wss?uid=swg21669554
http://www-01.ibm.com/support/docview.wss?uid=swg21676091
http://www-01.ibm.com/support/docview.wss?uid=swg21676092
http://www.apache.org/dist/httpd/CHANGES_2.4.9
http://www.oracle.com/technetwork/topics/security/cpujan2015-1972971.html
http://www.oracle.com/technetwork/topics/security/cpujul2014-1972956.html
http://www.securityfocus.com/archive/1/534161/100/0/threaded
http://www.securityfocus.com/bid/66303
http://www.ubuntu.com/usn/USN-2152-1
http://www.vmware.com/security/advisories/VMSA-2014-0012.html
https://blogs.oracle.com/sunsecurity/entry/multiple_input_validation_vulnerabilities_in1
https://httpd.apache.org/security/vulnerabilities_24.html
https://puppet.com/security/cve/cve-2013-6438
https://support.apple.com/HT204659
https://support.apple.com/kb/HT6535

Summary

The mod_proxy module in the Apache HTTP Server 1.3.x through 1.3.42, 2.0.x through 2.0.64, and 2.2.x through 2.2.21 does not properly interact with use of (1) RewriteRule and (2) ProxyPassMatch pattern matches for configuration of a reverse proxy, which allows remote attackers to send requests to intranet servers via a malformed URI containing an initial @ (at sign) character.

CVE-2011-3368 Information	
CVSS Score	5.0
CWE	CWE-20
Vulnerability impact	
Confidentiality	PARTIAL
Integrity	NONE
Availability	NONE
Access methodology information	
Vector	NETWORK
Complexity	LOW
Authentication	NONE

Vulnerable configs

Apache Software Foundation Apache HTTP Server 1.3 Apache Software Foundation Apache HTTP Server 1.3.0 Apache Software Foundation Apache HTTP Server 1.3.1
Apache Software Foundation Apache HTTP Server 1.3.1.1 Apache Software Foundation Apache HTTP Server 1.3.2 Apache Software Foundation Apache HTTP Server 1.3.3
Apache Software Foundation Apache HTTP Server 1.3.4 Apache Software Foundation Apache HTTP Server 1.3.5 Apache Software Foundation Apache HTTP Server 1.3.6
Apache Software Foundation Apache HTTP Server 1.3.7 Apache Software Foundation Apache HTTP Server 1.3.8 Apache Software Foundation Apache HTTP Server 1.3.9
Apache Software Foundation Apache 1.3.10 Apache Software Foundation Apache HTTP Server 1.3.11 Apache Software Foundation Apache HTTP Server 1.3.12
Apache Software Foundation Apache 1.3.13 Apache Software Foundation Apache HTTP Server 1.3.14 Apache Software Foundation Apache 1.3.15
Apache Software Foundation Apache 1.3.16 Apache Software Foundation Apache HTTP Server 1.3.17 Apache Software Foundation Apache HTTP Server 1.3.18
Apache Software Foundation Apache HTTP Server 1.3.19 Apache Software Foundation Apache HTTP Server 1.3.20 Apache Software Foundation Apache HTTP Server 1.3.22
Apache Software Foundation Apache HTTP Server 1.3.23 Apache Software Foundation Apache HTTP Server 1.3.24 Apache Software Foundation Apache HTTP Server 1.3.25
Apache Software Foundation Apache HTTP Server 1.3.26 Apache Software Foundation Apache HTTP Server 1.3.27 Apache Software Foundation Apache HTTP Server 1.3.28
Apache Software Foundation Apache HTTP Server 1.3.29 Apache Software Foundation Apache HTTP Server 1.3.30 Apache Software Foundation Apache HTTP Server 1.3.31
Apache Software Foundation Apache HTTP Server 1.3.32 Apache Software Foundation Apache HTTP Server 1.3.33 Apache Software Foundation Apache HTTP Server 1.3.34
Apache Software Foundation Apache HTTP Server 1.3.35 Apache Software Foundation Apache HTTP Server 1.3.36 Apache Software Foundation Apache HTTP Server 1.3.37
Apache Software Foundation Apache HTTP Server 1.3.38 Apache Software Foundation Apache HTTP Server 1.3.39 Apache Software Foundation Apache HTTP Server 1.3.41
Apache Software Foundation Apache HTTP Server 1.3.42 Apache Software Foundation Apache HTTP Server 1.3.65 Apache Software Foundation Apache HTTP Server 1.3.68
Apache Software Foundation Apache HTTP Server 2.0 Apache Software Foundation Apache HTTP Server 2.0.9a Apache Software Foundation Apache HTTP Server 2.0.28
Apache Software Foundation Apache HTTP Server 2.0.28 Beta Apache Software Foundation Apache HTTP Server 2.0.32 Apache Software Foundation Apache HTTP Server 2.0.32 Beta
Apache Software Foundation Apache HTTP Server 2.0.34 Beta Apache Software Foundation Apache HTTP Server 2.0.35 Apache Software Foundation Apache HTTP Server 2.0.36
Apache Software Foundation Apache HTTP Server 2.0.37 Apache Software Foundation Apache HTTP Server 2.0.38 Apache Software Foundation Apache HTTP Server 2.0.39
Apache Software Foundation Apache HTTP Server 2.0.40 Apache Software Foundation Apache HTTP Server 2.0.41 Apache Software Foundation Apache HTTP Server 2.0.42
Apache Software Foundation Apache HTTP Server 2.0.43 Apache Software Foundation Apache HTTP Server 2.0.44 Apache Software Foundation Apache HTTP Server 2.0.45
Apache Software Foundation Apache HTTP Server 2.0.46 Apache Software Foundation Apache HTTP Server 2.0.47 Apache Software Foundation Apache HTTP Server 2.0.48
Apache Software Foundation Apache HTTP Server 2.0.49 Apache Software Foundation Apache HTTP Server 2.0.50 Apache Software Foundation Apache HTTP Server 2.0.51
Apache Software Foundation Apache HTTP Server 2.0.52 Apache Software Foundation Apache HTTP Server 2.0.53 Apache Software Foundation Apache HTTP Server 2.0.54
Apache Software Foundation Apache HTTP Server 2.0.55 Apache Software Foundation Apache HTTP Server 2.0.56 Apache Software Foundation Apache HTTP Server 2.0.57
Apache Software Foundation Apache HTTP Server 2.0.58 Apache Software Foundation HTTP Server 2.0.59 Apache Software Foundation Apache HTTP Server 2.0.60 dev
Apache Software Foundation HTTP Server 2.0.61 Apache Software Foundation Apache HTTP Server 2.0.63 Apache Software Foundation Apache HTTP Server 2.0.64

Apache Software Foundation Apache HTTP Server 2.2.0
Apache Software Foundation Apache HTTP Server 2.2.1
Apache Software Foundation Apache HTTP Server 2.2.2
Apache Software Foundation Apache HTTP Server 2.2.3
Apache Software Foundation Apache HTTP Server 2.2.4
Apache Software Foundation Apache HTTP Server 2.2.6
Apache Software Foundation Apache HTTP Server 2.2.8
Apache Software Foundation Apache HTTP Server 2.2.9
Apache Software Foundation Apache HTTP Server 2.2.10
Apache Software Foundation Apache HTTP Server 2.2.11
Apache Software Foundation Apache HTTP Server 2.2.12
Apache Software Foundation Apache HTTP Server 2.2.13
Apache Software Foundation Apache HTTP Server 2.2.14
Apache Software Foundation Apache HTTP Server 2.2.15
Apache Software Foundation Apache HTTP Server 2.2.16
Apache Software Foundation Apache HTTP Server 2.2.18
Apache Software Foundation Apache HTTP Server 2.2.19
Apache Software Foundation Apache HTTP Server 2.2.20
Apache HTTP Server 2.2.21

References

http://kb.juniper.net/JSA10585
http://lists.apple.com/archives/security-announce/2012/Sep/msg00004.html
http://lists.opensuse.org/opensuse-security-announce/2011-11/msg00011.html
http://lists.opensuse.org/opensuse-updates/2013-02/msg00009.html
http://lists.opensuse.org/opensuse-updates/2013-02/msg00012.html
http://marc.info/?l=bugtraq&m=133294460209056&w=2
http://marc.info/?l=bugtraq&m=134987041210674&w=2
http://rhn.redhat.com/errata/RHSA-2012-0542.html
http://rhn.redhat.com/errata/RHSA-2012-0543.html
http://seclists.org/fulldisclosure/2011/Oct/232
http://seclists.org/fulldisclosure/2011/Oct/273
http://support.apple.com/kb/HT5501
http://svn.apache.org/viewvc?view=revision&revision=1179239
http://web.archiveorange.com/archive/v/ZyS0hzECD5zzb2NkvQlt
http://www-01.ibm.com/support/docview.wss?uid=nas2064c7e5f53452ff686257927003c8d42
http://www-01.ibm.com/support/docview.wss?uid=nas2b7c57b1f1035675186257927003c8d48
http://www.contextis.com/research/blog/reverseproxybypass/
http://www.debian.org/security/2012/dsa-2405
http://www.exploit-db.com/exploits/17969
http://www.mandriva.com/security/advisories?name=MDVSA-2011:144
http://www.mandriva.com/security/advisories?name=MDVSA-2013:150
http://www.oracle.com/technetwork/topics/security/cpujan2015-1972971.html
http://www.oracle.com/technetwork/topics/security/cpujul2012-392727.html
http://www.redhat.com/support/errata/RHSA-2011-1391.html
http://www.redhat.com/support/errata/RHSA-2011-1392.html
http://www.securityfocus.com/bid/49957
http://www.securitytracker.com/id?1026144
https://bugzilla.redhat.com/show_bug.cgi?id=740045
https://exchange.xforce.ibmcloud.com/vulnerabilities/70336

Summary

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.

CVE-2008-2364 Information	
CVSS Score	5.0
CWE	CWE-399
Vulnerability impact	
Confidentiality	NONE
Integrity	NONE
Availability	PARTIAL
Access methodology information	
Vector	NETWORK
Complexity	LOW
Authentication	NONE

Vulnerable configs

Apache Software Foundation Apache HTTP Server 2.0.63

Apache Software Foundation Apache HTTP Server 2.2.8

References

http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=c01539432
http://lists.apple.com/archives/security-announce/2008/Oct/msg00001.html
http://lists.opensuse.org/opensuse-security-announce/2009-03/msg00001.html
http://lists.opensuse.org/opensuse-security-announce/2009-03/msg00004.html
http://marc.info/?l=bugtraq&m=123376588623823&w=2
http://marc.info/?l=bugtraq&m=125631037611762&w=2
http://rhn.redhat.com/errata/RHSA-2008-0967.html
http://security.gentoo.org/glsa/glsa-200807-06.xml

http://sunsolve.sun.com/search/document.do?assetkey=1-26-247666-1
http://support.apple.com/kb/HT3216
http://svn.apache.org/viewvc/httpd/httpd/trunk/modules/proxy/mod_proxy_http.c?r1=666154&r2=66615
http://wiki.rpath.com/wiki/Advisories:rPSA-2008-0328
http://www-01.ibm.com/support/docview.wss?uid=swg27008517
http://www-1.ibm.com/support/docview.wss?uid=swg1PK67579
http://www.mandriva.com/security/advisories?name=MDVSA-2008:195
http://www.mandriva.com/security/advisories?name=MDVSA-2008:237
http://www.oracle.com/technetwork/topics/security/cpujuly2013-1899826.html
http://www.redhat.com/support/errata/RHSA-2008-0966.html
http://www.securityfocus.com/archive/1/494858/100/0/threaded
http://www.securityfocus.com/archive/1/498567/100/0/threaded
http://www.securityfocus.com/bid/29653
http://www.securityfocus.com/bid/31681
http://www.securitytracker.com/id?1020267
http://www.ubuntu.com/usn/USN-731-1
http://www.vupen.com/english/advisories/2008/1798
http://www.vupen.com/english/advisories/2008/2780
http://www.vupen.com/english/advisories/2009/0320
https://exchange.xforce.ibmcloud.com/vulnerabilities/42987
https://www.redhat.com/archives/fedora-package-announce/2008-August/msg00055.html
https://www.redhat.com/archives/fedora-package-announce/2008-August/msg00153.html

Summary

The log_cookie function in mod_log_config.c in the mod_log_config module in the Apache HTTP Server before 2.4.8 allows remote attackers to cause a denial of service (segmentation fault and daemon crash) via a crafted cookie that is not properly handled during truncation.

CVE-2014-0098 Information	
CVSS Score	5.0
CWE	CWE-20
Vulnerability impact	
Confidentiality	NONE
Integrity	NONE
Availability	PARTIAL
Access methodology information	
Vector	NETWORK
Complexity	LOW
Authentication	NONE

Vulnerable configs

Apache Software Foundation Apache HTTP Server 2.0 Apache Software Foundation Apache HTTP Server 2.0.9a Apache Software Foundation Apache HTTP Server 2.0.28
Apache Software Foundation Apache HTTP Server 2.0.28 Beta Apache Software Foundation Apache HTTP Server 2.0.32 Apache Software Foundation Apache HTTP Server 2.0.32 Beta
Apache Software Foundation Apache HTTP Server 2.0.34 Beta Apache Software Foundation Apache HTTP Server 2.0.35 Apache Software Foundation Apache HTTP Server 2.0.36
Apache Software Foundation Apache HTTP Server 2.0.37 Apache Software Foundation Apache HTTP Server 2.0.38 Apache Software Foundation Apache HTTP Server 2.0.39
Apache Software Foundation Apache HTTP Server 2.0.40 Apache Software Foundation Apache HTTP Server 2.0.41 Apache Software Foundation Apache HTTP Server 2.0.42
Apache Software Foundation Apache HTTP Server 2.0.43 Apache Software Foundation Apache HTTP Server 2.0.44 Apache Software Foundation Apache HTTP Server 2.0.45
Apache Software Foundation Apache HTTP Server 2.0.46 Apache Software Foundation Apache HTTP Server 2.0.47 Apache Software Foundation Apache HTTP Server 2.0.48
Apache Software Foundation Apache HTTP Server 2.0.49 Apache Software Foundation Apache HTTP Server 2.0.50 Apache Software Foundation Apache HTTP Server 2.0.51
Apache Software Foundation Apache HTTP Server 2.0.52 Apache Software Foundation Apache HTTP Server 2.0.53 Apache Software Foundation Apache HTTP Server 2.0.54
Apache Software Foundation Apache HTTP Server 2.0.55 Apache Software Foundation Apache HTTP Server 2.0.56 Apache Software Foundation Apache HTTP Server 2.0.57
Apache Software Foundation Apache HTTP Server 2.0.58 Apache Software Foundation HTTP Server 2.0.59 Apache Software Foundation Apache HTTP Server 2.0.60 dev
Apache Software Foundation HTTP Server 2.0.61 Apache Software Foundation Apache HTTP Server 2.0.63 Apache Software Foundation Apache HTTP Server 2.0.64
Apache Software Foundation Apache HTTP Server 2.1 Apache Software Foundation Apache HTTP Server 2.1.1 Apache Software Foundation Apache HTTP Server 2.1.2
Apache Software Foundation Apache HTTP Server 2.1.3 Apache Software Foundation Apache HTTP Server 2.1.4 Apache Software Foundation Apache HTTP Server 2.1.5
Apache Software Foundation Apache HTTP Server 2.1.6 Apache Software Foundation Apache HTTP Server 2.1.7 Apache Software Foundation Apache HTTP Server 2.1.8
Apache Software Foundation Apache HTTP Server 2.1.9 Apache Software Foundation Apache HTTP Server 2.2 Apache Software Foundation Apache HTTP Server 2.2.0
Apache Software Foundation Apache HTTP Server 2.2.1 Apache Software Foundation Apache HTTP Server 2.2.2 Apache Software Foundation Apache HTTP Server 2.2.3
Apache Software Foundation Apache HTTP Server 2.2.4 Apache Software Foundation Apache HTTP Server 2.2.6 Apache Software Foundation Apache HTTP Server 2.2.8
Apache Software Foundation Apache HTTP Server 2.2.9 Apache Software Foundation Apache HTTP Server 2.2.10 Apache Software Foundation Apache HTTP Server 2.2.11
Apache Software Foundation Apache HTTP Server 2.2.12 Apache Software Foundation Apache HTTP Server 2.2.13 Apache Software Foundation Apache HTTP Server 2.2.14
Apache Software Foundation Apache HTTP Server 2.2.15 Apache Software Foundation Apache HTTP Server 2.2.16 Apache Software Foundation Apache HTTP Server 2.2.17
Apache Software Foundation Apache HTTP Server 2.2.18 Apache Software Foundation Apache HTTP Server 2.2.19 Apache Software Foundation Apache HTTP Server 2.2.20
Apache HTTP Server 2.2.21 Apache Software Foundation Apache HTTP Server 2.2.22 Apache Software Foundation Apache HTTP Server 2.2.23
Apache Software Foundation Apache HTTP Server 2.2.24 Apache Software Foundation Apache HTTP Server 2.2.25 Apache Software Foundation Apache HTTP Server 2.3.0
Apache Software Foundation Apache HTTP Server 2.3.1 Apache Software Foundation Apache HTTP Server 2.3.2 Apache Software Foundation Apache HTTP Server 2.3.3
Apache Software Foundation Apache HTTP Server 2.3.4 Apache Software Foundation Apache HTTP Server 2.3.5 Apache Software Foundation Apache HTTP Server 2.3.6
Apache Software Foundation Apache HTTP Server 2.3.7 Apache Software Foundation Apache HTTP Server 2.3.8 Apache Software Foundation Apache HTTP Server 2.3.9
Apache Software Foundation Apache HTTP Server 2.3.10 Apache Software Foundation Apache HTTP Server 2.3.11 Apache Software Foundation Apache HTTP Server 2.3.12
Apache Software Foundation Apache HTTP Server 2.3.13 Apache Software Foundation Apache HTTP Server 2.3.14 Apache Software Foundation Apache HTTP Server 2.3.15
Apache Software Foundation Apache HTTP Server 2.3.16 Apache Software Foundation Apache HTTP Server 2.4.0 Apache Software Foundation Apache HTTP Server 2.4.1
Apache Software Foundation Apache HTTP Server 2.4.2 Apache Software Foundation Apache HTTP Server 2.4.3 Apache Software Foundation Apache HTTP Server 2.4.4

References

http://advisories.mageia.org/MGASA-2014-0135.html
http://archives.neohapsis.com/archives/bugtraq/2014-10/0101.html
http://kb.juniper.net/InfoCenter/index?page=content&id=JSA10698
http://lists.apple.com/archives/security-announce/2015/Apr/msg00001.html
http://marc.info/?l=bugtraq&m=141017844705317&w=2
http://marc.info/?l=bugtraq&m=141390017113542&w=2
http://seclists.org/fulldisclosure/2014/Dec/23
http://secunia.com/advisories/59219
http://security.gentoo.org/glsa/glsa-201408-12.xml
http://support.f5.com/kb/en-us/solutions/public/15000/300/sol15320.html
http://svn.apache.org/repos/asf/httpd/httpd/branches/2.2.x/CHANGES
http://svn.apache.org/viewvc/httpd/httpd/trunk/modules/loggers/mod_log_config.c
http://svn.apache.org/viewvc/httpd/httpd/trunk/modules/loggers/mod_log_config.c?r1=1575394&r2=1575
http://www-01.ibm.com/support/docview.wss?uid=swg21668973
http://www-01.ibm.com/support/docview.wss?uid=swg21676091
http://www-01.ibm.com/support/docview.wss?uid=swg21676092
http://www.apache.org/dist/httpd/CHANGES_2.4.9
http://www.oracle.com/technetwork/topics/security/cpujan2015-1972971.html
http://www.oracle.com/technetwork/topics/security/cpujul2014-1972956.html
http://www.securityfocus.com/archive/1/534161/100/0/threaded
http://www.securityfocus.com/bid/66303
http://www.ubuntu.com/usn/USN-2152-1
http://www.vmware.com/security/advisories/VMSA-2014-0012.html
https://blogs.oracle.com/sunsecurity/entry/multiple_input_validation_vulnerabilities_in1
https://httpd.apache.org/security/vulnerabilities_24.html
https://puppet.com/security/cve/cve-2014-0098
https://support.apple.com/HT204659
https://support.apple.com/kb/HT6535

Summary

The Apache HTTP Server 1.x and 2.x allows remote attackers to cause a denial of service (daemon outage) via partial HTTP requests, as demonstrated by Slowloris, related to the lack of the mod_reqtimeout module in versions before 2.2.15.

CVE-2007-6750 Information	
CVSS Score	5.0
CWE	CWE-399
Vulnerability impact	
Confidentiality	NONE
Integrity	NONE
Availability	PARTIAL
Access methodology information	
Vector	NETWORK
Complexity	LOW
Authentication	NONE

Vulnerable configs

Apache Software Foundation Apache HTTP Server 1.0		
Apache Software Foundation Apache HTTP Server 1.0.2	Apache Software Foundation Apache HTTP Server 1.0.3	Apache Software Foundation Apache HTTP Server 1.0.5
Apache Software Foundation Apache HTTP Server 1.1	Apache Software Foundation Apache HTTP Server 1.1.1	Apache Software Foundation Apache 1.2
Apache Software Foundation Apache HTTP Server 1.2.4	Apache Software Foundation Apache HTTP Server 1.2.5	Apache Software Foundation Apache HTTP Server 1.2.6
Apache Software Foundation Apache 1.29	Apache Software Foundation Apache HTTP Server 1.3	Apache Software Foundation Apache HTTP Server 1.3.0
Apache Software Foundation Apache HTTP Server 1.3.1	Apache Software Foundation Apache HTTP Server 1.3.1.1	Apache Software Foundation Apache HTTP Server 1.3.2
Apache Software Foundation Apache HTTP Server 1.3.3	Apache Software Foundation Apache HTTP Server 1.3.4	Apache Software Foundation Apache HTTP Server 1.3.5
Apache Software Foundation Apache HTTP Server 1.3.6	Apache Software Foundation Apache HTTP Server 1.3.7	Apache Software Foundation Apache HTTP Server 1.3.8
Apache Software Foundation Apache HTTP Server 1.3.9	Apache Software Foundation Apache 1.3.10	Apache Software Foundation Apache HTTP Server 1.3.11
Apache Software Foundation Apache HTTP Server 1.3.12	Apache Software Foundation Apache 1.3.13	Apache Software Foundation Apache HTTP Server 1.3.14
Apache Software Foundation Apache 1.3.15	Apache Software Foundation Apache 1.3.16	Apache Software Foundation Apache HTTP Server 1.3.17
Apache Software Foundation Apache HTTP Server 1.3.18	Apache Software Foundation Apache HTTP Server 1.3.19	Apache Software Foundation Apache HTTP Server 1.3.20
Apache Software Foundation Apache HTTP Server 1.3.22	Apache Software Foundation Apache HTTP Server 1.3.23	Apache Software Foundation Apache HTTP Server 1.3.24
Apache Software Foundation Apache HTTP Server 1.3.25	Apache Software Foundation Apache HTTP Server 1.3.26	Apache Software Foundation Apache HTTP Server 1.3.27
Apache Software Foundation Apache HTTP Server 1.3.28	Apache Software Foundation Apache HTTP Server 1.3.29	Apache Software Foundation Apache HTTP Server 1.3.30
Apache Software Foundation Apache HTTP Server 1.3.31	Apache Software Foundation Apache HTTP Server 1.3.32	Apache Software Foundation Apache HTTP Server 1.3.33
Apache Software Foundation Apache HTTP Server 1.3.34	Apache Software Foundation Apache HTTP Server 1.3.35	Apache Software Foundation Apache HTTP Server 1.3.36
Apache Software Foundation Apache HTTP Server 1.3.37	Apache Software Foundation Apache HTTP Server 1.3.38	Apache Software Foundation Apache HTTP Server 1.3.39
Apache Software Foundation Apache HTTP Server 1.3.41	Apache Software Foundation Apache HTTP Server 1.3.42	Apache Software Foundation Apache HTTP Server 1.3.65
Apache Software Foundation Apache HTTP Server 1.3.68	Apache Software Foundation Apache HTTP Server 1.4.0	Apache Software Foundation Apache HTTP Server 1.99
Apache Software Foundation Apache HTTP Server 2.0	Apache Software Foundation Apache HTTP Server 2.0.9a	Apache Software Foundation Apache HTTP Server 2.0.28
Apache Software Foundation Apache HTTP Server 2.0.28 Beta	Apache Software Foundation Apache HTTP Server 2.0.32	Apache Software Foundation Apache HTTP Server 2.0.32 Beta
Apache Software Foundation Apache HTTP Server 2.0.34 Beta	Apache Software Foundation Apache HTTP Server 2.0.35	Apache Software Foundation Apache HTTP Server 2.0.36
Apache Software Foundation Apache HTTP Server 2.0.37	Apache Software Foundation Apache HTTP Server 2.0.38	Apache Software Foundation Apache HTTP Server 2.0.39
Apache Software Foundation Apache HTTP Server 2.0.40	Apache Software Foundation Apache HTTP Server 2.0.41	Apache Software Foundation Apache HTTP Server 2.0.42
Apache Software Foundation Apache HTTP Server 2.0.43	Apache Software Foundation Apache HTTP Server 2.0.44	Apache Software Foundation Apache HTTP Server 2.0.45
Apache Software Foundation Apache HTTP Server 2.0.46	Apache Software Foundation Apache HTTP Server 2.0.47	Apache Software Foundation Apache HTTP Server 2.0.48
Apache Software Foundation Apache HTTP Server 2.0.49	Apache Software Foundation Apache HTTP Server 2.0.50	Apache Software Foundation Apache HTTP Server 2.0.51
Apache Software Foundation Apache HTTP Server 2.0.52	Apache Software Foundation Apache HTTP Server 2.0.53	Apache Software Foundation Apache HTTP Server 2.0.54
Apache Software Foundation Apache HTTP Server 2.0.55	Apache Software Foundation Apache HTTP Server 2.0.56	Apache Software Foundation Apache HTTP Server 2.0.57
Apache Software Foundation Apache HTTP Server 2.0.58	Apache Software Foundation HTTP Server 2.0.59	Apache Software Foundation Apache HTTP Server 2.0.60 dev
Apache Software Foundation HTTP Server 2.0.61	Apache Software Foundation Apache HTTP Server 2.0.63	Apache Software Foundation Apache HTTP Server 2.1

Apache Software Foundation Apache HTTP Server 2.1.1
Apache Software Foundation Apache HTTP Server 2.1.2
Apache Software Foundation Apache HTTP Server 2.1.3
Apache Software Foundation Apache HTTP Server 2.1.4
Apache Software Foundation Apache HTTP Server 2.1.5
Apache Software Foundation Apache HTTP Server 2.1.6
Apache Software Foundation Apache HTTP Server 2.1.7
Apache Software Foundation Apache HTTP Server 2.1.8
Apache Software Foundation Apache HTTP Server 2.1.9
Apache Software Foundation Apache HTTP Server 2.2
Apache Software Foundation Apache HTTP Server 2.2.0
Apache Software Foundation Apache HTTP Server 2.2.1
Apache Software Foundation Apache HTTP Server 2.2.2
Apache Software Foundation Apache HTTP Server 2.2.3
Apache Software Foundation Apache HTTP Server 2.2.4
Apache Software Foundation Apache HTTP Server 2.2.6
Apache Software Foundation Apache HTTP Server 2.2.8
Apache Software Foundation Apache HTTP Server 2.2.9
Apache Software Foundation Apache HTTP Server 2.2.10
Apache Software Foundation Apache HTTP Server 2.2.11
Apache Software Foundation Apache HTTP Server 2.2.12
Apache Software Foundation Apache HTTP Server 2.2.13
Apache Software Foundation Apache HTTP Server 2.2.14

References

http://archives.neohapsis.com/archives/bugtraq/2007-01/0229.html
http://ha.ckers.org/slowloris/
http://lists.opensuse.org/opensuse-security-announce/2012-02/msg00026.html
http://lists.opensuse.org/opensuse-security-announce/2012-03/msg00002.html
http://marc.info/?l=bugtraq&m=136612293908376&w=2
http://www.securityfocus.com/bid/21865
http://www.securitytracker.com/id/1038144
https://exchange.xforce.ibmcloud.com/vulnerabilities/72345
https://h20566.www2.hpe.com/portal/site/hpsc/public/kb/docDisplay?docId=emr_na-c05111017
https://h20566.www2.hpe.com/portal/site/hpsc/public/kb/docDisplay?docId=emr_na-c05158380

Summary

The (1) mod_cache and (2) mod_dav modules in the Apache HTTP Server 2.2.x before 2.2.16 allow remote attackers to cause a denial of service (process crash) via a request that lacks a path.

CVE-2010-1452 Information	
CVSS Score	5.0
CWE	Unknown
Vulnerability impact	
Confidentiality	NONE
Integrity	NONE
Availability	PARTIAL
Access methodology information	
Vector	NETWORK
Complexity	LOW
Authentication	NONE

Vulnerable configs

Apache Software Foundation Apache HTTP Server
Apache Software Foundation Apache HTTP Server 2.2
Apache Software Foundation Apache HTTP Server 2.2.0
Apache Software Foundation Apache HTTP Server 2.2.1
Apache Software Foundation Apache HTTP Server 2.2.2
Apache Software Foundation Apache HTTP Server 2.2.3
Apache Software Foundation Apache HTTP Server 2.2.4
Apache Software Foundation Apache HTTP Server 2.2.6
cpe:2.3:a:apache:http_server:2.2.7
Apache Software Foundation Apache HTTP Server 2.2.8
Apache Software Foundation Apache HTTP Server 2.2.9
Apache Software Foundation Apache HTTP Server 2.2.10
Apache Software Foundation Apache HTTP Server 2.2.11
Apache Software Foundation Apache HTTP Server 2.2.12
Apache Software Foundation Apache HTTP Server 2.2.13
Apache Software Foundation Apache HTTP Server 2.2.14
Apache Software Foundation Apache HTTP Server 2.2.15

References

http://blogs.sun.com/security/entry/cve_2010_1452_mod_dav
http://httpd.apache.org/security/vulnerabilities_22.html
http://lists.apple.com/archives/security-announce/2011/Mar/msg00006.html
http://lists.opensuse.org/opensuse-security-announce/2011-09/msg00009.html
http://lists.opensuse.org/opensuse-security-announce/2011-11/msg00008.html
http://marc.info/?l=apache-announce&m=128009718610929&w=2
http://marc.info/?l=bugtraq&m=129190899612998&w=2

http://marc.info/?l=bugtraq&m=133355494609819&w=2
http://slackware.com/security/viewer.php?l=slackware-security&y=2010&m=slackware-security.467395
http://support.apple.com/kb/HT4581
http://ubuntu.com/usn/usn-1021-1
http://www.redhat.com/support/errata/RHSA-2010-0659.html
http://www.redhat.com/support/errata/RHSA-2011-0896.html
http://www.redhat.com/support/errata/RHSA-2011-0897.html
http://www.vupen.com/english/advisories/2010/2218
http://www.vupen.com/english/advisories/2010/3064
http://www.vupen.com/english/advisories/2011/0291
https://issues.apache.org/bugzilla/show_bug.cgi?id=49246

Summary

The ap_proxy_ajp_request function in mod_proxy_ajp.c in mod_proxy_ajp in the Apache HTTP Server 2.2.x before 2.2.15 does not properly handle certain situations in which a client sends no request body, which allows remote attackers to cause a denial of service (backend server outage) via a crafted request, related to use of a 500 error code instead of the appropriate 400 error code.

CVE-2010-0408 Information	
CVSS Score	5.0
CWE	Unknown
Vulnerability impact	
Confidentiality	NONE
Integrity	NONE
Availability	PARTIAL
Access methodology information	
Vector	NETWORK
Complexity	LOW
Authentication	NONE

Vulnerable configs

Apache Software Foundation Apache HTTP Server
Apache Software Foundation Apache HTTP Server 2.2
Apache Software Foundation Apache HTTP Server 2.2.0
Apache Software Foundation Apache HTTP Server 2.2.2
Apache Software Foundation Apache HTTP Server 2.2.3
Apache Software Foundation Apache HTTP Server 2.2.4
Apache Software Foundation Apache HTTP Server 2.2.6
Apache Software Foundation Apache HTTP Server 2.2.8
Apache Software Foundation Apache HTTP Server 2.2.9
Apache Software Foundation Apache HTTP Server 2.2.11
Apache Software Foundation Apache HTTP Server 2.2.12
Apache Software Foundation Apache HTTP Server 2.2.13
Apache Software Foundation Apache HTTP Server 2.2.14

References

http://httpd.apache.org/security/vulnerabilities_22.html
http://lists.apple.com/archives/security-announce/2010//Nov/msg00000.html
http://lists.fedoraproject.org/pipermail/package-announce/2010-April/039957.html
http://lists.fedoraproject.org/pipermail/package-announce/2010-May/040652.html
http://lists.opensuse.org/opensuse-security-announce/2010-04/msg00006.html

http://marc.info/?l=bugtraq&m=127557640302499&w=2
http://support.apple.com/kb/HT4435
http://svn.apache.org/viewvc/httpd/httpd/branches/2.2.x/modules/proxy/mod_proxy_ajp.c?r1=917876&r2
http://svn.apache.org/viewvc?view=revision&revision=917876
http://www-01.ibm.com/support/docview.wss?uid=swg1PM08939
http://www-01.ibm.com/support/docview.wss?uid=swg1PM12247
http://www-01.ibm.com/support/docview.wss?uid=swg1PM15829
http://www.debian.org/security/2010/dsa-2035
http://www.mandriva.com/security/advisories?name=MDVSA-2010:053
http://www.mandriva.com/security/advisories?name=MDVSA-2013:150
http://www.oracle.com/technetwork/topics/security/cpuapr2013-1899555.html
http://www.redhat.com/support/errata/RHSA-2010-0168.html
http://www.securityfocus.com/bid/38491
http://www.vupen.com/english/advisories/2010/0911
http://www.vupen.com/english/advisories/2010/0994
http://www.vupen.com/english/advisories/2010/1001
http://www.vupen.com/english/advisories/2010/1057
http://www.vupen.com/english/advisories/2010/1411
https://bugzilla.redhat.com/show_bug.cgi?id=569905

Summary

The Solaris pollset feature in the Event Port backend in poll/unix/port.c in the Apache Portable Runtime (APR) library before 1.3.9, as used in the Apache HTTP Server before 2.2.14 and other products, does not properly handle errors, which allows remote attackers to cause a denial of service (daemon hang) via unspecified HTTP requests, related to the prefork and event MPMs.

CVE-2009-2699 Information	
CVSS Score	5.0
CWE	Unknown
Vulnerability impact	
Confidentiality	NONE
Integrity	NONE
Availability	PARTIAL
Access methodology information	
Vector	NETWORK
Complexity	LOW
Authentication	NONE

Vulnerable configs

Apache Software Foundation Apache HTTP Server

Apache Software Foundation Apache HTTP Server 0.8.11	Apache Software Foundation Apache HTTP Server 0.8.14	Apache Software Foundation Apache HTTP Server 1.0.2
Apache Software Foundation Apache HTTP Server 1.0.3	Apache Software Foundation Apache HTTP Server 1.0.5	Apache Software Foundation Apache HTTP Server 1.1
Apache Software Foundation Apache HTTP Server 1.1.1	Apache Software Foundation Apache 1.2	Apache Software Foundation Apache HTTP Server 1.2.4
Apache Software Foundation Apache HTTP Server 1.2.5	Apache Software Foundation Apache HTTP Server 1.2.6	Apache Software Foundation Apache 1.29
Apache Software Foundation Apache HTTP Server 1.3	Apache Software Foundation Apache HTTP Server 1.3.0	Apache Software Foundation Apache HTTP Server 1.3.1
Apache Software Foundation Apache HTTP Server 1.3.1.1	Apache Software Foundation Apache HTTP Server 1.3.2	Apache Software Foundation Apache HTTP Server 1.3.3
Apache Software Foundation Apache HTTP Server 1.3.4	Apache Software Foundation Apache HTTP Server 1.3.5	Apache Software Foundation Apache HTTP Server 1.3.6
Apache Software Foundation Apache HTTP Server 1.3.7	Apache Software Foundation Apache HTTP Server 1.3.8	Apache Software Foundation Apache HTTP Server 1.3.9
Apache Software Foundation Apache 1.3.10	Apache Software Foundation Apache HTTP Server 1.3.11	Apache Software Foundation Apache HTTP Server 1.3.12
Apache Software Foundation Apache 1.3.13	Apache Software Foundation Apache HTTP Server 1.3.14	Apache Software Foundation Apache 1.3.15
Apache Software Foundation Apache 1.3.16	Apache Software Foundation Apache HTTP Server 1.3.17	Apache Software Foundation Apache HTTP Server 1.3.18
Apache Software Foundation Apache HTTP Server 1.3.19	Apache Software Foundation Apache HTTP Server 1.3.20	Apache Software Foundation Apache HTTP Server 1.3.22
Apache Software Foundation Apache HTTP Server 1.3.23	Apache Software Foundation Apache HTTP Server 1.3.24	Apache Software Foundation Apache HTTP Server 1.3.25
Apache Software Foundation Apache HTTP Server 1.3.26	Apache Software Foundation Apache HTTP Server 1.3.27	Apache Software Foundation Apache HTTP Server 1.3.28
Apache Software Foundation Apache HTTP Server 1.3.29	Apache Software Foundation Apache HTTP Server 1.3.30	Apache Software Foundation Apache HTTP Server 1.3.31
Apache Software Foundation Apache HTTP Server 1.3.32	Apache Software Foundation Apache HTTP Server 1.3.33	Apache Software Foundation Apache HTTP Server 1.3.34
Apache Software Foundation Apache HTTP Server 1.3.35	Apache Software Foundation Apache HTTP Server 1.3.36	Apache Software Foundation Apache HTTP Server 1.3.37
Apache Software Foundation Apache HTTP Server 1.3.38	Apache Software Foundation Apache HTTP Server 1.3.39	Apache Software Foundation Apache HTTP Server 1.3.65
Apache Software Foundation Apache HTTP Server 1.3.68	Apache Software Foundation Apache HTTP Server 1.4.0	Apache Software Foundation Apache HTTP Server 1.99
Apache Software Foundation Apache HTTP Server 2.0	Apache Software Foundation Apache HTTP Server 2.0.9a	Apache Software Foundation Apache HTTP Server 2.0.28
Apache Software Foundation Apache HTTP Server 2.0.32	Apache Software Foundation Apache HTTP Server 2.0.32 Beta	Apache Software Foundation Apache HTTP Server 2.0.34 Beta
Apache Software Foundation Apache HTTP Server 2.0.35	Apache Software Foundation Apache HTTP Server 2.0.36	Apache Software Foundation Apache HTTP Server 2.0.37
Apache Software Foundation Apache HTTP Server 2.0.38	Apache Software Foundation Apache HTTP Server 2.0.39	Apache Software Foundation Apache HTTP Server 2.0.40
Apache Software Foundation Apache HTTP Server 2.0.41	Apache Software Foundation Apache HTTP Server 2.0.42	Apache Software Foundation Apache HTTP Server 2.0.43
Apache Software Foundation Apache HTTP Server 2.0.44	Apache Software Foundation Apache HTTP Server 2.0.45	Apache Software Foundation Apache HTTP Server 2.0.46
Apache Software Foundation Apache HTTP Server 2.0.47	Apache Software Foundation Apache HTTP Server 2.0.48	Apache Software Foundation Apache HTTP Server 2.0.49

Apache Software Foundation Apache HTTP Server 2.0.50 Apache Software Foundation Apache HTTP Server 2.0.51 Apache Software Foundation Apache HTTP Server 2.0.52
Apache Software Foundation Apache HTTP Server 2.0.53 Apache Software Foundation Apache HTTP Server 2.0.54 Apache Software Foundation Apache HTTP Server 2.0.55
Apache Software Foundation Apache HTTP Server 2.0.56 Apache Software Foundation Apache HTTP Server 2.0.57 Apache Software Foundation Apache HTTP Server 2.0.58
Apache Software Foundation HTTP Server 2.0.59 Apache Software Foundation Apache HTTP Server 2.0.60 dev Apache Software Foundation Apache HTTP Server 2.1
Apache Software Foundation Apache HTTP Server 2.1.1 Apache Software Foundation Apache HTTP Server 2.1.2 Apache Software Foundation Apache HTTP Server 2.1.3
Apache Software Foundation Apache HTTP Server 2.1.4 Apache Software Foundation Apache HTTP Server 2.1.5 Apache Software Foundation Apache HTTP Server 2.1.6
Apache Software Foundation Apache HTTP Server 2.1.7 Apache Software Foundation Apache HTTP Server 2.1.8 Apache Software Foundation Apache HTTP Server 2.1.9
Apache Software Foundation Apache HTTP Server 2.2 Apache Software Foundation Apache HTTP Server 2.2.0 Apache Software Foundation Apache HTTP Server 2.2.1
Apache Software Foundation Apache HTTP Server 2.2.2 Apache Software Foundation Apache HTTP Server 2.2.3 Apache Software Foundation Apache HTTP Server 2.2.4
Apache Software Foundation Apache HTTP Server 2.2.6 cpe:2.3:a:apache:http_server:2.2.7 Apache Software Foundation Apache HTTP Server 2.2.8
Apache Software Foundation Apache HTTP Server 2.2.9 Apache Software Foundation Apache HTTP Server 2.2.10 Apache Software Foundation Apache HTTP Server 2.2.11
Apache Software Foundation Apache HTTP Server 2.2.12 Apache Software Foundation Apache HTTP Server 2.2.13 cpe:2.3:a:apache:apr:0.9.7
cpe:2.3:a:apache:apr:0.9.17 cpe:2.3:a:apache:apr:0.9.18 cpe:2.3:a:apache:apr:1.2.1
cpe:2.3:a:apache:apr:1.3.8

References

http://marc.info/?l=bugtraq&m=133355494609819&w=2

http://securitytracker.com/id?1022988

http://www.apache.org/dist/httpd/CHANGES_2.2.14

http://www.mandriva.com/security/advisories?name=MDVSA-2013:150

http://www.oracle.com/technetwork/topics/security/cpuapr2013-1899555.html

http://www.securityfocus.com/bid/36596

https://exchange.xforce.ibmcloud.com/vulnerabilities/53666

https://issues.apache.org/bugzilla/show_bug.cgi?id=47645

Summary

The Apache HTTP Server 2.2.11 and earlier 2.2 versions does not properly handle Options=IncludesNOEXEC in the AllowOverride directive, which allows local users to gain privileges by configuring (1) Options Includes, (2) Options +Includes, or (3) Options +IncludesNOEXEC in a .htaccess file, and then inserting an exec element in a .shtml file.

CVE-2009-1195 Information	
CVSS Score	4.9
CWE	CWE-16
Vulnerability impact	
Confidentiality	NONE
Integrity	NONE
Availability	COMPLETE
Access methodology information	
Vector	LOCAL
Complexity	LOW
Authentication	NONE

Vulnerable configs

Apache Software Foundation Apache HTTP Server
Apache Software Foundation Apache HTTP Server 2.2
Apache Software Foundation Apache HTTP Server 2.2.0
Apache Software Foundation Apache HTTP Server 2.2.1
Apache Software Foundation Apache HTTP Server 2.2.2
cpe:2.3:a:apache:http_server:2.2.2:-:windows
Apache Software Foundation Apache HTTP Server 2.2.3
cpe:2.3:a:apache:http_server:2.2.3:-:windows
Apache Software Foundation Apache HTTP Server 2.2.4
Apache Software Foundation Apache HTTP Server 2.2.6
cpe:2.3:a:apache:http_server:2.2.7
Apache Software Foundation Apache HTTP Server 2.2.8
Apache Software Foundation Apache HTTP Server 2.2.9
Apache Software Foundation Apache HTTP Server 2.2.10
Apache Software Foundation Apache HTTP Server 2.2.11

References

http://lists.apple.com/archives/security-announce/2009/Nov/msg00000.html
http://lists.opensuse.org/opensuse-security-announce/2009-10/msg00006.html
http://marc.info/?l=apache-httpd-dev&m=124048996106302&w=2
http://marc.info/?l=bugtraq&m=129190899612998&w=2
http://security.gentoo.org/glsa/glsa-200907-04.xml
http://support.apple.com/kb/HT3937

http://svn.apache.org/viewvc?view=rev&revision=772997
http://wiki.rpath.com/Advisories:rPSA-2009-0142
http://www.debian.org/security/2009/dsa-1816
http://www.mandriva.com/security/advisories?name=MDVSA-2009:124
http://www.redhat.com/support/errata/RHSA-2009-1075.html
http://www.redhat.com/support/errata/RHSA-2009-1156.html
http://www.securityfocus.com/archive/1/507852/100/0/threaded
http://www.securityfocus.com/archive/1/507857/100/0/threaded
http://www.securityfocus.com/bid/35115
http://www.securitytracker.com/id?1022296
http://www.ubuntu.com/usn/usn-787-1
http://www.vupen.com/english/advisories/2009/1444
http://www.vupen.com/english/advisories/2009/3184
https://bugzilla.redhat.com/show_bug.cgi?id=489436
https://exchange.xforce.ibmcloud.com/vulnerabilities/50808
https://www.redhat.com/archives/fedora-package-announce/2009-August/msg01363.html

Summary

scoreboard.c in the Apache HTTP Server 2.2.21 and earlier might allow local users to cause a denial of service (daemon crash during shutdown) or possibly have unspecified other impact by modifying a certain type field within a scoreboard shared memory segment, leading to an invalid call to the free function.

CVE-2012-0031 Information	
CVSS Score	4.6
CWE	CWE-399
Vulnerability impact	
Confidentiality	PARTIAL
Integrity	PARTIAL
Availability	PARTIAL
Access methodology information	
Vector	LOCAL
Complexity	LOW
Authentication	NONE

Vulnerable configs

Apache Software Foundation Apache HTTP Server 1.0		Apache Software Foundation Apache HTTP Server 1.0.2
Apache Software Foundation Apache HTTP Server 1.0.3	Apache Software Foundation Apache HTTP Server 1.0.5	Apache Software Foundation Apache HTTP Server 1.1
Apache Software Foundation Apache HTTP Server 1.1.1	Apache Software Foundation Apache 1.2	Apache Software Foundation Apache HTTP Server 1.2.4
Apache Software Foundation Apache HTTP Server 1.2.5	Apache Software Foundation Apache HTTP Server 1.2.6	Apache Software Foundation Apache 1.29
Apache Software Foundation Apache HTTP Server 1.3	Apache Software Foundation Apache HTTP Server 1.3.0	Apache Software Foundation Apache HTTP Server 1.3.1
Apache Software Foundation Apache HTTP Server 1.3.1.1	Apache Software Foundation Apache HTTP Server 1.3.2	Apache Software Foundation Apache HTTP Server 1.3.3
Apache Software Foundation Apache HTTP Server 1.3.4	Apache Software Foundation Apache HTTP Server 1.3.5	Apache Software Foundation Apache HTTP Server 1.3.6
Apache Software Foundation Apache HTTP Server 1.3.7	Apache Software Foundation Apache HTTP Server 1.3.8	Apache Software Foundation Apache HTTP Server 1.3.9
Apache Software Foundation Apache 1.3.10	Apache Software Foundation Apache HTTP Server 1.3.11	Apache Software Foundation Apache HTTP Server 1.3.12
Apache Software Foundation Apache 1.3.13	Apache Software Foundation Apache HTTP Server 1.3.14	Apache Software Foundation Apache 1.3.15
Apache Software Foundation Apache 1.3.16	Apache Software Foundation Apache HTTP Server 1.3.17	Apache Software Foundation Apache HTTP Server 1.3.18
Apache Software Foundation Apache HTTP Server 1.3.19	Apache Software Foundation Apache HTTP Server 1.3.20	Apache Software Foundation Apache HTTP Server 1.3.22
Apache Software Foundation Apache HTTP Server 1.3.23	Apache Software Foundation Apache HTTP Server 1.3.24	Apache Software Foundation Apache HTTP Server 1.3.25
Apache Software Foundation Apache HTTP Server 1.3.26	Apache Software Foundation Apache HTTP Server 1.3.27	Apache Software Foundation Apache HTTP Server 1.3.28
Apache Software Foundation Apache HTTP Server 1.3.29	Apache Software Foundation Apache HTTP Server 1.3.30	Apache Software Foundation Apache HTTP Server 1.3.31
Apache Software Foundation Apache HTTP Server 1.3.32	Apache Software Foundation Apache HTTP Server 1.3.33	Apache Software Foundation Apache HTTP Server 1.3.34
Apache Software Foundation Apache HTTP Server 1.3.35	Apache Software Foundation Apache HTTP Server 1.3.36	Apache Software Foundation Apache HTTP Server 1.3.37
Apache Software Foundation Apache HTTP Server 1.3.38	Apache Software Foundation Apache HTTP Server 1.3.39	Apache Software Foundation Apache HTTP Server 1.3.41
Apache Software Foundation Apache HTTP Server 1.3.42	Apache Software Foundation Apache HTTP Server 1.3.65	Apache Software Foundation Apache HTTP Server 1.3.68
Apache Software Foundation Apache HTTP Server 1.4.0	Apache Software Foundation Apache HTTP Server 1.99	Apache Software Foundation Apache HTTP Server 2.0
Apache Software Foundation Apache HTTP Server 2.0.9a	Apache Software Foundation Apache HTTP Server 2.0.28	Apache Software Foundation Apache HTTP Server 2.0.28 Beta
Apache Software Foundation Apache HTTP Server 2.0.32	Apache Software Foundation Apache HTTP Server 2.0.32 Beta	Apache Software Foundation Apache HTTP Server 2.0.34 Beta
Apache Software Foundation Apache HTTP Server 2.0.35	Apache Software Foundation Apache HTTP Server 2.0.36	Apache Software Foundation Apache HTTP Server 2.0.37
Apache Software Foundation Apache HTTP Server 2.0.38	Apache Software Foundation Apache HTTP Server 2.0.39	Apache Software Foundation Apache HTTP Server 2.0.40
Apache Software Foundation Apache HTTP Server 2.0.41	Apache Software Foundation Apache HTTP Server 2.0.42	Apache Software Foundation Apache HTTP Server 2.0.43
Apache Software Foundation Apache HTTP Server 2.0.44	Apache Software Foundation Apache HTTP Server 2.0.45	Apache Software Foundation Apache HTTP Server 2.0.46
Apache Software Foundation Apache HTTP Server 2.0.47	Apache Software Foundation Apache HTTP Server 2.0.48	Apache Software Foundation Apache HTTP Server 2.0.49
Apache Software Foundation Apache HTTP Server 2.0.50	Apache Software Foundation Apache HTTP Server 2.0.51	Apache Software Foundation Apache HTTP Server 2.0.52
Apache Software Foundation Apache HTTP Server 2.0.53	Apache Software Foundation Apache HTTP Server 2.0.54	Apache Software Foundation Apache HTTP Server 2.0.55
Apache Software Foundation Apache HTTP Server 2.0.56	Apache Software Foundation Apache HTTP Server 2.0.57	Apache Software Foundation Apache HTTP Server 2.0.58

Apache Software Foundation HTTP Server 2.0.59
Apache Software Foundation Apache HTTP Server 2.0.60 dev
Apache Software Foundation HTTP Server 2.0.61
Apache Software Foundation Apache HTTP Server 2.0.63
Apache Software Foundation Apache HTTP Server 2.1
Apache Software Foundation Apache HTTP Server 2.1.1
Apache Software Foundation Apache HTTP Server 2.1.2
Apache Software Foundation Apache HTTP Server 2.1.3
Apache Software Foundation Apache HTTP Server 2.1.4
Apache Software Foundation Apache HTTP Server 2.1.5
Apache Software Foundation Apache HTTP Server 2.1.6
Apache Software Foundation Apache HTTP Server 2.1.7
Apache Software Foundation Apache HTTP Server 2.1.8
Apache Software Foundation Apache HTTP Server 2.1.9
Apache Software Foundation Apache HTTP Server 2.2
Apache Software Foundation Apache HTTP Server 2.2.0
Apache Software Foundation Apache HTTP Server 2.2.1
Apache Software Foundation Apache HTTP Server 2.2.2
Apache Software Foundation Apache HTTP Server 2.2.3
Apache Software Foundation Apache HTTP Server 2.2.4
Apache Software Foundation Apache HTTP Server 2.2.6
Apache Software Foundation Apache HTTP Server 2.2.8
Apache Software Foundation Apache HTTP Server 2.2.9
Apache Software Foundation Apache HTTP Server 2.2.10
Apache Software Foundation Apache HTTP Server 2.2.11
Apache Software Foundation Apache HTTP Server 2.2.12
Apache Software Foundation Apache HTTP Server 2.2.13
Apache Software Foundation Apache HTTP Server 2.2.14
Apache Software Foundation Apache HTTP Server 2.2.15
Apache Software Foundation Apache HTTP Server 2.2.16
Apache Software Foundation Apache HTTP Server 2.2.17
Apache Software Foundation Apache HTTP Server 2.2.18
Apache Software Foundation Apache HTTP Server 2.2.19
Apache Software Foundation Apache HTTP Server 2.2.20
Apache HTTP Server 2.2.21

References

http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=c03360041

http://lists.apple.com/archives/security-announce/2012/Sep/msg00004.html

http://lists.opensuse.org/opensuse-security-announce/2012-02/msg00026.html

http://lists.opensuse.org/opensuse-security-announce/2012-03/msg00002.html

http://marc.info/?l=bugtraq&m=133294460209056&w=2

http://marc.info/?l=bugtraq&m=133494237717847&w=2

http://marc.info/?l=bugtraq&m=134987041210674&w=2

http://rhn.redhat.com/errata/RHSA-2012-0128.html

http://rhn.redhat.com/errata/RHSA-2012-0542.html

http://rhn.redhat.com/errata/RHSA-2012-0543.html

http://support.apple.com/kb/HT5501

http://svn.apache.org/viewvc?view=revision&revision=1230065

http://www.debian.org/security/2012/dsa-2405

http://www.halfdog.net/Security/2011/ApacheScoreboardInvalidFreeOnShutdown/

http://www.mandriva.com/security/advisories?name=MDVSA-2012:012

http://www.mandriva.com/security/advisories?name=MDVSA-2013:150

http://www.oracle.com/technetwork/topics/security/cpujul2012-392727.html

http://www.securityfocus.com/bid/51407

https://bugzilla.redhat.com/show_bug.cgi?id=773744

Summary

Integer overflow in the ap_pregsub function in server/util.c in the Apache HTTP Server 2.0.x through 2.0.64 and 2.2.x through 2.2.21, when the mod_setenvif module is enabled, allows local users to gain privileges via a .htaccess file with a crafted SetEnvIf directive, in conjunction with a crafted HTTP request header, leading to a heap-based buffer overflow.

CVE-2011-3607 Information	
CVSS Score	4.4
CWE	CWE-189
Vulnerability impact	
Confidentiality	PARTIAL
Integrity	PARTIAL
Availability	PARTIAL
Access methodology information	
Vector	LOCAL
Complexity	MEDIUM
Authentication	NONE

Vulnerable configs

Apache Software Foundation Apache HTTP Server 2.0		
Apache Software Foundation Apache HTTP Server 2.0.9a	Apache Software Foundation Apache HTTP Server 2.0.28	Apache Software Foundation Apache HTTP Server 2.0.28 Beta
Apache Software Foundation Apache HTTP Server 2.0.32	Apache Software Foundation Apache HTTP Server 2.0.32 Beta	Apache Software Foundation Apache HTTP Server 2.0.34 Beta
Apache Software Foundation Apache HTTP Server 2.0.35	Apache Software Foundation Apache HTTP Server 2.0.36	Apache Software Foundation Apache HTTP Server 2.0.37
Apache Software Foundation Apache HTTP Server 2.0.38	Apache Software Foundation Apache HTTP Server 2.0.39	Apache Software Foundation Apache HTTP Server 2.0.40
Apache Software Foundation Apache HTTP Server 2.0.41	Apache Software Foundation Apache HTTP Server 2.0.42	Apache Software Foundation Apache HTTP Server 2.0.43
Apache Software Foundation Apache HTTP Server 2.0.44	Apache Software Foundation Apache HTTP Server 2.0.45	Apache Software Foundation Apache HTTP Server 2.0.46
Apache Software Foundation Apache HTTP Server 2.0.47	Apache Software Foundation Apache HTTP Server 2.0.48	Apache Software Foundation Apache HTTP Server 2.0.49
Apache Software Foundation Apache HTTP Server 2.0.50	Apache Software Foundation Apache HTTP Server 2.0.51	Apache Software Foundation Apache HTTP Server 2.0.52
Apache Software Foundation Apache HTTP Server 2.0.53	Apache Software Foundation Apache HTTP Server 2.0.54	Apache Software Foundation Apache HTTP Server 2.0.55
Apache Software Foundation Apache HTTP Server 2.0.56	Apache Software Foundation Apache HTTP Server 2.0.57	Apache Software Foundation Apache HTTP Server 2.0.58
Apache Software Foundation HTTP Server 2.0.59	Apache Software Foundation Apache HTTP Server 2.0.60 dev	Apache Software Foundation HTTP Server 2.0.61
Apache Software Foundation Apache HTTP Server 2.0.63	Apache Software Foundation Apache HTTP Server 2.0.64	Apache Software Foundation Apache HTTP Server 2.2.0
Apache Software Foundation Apache HTTP Server 2.2.1	Apache Software Foundation Apache HTTP Server 2.2.2	Apache Software Foundation Apache HTTP Server 2.2.3
Apache Software Foundation Apache HTTP Server 2.2.4	Apache Software Foundation Apache HTTP Server 2.2.6	Apache Software Foundation Apache HTTP Server 2.2.8
Apache Software Foundation Apache HTTP Server 2.2.9	Apache Software Foundation Apache HTTP Server 2.2.10	Apache Software Foundation Apache HTTP Server 2.2.11
Apache Software Foundation Apache HTTP Server 2.2.12	Apache Software Foundation Apache HTTP Server 2.2.13	Apache Software Foundation Apache HTTP Server 2.2.14
Apache Software Foundation Apache HTTP Server 2.2.15	Apache Software Foundation Apache HTTP Server 2.2.16	Apache Software Foundation Apache HTTP Server 2.2.18
Apache Software Foundation Apache HTTP Server 2.2.19	Apache Software Foundation Apache HTTP Server 2.2.20	Apache HTTP Server 2.2.21

References

http://archives.neohapsis.com/archives/fulldisclosure/2011-11/0023.html

http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=c03360041
http://lists.apple.com/archives/security-announce/2012/Sep/msg00004.html
http://marc.info/?l=bugtraq&m=133294460209056&w=2
http://marc.info/?l=bugtraq&m=133494237717847&w=2
http://marc.info/?l=bugtraq&m=134987041210674&w=2
http://rhn.redhat.com/errata/RHSA-2012-0128.html
http://rhn.redhat.com/errata/RHSA-2012-0542.html
http://rhn.redhat.com/errata/RHSA-2012-0543.html
http://securitytracker.com/id?1026267
http://support.apple.com/kb/HT5501
http://www.debian.org/security/2012/dsa-2405
http://www.fujitsu.com/global/support/software/security/products-f/interstage-201303e.html
http://www.halfdog.net/Security/2011/ApacheModSetEnvIfIntegerOverflow/
http://www.halfdog.net/Security/2011/ApacheModSetEnvIfIntegerOverflow/DemoExploit.html
http://www.mandriva.com/security/advisories?name=MDVSA-2012:003
http://www.mandriva.com/security/advisories?name=MDVSA-2013:150
http://www.oracle.com/technetwork/topics/security/cpujan2015-1972971.html
http://www.oracle.com/technetwork/topics/security/cpujul2012-392727.html
http://www.securityfocus.com/bid/50494
https://bugs.launchpad.net/ubuntu/+source/apache2/+bug/811422
https://bugzilla.redhat.com/show_bug.cgi?id=750935
https://exchange.xforce.ibmcloud.com/vulnerabilities/71093

Summary

The mod_proxy module in the Apache HTTP Server 1.3.x through 1.3.42, 2.0.x through 2.0.64, and 2.2.x through 2.2.21, when the Revision 1179239 patch is in place, does not properly interact with use of (1) RewriteRule and (2) ProxyPassMatch pattern matches for configuration of a reverse proxy, which allows remote attackers to send requests to intranet servers via a malformed URI containing an @ (at sign) character and a : (colon) character in invalid positions. NOTE: this vulnerability exists because of an incomplete fix for CVE-2011-3368.

CVE-2011-4317 Information	
CVSS Score	4.3
CWE	CWE-20
Vulnerability impact	
Confidentiality	NONE
Integrity	PARTIAL
Availability	NONE
Access methodology information	
Vector	NETWORK
Complexity	MEDIUM
Authentication	NONE

Vulnerable configs

Apache Software Foundation Apache HTTP Server 1.3	Apache Software Foundation Apache HTTP Server 1.3.0	Apache Software Foundation Apache HTTP Server 1.3.1
Apache Software Foundation Apache HTTP Server 1.3.1.1	Apache Software Foundation Apache HTTP Server 1.3.2	Apache Software Foundation Apache HTTP Server 1.3.3
Apache Software Foundation Apache HTTP Server 1.3.4	Apache Software Foundation Apache HTTP Server 1.3.5	Apache Software Foundation Apache HTTP Server 1.3.6
Apache Software Foundation Apache HTTP Server 1.3.7	Apache Software Foundation Apache HTTP Server 1.3.8	Apache Software Foundation Apache HTTP Server 1.3.9
Apache Software Foundation Apache 1.3.10	Apache Software Foundation Apache HTTP Server 1.3.11	Apache Software Foundation Apache HTTP Server 1.3.12
Apache Software Foundation Apache 1.3.13	Apache Software Foundation Apache HTTP Server 1.3.14	Apache Software Foundation Apache 1.3.15
Apache Software Foundation Apache 1.3.16	Apache Software Foundation Apache HTTP Server 1.3.17	Apache Software Foundation Apache HTTP Server 1.3.18
Apache Software Foundation Apache HTTP Server 1.3.19	Apache Software Foundation Apache HTTP Server 1.3.20	Apache Software Foundation Apache HTTP Server 1.3.22
Apache Software Foundation Apache HTTP Server 1.3.23	Apache Software Foundation Apache HTTP Server 1.3.24	Apache Software Foundation Apache HTTP Server 1.3.25
Apache Software Foundation Apache HTTP Server 1.3.26	Apache Software Foundation Apache HTTP Server 1.3.27	Apache Software Foundation Apache HTTP Server 1.3.28
Apache Software Foundation Apache HTTP Server 1.3.29	Apache Software Foundation Apache HTTP Server 1.3.30	Apache Software Foundation Apache HTTP Server 1.3.31
Apache Software Foundation Apache HTTP Server 1.3.32	Apache Software Foundation Apache HTTP Server 1.3.33	Apache Software Foundation Apache HTTP Server 1.3.34
Apache Software Foundation Apache HTTP Server 1.3.35	Apache Software Foundation Apache HTTP Server 1.3.36	Apache Software Foundation Apache HTTP Server 1.3.37
Apache Software Foundation Apache HTTP Server 1.3.38	Apache Software Foundation Apache HTTP Server 1.3.39	Apache Software Foundation Apache HTTP Server 1.3.41
Apache Software Foundation Apache HTTP Server 1.3.42	Apache Software Foundation Apache HTTP Server 1.3.65	Apache Software Foundation Apache HTTP Server 1.3.68
Apache Software Foundation Apache HTTP Server 2.0	Apache Software Foundation Apache HTTP Server 2.0.9a	Apache Software Foundation Apache HTTP Server 2.0.28
Apache Software Foundation Apache HTTP Server 2.0.28 Beta	Apache Software Foundation Apache HTTP Server 2.0.32	Apache Software Foundation Apache HTTP Server 2.0.32 Beta
Apache Software Foundation Apache HTTP Server 2.0.34 Beta	Apache Software Foundation Apache HTTP Server 2.0.35	Apache Software Foundation Apache HTTP Server 2.0.36
Apache Software Foundation Apache HTTP Server 2.0.37	Apache Software Foundation Apache HTTP Server 2.0.38	Apache Software Foundation Apache HTTP Server 2.0.39
Apache Software Foundation Apache HTTP Server 2.0.40	Apache Software Foundation Apache HTTP Server 2.0.41	Apache Software Foundation Apache HTTP Server 2.0.42
Apache Software Foundation Apache HTTP Server 2.0.43	Apache Software Foundation Apache HTTP Server 2.0.44	Apache Software Foundation Apache HTTP Server 2.0.45
Apache Software Foundation Apache HTTP Server 2.0.46	Apache Software Foundation Apache HTTP Server 2.0.47	Apache Software Foundation Apache HTTP Server 2.0.48
Apache Software Foundation Apache HTTP Server 2.0.49	Apache Software Foundation Apache HTTP Server 2.0.50	Apache Software Foundation Apache HTTP Server 2.0.51
Apache Software Foundation Apache HTTP Server 2.0.52	Apache Software Foundation Apache HTTP Server 2.0.53	Apache Software Foundation Apache HTTP Server 2.0.54

Apache Software Foundation Apache HTTP Server 2.0.55 Apache Software Foundation Apache HTTP Server 2.0.56 Apache Software Foundation Apache HTTP Server 2.0.57
Apache Software Foundation Apache HTTP Server 2.0.58 Apache Software Foundation HTTP Server 2.0.59 Apache Software Foundation Apache HTTP Server 2.0.60 dev
Apache Software Foundation HTTP Server 2.0.61 Apache Software Foundation Apache HTTP Server 2.0.63 Apache Software Foundation Apache HTTP Server 2.0.64
Apache Software Foundation Apache HTTP Server 2.2.0 Apache Software Foundation Apache HTTP Server 2.2.1 Apache Software Foundation Apache HTTP Server 2.2.2
Apache Software Foundation Apache HTTP Server 2.2.3 Apache Software Foundation Apache HTTP Server 2.2.4 Apache Software Foundation Apache HTTP Server 2.2.6
Apache Software Foundation Apache HTTP Server 2.2.8 Apache Software Foundation Apache HTTP Server 2.2.9 Apache Software Foundation Apache HTTP Server 2.2.10
Apache Software Foundation Apache HTTP Server 2.2.11 Apache Software Foundation Apache HTTP Server 2.2.12 Apache Software Foundation Apache HTTP Server 2.2.13
Apache Software Foundation Apache HTTP Server 2.2.14 Apache Software Foundation Apache HTTP Server 2.2.15 Apache Software Foundation Apache HTTP Server 2.2.16
Apache Software Foundation Apache HTTP Server 2.2.18 Apache Software Foundation Apache HTTP Server 2.2.19 Apache Software Foundation Apache HTTP Server 2.2.20
Apache HTTP Server 2.2.21

References

http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=c03360041
http://kb.juniper.net/JSA10585
http://lists.apple.com/archives/security-announce/2012/Sep/msg00004.html
http://lists.opensuse.org/opensuse-updates/2013-02/msg00009.html
http://lists.opensuse.org/opensuse-updates/2013-02/msg00012.html
http://marc.info/?l=bugtraq&m=133294460209056&w=2
http://marc.info/?l=bugtraq&m=134987041210674&w=2
http://rhn.redhat.com/errata/RHSA-2012-0128.html
http://support.apple.com/kb/HT5501
http://thread.gmane.org/gmane.comp.apache.devel/46440
http://www.debian.org/security/2012/dsa-2405
http://www.mandriva.com/security/advisories?name=MDVSA-2012:003
http://www.mandriva.com/security/advisories?name=MDVSA-2013:150
http://www.oracle.com/technetwork/topics/security/cpujan2015-1972971.html
http://www.oracle.com/technetwork/topics/security/cpujul2012-392727.html
http://www.securitytracker.com/id?1026353
https://bugzilla.redhat.com/show_bug.cgi?id=756483
https://community.qualys.com/blogs/securitylabs/2011/11/23/apache-reverse-proxy-bypass-issue

Summary

The mod_proxy_ajp module in the Apache HTTP Server before 2.2.21, when used with mod_proxy_balancer in certain configurations, allows remote attackers to cause a denial of service (temporary "error state" in the backend server) via a malformed HTTP request.

CVE-2011-3348 Information	
CVSS Score	4.3
CWE	CWE-399
Vulnerability impact	
Confidentiality	NONE
Integrity	NONE
Availability	PARTIAL
Access methodology information	
Vector	NETWORK
Complexity	MEDIUM
Authentication	NONE

Vulnerable configs

Apache Software Foundation Apache HTTP Server 0.8.11		Apache Software Foundation Apache HTTP Server 0.8.14
Apache Software Foundation Apache HTTP Server 1.0	Apache Software Foundation Apache HTTP Server 1.0.2	Apache Software Foundation Apache HTTP Server 1.0.3
Apache Software Foundation Apache HTTP Server 1.0.5	Apache Software Foundation Apache HTTP Server 1.1	Apache Software Foundation Apache HTTP Server 1.1.1
Apache Software Foundation Apache 1.2	Apache Software Foundation Apache HTTP Server 1.2.4	Apache Software Foundation Apache HTTP Server 1.2.5
Apache Software Foundation Apache HTTP Server 1.2.6	Apache Software Foundation Apache 1.29	Apache Software Foundation Apache HTTP Server 1.3
Apache Software Foundation Apache HTTP Server 1.3.0	Apache Software Foundation Apache HTTP Server 1.3.1	Apache Software Foundation Apache HTTP Server 1.3.1.1
Apache Software Foundation Apache HTTP Server 1.3.2	Apache Software Foundation Apache HTTP Server 1.3.3	Apache Software Foundation Apache HTTP Server 1.3.4
Apache Software Foundation Apache HTTP Server 1.3.5	Apache Software Foundation Apache HTTP Server 1.3.6	Apache Software Foundation Apache HTTP Server 1.3.7
Apache Software Foundation Apache HTTP Server 1.3.8	Apache Software Foundation Apache HTTP Server 1.3.9	Apache Software Foundation Apache 1.3.10
Apache Software Foundation Apache HTTP Server 1.3.11	Apache Software Foundation Apache HTTP Server 1.3.12	Apache Software Foundation Apache 1.3.13
Apache Software Foundation Apache HTTP Server 1.3.14	Apache Software Foundation Apache 1.3.15	Apache Software Foundation Apache 1.3.16
Apache Software Foundation Apache HTTP Server 1.3.17	Apache Software Foundation Apache HTTP Server 1.3.18	Apache Software Foundation Apache HTTP Server 1.3.19
Apache Software Foundation Apache HTTP Server 1.3.20	Apache Software Foundation Apache HTTP Server 1.3.22	Apache Software Foundation Apache HTTP Server 1.3.23
Apache Software Foundation Apache HTTP Server 1.3.24	Apache Software Foundation Apache HTTP Server 1.3.25	Apache Software Foundation Apache HTTP Server 1.3.26
Apache Software Foundation Apache HTTP Server 1.3.27	Apache Software Foundation Apache HTTP Server 1.3.28	Apache Software Foundation Apache HTTP Server 1.3.29
Apache Software Foundation Apache HTTP Server 1.3.30	Apache Software Foundation Apache HTTP Server 1.3.31	Apache Software Foundation Apache HTTP Server 1.3.32
Apache Software Foundation Apache HTTP Server 1.3.33	Apache Software Foundation Apache HTTP Server 1.3.34	Apache Software Foundation Apache HTTP Server 1.3.35
Apache Software Foundation Apache HTTP Server 1.3.36	Apache Software Foundation Apache HTTP Server 1.3.37	Apache Software Foundation Apache HTTP Server 1.3.38
Apache Software Foundation Apache HTTP Server 1.3.39	Apache Software Foundation Apache HTTP Server 1.3.41	Apache Software Foundation Apache HTTP Server 1.3.42
Apache Software Foundation Apache HTTP Server 1.3.65	Apache Software Foundation Apache HTTP Server 1.3.68	Apache Software Foundation Apache HTTP Server 1.4.0
Apache Software Foundation Apache HTTP Server 1.99	Apache Software Foundation Apache HTTP Server 2.0	Apache Software Foundation Apache HTTP Server 2.0.9a
Apache Software Foundation Apache HTTP Server 2.0.28	Apache Software Foundation Apache HTTP Server 2.0.28 Beta	Apache Software Foundation Apache HTTP Server 2.0.32
Apache Software Foundation Apache HTTP Server 2.0.32 Beta	Apache Software Foundation Apache HTTP Server 2.0.34 Beta	Apache Software Foundation Apache HTTP Server 2.0.35
Apache Software Foundation Apache HTTP Server 2.0.36	Apache Software Foundation Apache HTTP Server 2.0.37	Apache Software Foundation Apache HTTP Server 2.0.38
Apache Software Foundation Apache HTTP Server 2.0.39	Apache Software Foundation Apache HTTP Server 2.0.40	Apache Software Foundation Apache HTTP Server 2.0.41
Apache Software Foundation Apache HTTP Server 2.0.42	Apache Software Foundation Apache HTTP Server 2.0.43	Apache Software Foundation Apache HTTP Server 2.0.44
Apache Software Foundation Apache HTTP Server 2.0.45	Apache Software Foundation Apache HTTP Server 2.0.46	Apache Software Foundation Apache HTTP Server 2.0.47
Apache Software Foundation Apache HTTP Server 2.0.48	Apache Software Foundation Apache HTTP Server 2.0.49	Apache Software Foundation Apache HTTP Server 2.0.50
Apache Software Foundation Apache HTTP Server 2.0.51	Apache Software Foundation Apache HTTP Server 2.0.52	Apache Software Foundation Apache HTTP Server 2.0.53
Apache Software Foundation Apache HTTP Server 2.0.54	Apache Software Foundation Apache HTTP Server 2.0.55	Apache Software Foundation Apache HTTP Server 2.0.56
Apache Software Foundation Apache HTTP Server 2.0.57	Apache Software Foundation Apache HTTP Server 2.0.58	Apache Software Foundation HTTP Server 2.0.59
Apache Software Foundation Apache HTTP Server 2.0.60 dev	Apache Software Foundation HTTP Server 2.0.61	Apache Software Foundation Apache HTTP Server 2.0.63

Apache Software Foundation Apache HTTP Server 2.1
Apache Software Foundation Apache HTTP Server 2.1.1
Apache Software Foundation Apache HTTP Server 2.1.2
Apache Software Foundation Apache HTTP Server 2.1.3
Apache Software Foundation Apache HTTP Server 2.1.4
Apache Software Foundation Apache HTTP Server 2.1.5
Apache Software Foundation Apache HTTP Server 2.1.6
Apache Software Foundation Apache HTTP Server 2.1.7
Apache Software Foundation Apache HTTP Server 2.1.8
Apache Software Foundation Apache HTTP Server 2.1.9
Apache Software Foundation Apache HTTP Server 2.2
Apache Software Foundation Apache HTTP Server 2.2.0
Apache Software Foundation Apache HTTP Server 2.2.1
Apache Software Foundation Apache HTTP Server 2.2.2
Apache Software Foundation Apache HTTP Server 2.2.3
Apache Software Foundation Apache HTTP Server 2.2.4
Apache Software Foundation Apache HTTP Server 2.2.6
Apache Software Foundation Apache HTTP Server 2.2.8
Apache Software Foundation Apache HTTP Server 2.2.9
Apache Software Foundation Apache HTTP Server 2.2.10
Apache Software Foundation Apache HTTP Server 2.2.11
Apache Software Foundation Apache HTTP Server 2.2.12
Apache Software Foundation Apache HTTP Server 2.2.13
Apache Software Foundation Apache HTTP Server 2.2.14
Apache Software Foundation Apache HTTP Server 2.2.15
Apache Software Foundation Apache HTTP Server 2.2.16
Apache Software Foundation Apache HTTP Server 2.2.17
Apache Software Foundation Apache HTTP Server 2.2.18
Apache Software Foundation Apache HTTP Server 2.2.20

References

http://community.jboss.org/message/625307
http://httpd.apache.org/security/vulnerabilities_22.html##2.2.21
http://lists.apple.com/archives/security-announce/2012/Feb/msg00000.html
http://marc.info/?l=bugtraq&m=131731002122529&w=2
http://marc.info/?l=bugtraq&m=132033751509019&w=2
http://rhn.redhat.com/errata/RHSA-2012-0542.html
http://rhn.redhat.com/errata/RHSA-2012-0543.html
http://support.apple.com/kb/HT5130
http://www.apache.org/dist/httpd/Announcement2.2.html
http://www.mandriva.com/security/advisories?name=MDVSA-2011:168
http://www.oracle.com/technetwork/topics/security/cpujuly2013-1899826.html
http://www.redhat.com/support/errata/RHSA-2011-1391.html
http://www.securityfocus.com/bid/49616
http://www.securitytracker.com/id?1026054
https://exchange.xforce.ibmcloud.com/vulnerabilities/69804

Summary

Stack consumption vulnerability in the fnmatch implementation in apr_fnmatch.c in the Apache Portable Runtime (APR) library before 1.4.3 and the Apache HTTP Server before 2.2.18, and in fnmatch.c in libc in NetBSD 5.1, OpenBSD 4.8, FreeBSD, Apple Mac OS X 10.6, Oracle Solaris 10, and Android, allows context-dependent attackers to cause a denial of service (CPU and memory consumption) via *? sequences in the first argument, as demonstrated by attacks against mod_autoindex in httpd.

CVE-2011-0419 Information	
CVSS Score	4.3
CWE	CWE-399
Vulnerability impact	
Confidentiality	NONE
Integrity	NONE
Availability	PARTIAL
Access methodology information	
Vector	NETWORK
Complexity	MEDIUM
Authentication	NONE

Vulnerable configs

cpe:2.3:a:apache:portable_runtime:0.9.1		
cpe:2.3:a:apache:portable_runtime:0.9.2	cpe:2.3:a:apache:portable_runtime:0.9.2-dev	cpe:2.3:a:apache:portable_runtime:0.9.3
cpe:2.3:a:apache:portable_runtime:0.9.3-dev	cpe:2.3:a:apache:portable_runtime:0.9.4	cpe:2.3:a:apache:portable_runtime:0.9.5
cpe:2.3:a:apache:portable_runtime:0.9.6	cpe:2.3:a:apache:portable_runtime:0.9.7	cpe:2.3:a:apache:portable_runtime:0.9.7-dev
cpe:2.3:a:apache:portable_runtime:0.9.8	cpe:2.3:a:apache:portable_runtime:0.9.9	cpe:2.3:a:apache:portable_runtime:0.9.16-dev
cpe:2.3:a:apache:portable_runtime:1.3.0	cpe:2.3:a:apache:portable_runtime:1.3.1	cpe:2.3:a:apache:portable_runtime:1.3.2
cpe:2.3:a:apache:portable_runtime:1.3.3	cpe:2.3:a:apache:portable_runtime:1.3.4	cpe:2.3:a:apache:portable_runtime:1.3.4-dev
cpe:2.3:a:apache:portable_runtime:1.3.5	cpe:2.3:a:apache:portable_runtime:1.3.6	cpe:2.3:a:apache:portable_runtime:1.3.6-dev
cpe:2.3:a:apache:portable_runtime:1.3.7	cpe:2.3:a:apache:portable_runtime:1.3.8	cpe:2.3:a:apache:portable_runtime:1.3.9
cpe:2.3:a:apache:portable_runtime:1.3.10	cpe:2.3:a:apache:portable_runtime:1.3.11	cpe:2.3:a:apache:portable_runtime:1.3.12
cpe:2.3:a:apache:portable_runtime:1.3.13	cpe:2.3:a:apache:portable_runtime:1.4.0	cpe:2.3:a:apache:portable_runtime:1.4.1
cpe:2.3:a:apache:portable_runtime:1.4.2	Apache Software Foundation Apache HTTP Server 0.8.11	Apache Software Foundation Apache HTTP Server 0.8.14
Apache Software Foundation Apache HTTP Server 1.0	Apache Software Foundation Apache HTTP Server 1.0.2	Apache Software Foundation Apache HTTP Server 1.0.3
Apache Software Foundation Apache HTTP Server 1.0.5	Apache Software Foundation Apache HTTP Server 1.1	Apache Software Foundation Apache HTTP Server 1.1.1
Apache Software Foundation Apache 1.2	Apache Software Foundation Apache HTTP Server 1.2.4	Apache Software Foundation Apache HTTP Server 1.2.5
Apache Software Foundation Apache HTTP Server 1.2.6	Apache Software Foundation Apache 1.29	Apache Software Foundation Apache HTTP Server 1.3
Apache Software Foundation Apache HTTP Server 1.3.0	Apache Software Foundation Apache HTTP Server 1.3.1	Apache Software Foundation Apache HTTP Server 1.3.1.1
Apache Software Foundation Apache HTTP Server 1.3.2	Apache Software Foundation Apache HTTP Server 1.3.3	Apache Software Foundation Apache HTTP Server 1.3.4
Apache Software Foundation Apache HTTP Server 1.3.5	Apache Software Foundation Apache HTTP Server 1.3.6	Apache Software Foundation Apache HTTP Server 1.3.7
Apache Software Foundation Apache HTTP Server 1.3.8	Apache Software Foundation Apache HTTP Server 1.3.9	Apache Software Foundation Apache 1.3.10
Apache Software Foundation Apache HTTP Server 1.3.11	Apache Software Foundation Apache HTTP Server 1.3.12	Apache Software Foundation Apache 1.3.13
Apache Software Foundation Apache HTTP Server 1.3.14	Apache Software Foundation Apache 1.3.15	Apache Software Foundation Apache 1.3.16
Apache Software Foundation Apache HTTP Server 1.3.17	Apache Software Foundation Apache HTTP Server 1.3.18	Apache Software Foundation Apache HTTP Server 1.3.19
Apache Software Foundation Apache HTTP Server 1.3.20	Apache Software Foundation Apache HTTP Server 1.3.22	Apache Software Foundation Apache HTTP Server 1.3.23

Apache Software Foundation Apache HTTP Server 1.3.24	Apache Software Foundation Apache HTTP Server 1.3.25	Apache Software Foundation Apache HTTP Server 1.3.26
Apache Software Foundation Apache HTTP Server 1.3.27	Apache Software Foundation Apache HTTP Server 1.3.28	Apache Software Foundation Apache HTTP Server 1.3.29
Apache Software Foundation Apache HTTP Server 1.3.30	Apache Software Foundation Apache HTTP Server 1.3.31	Apache Software Foundation Apache HTTP Server 1.3.32
Apache Software Foundation Apache HTTP Server 1.3.33	Apache Software Foundation Apache HTTP Server 1.3.34	Apache Software Foundation Apache HTTP Server 1.3.35
Apache Software Foundation Apache HTTP Server 1.3.36	Apache Software Foundation Apache HTTP Server 1.3.37	Apache Software Foundation Apache HTTP Server 1.3.38
Apache Software Foundation Apache HTTP Server 1.3.39	Apache Software Foundation Apache HTTP Server 1.3.41	Apache Software Foundation Apache HTTP Server 1.3.42
Apache Software Foundation Apache HTTP Server 1.3.65	Apache Software Foundation Apache HTTP Server 1.3.68	Apache Software Foundation Apache HTTP Server 1.4.0
Apache Software Foundation Apache HTTP Server 1.99	Apache Software Foundation Apache HTTP Server 2.0	Apache Software Foundation Apache HTTP Server 2.0.9a
Apache Software Foundation Apache HTTP Server 2.0.28	Apache Software Foundation Apache HTTP Server 2.0.28 Beta	Apache Software Foundation Apache HTTP Server 2.0.32
Apache Software Foundation Apache HTTP Server 2.0.32 Beta	Apache Software Foundation Apache HTTP Server 2.0.34 Beta	Apache Software Foundation Apache HTTP Server 2.0.35
Apache Software Foundation Apache HTTP Server 2.0.36	Apache Software Foundation Apache HTTP Server 2.0.37	Apache Software Foundation Apache HTTP Server 2.0.38
Apache Software Foundation Apache HTTP Server 2.0.39	Apache Software Foundation Apache HTTP Server 2.0.40	Apache Software Foundation Apache HTTP Server 2.0.41
Apache Software Foundation Apache HTTP Server 2.0.42	Apache Software Foundation Apache HTTP Server 2.0.43	Apache Software Foundation Apache HTTP Server 2.0.44
Apache Software Foundation Apache HTTP Server 2.0.45	Apache Software Foundation Apache HTTP Server 2.0.46	Apache Software Foundation Apache HTTP Server 2.0.47
Apache Software Foundation Apache HTTP Server 2.0.48	Apache Software Foundation Apache HTTP Server 2.0.49	Apache Software Foundation Apache HTTP Server 2.0.50
Apache Software Foundation Apache HTTP Server 2.0.51	Apache Software Foundation Apache HTTP Server 2.0.52	Apache Software Foundation Apache HTTP Server 2.0.53
Apache Software Foundation Apache HTTP Server 2.0.54	Apache Software Foundation Apache HTTP Server 2.0.55	Apache Software Foundation Apache HTTP Server 2.0.56
Apache Software Foundation Apache HTTP Server 2.0.57	Apache Software Foundation Apache HTTP Server 2.0.58	Apache Software Foundation HTTP Server 2.0.59
Apache Software Foundation Apache HTTP Server 2.0.60 dev	Apache Software Foundation HTTP Server 2.0.61	Apache Software Foundation Apache HTTP Server 2.0.63
Apache Software Foundation Apache HTTP Server 2.1	Apache Software Foundation Apache HTTP Server 2.1.1	Apache Software Foundation Apache HTTP Server 2.1.2
Apache Software Foundation Apache HTTP Server 2.1.3	Apache Software Foundation Apache HTTP Server 2.1.4	Apache Software Foundation Apache HTTP Server 2.1.5
Apache Software Foundation Apache HTTP Server 2.1.6	Apache Software Foundation Apache HTTP Server 2.1.7	Apache Software Foundation Apache HTTP Server 2.1.8
Apache Software Foundation Apache HTTP Server 2.1.9	Apache Software Foundation Apache HTTP Server 2.2	Apache Software Foundation Apache HTTP Server 2.2.0
Apache Software Foundation Apache HTTP Server 2.2.1	Apache Software Foundation Apache HTTP Server 2.2.2	Apache Software Foundation Apache HTTP Server 2.2.3
Apache Software Foundation Apache HTTP Server 2.2.4	Apache Software Foundation Apache HTTP Server 2.2.6	Apache Software Foundation Apache HTTP Server 2.2.8
Apache Software Foundation Apache HTTP Server 2.2.9	Apache Software Foundation Apache HTTP Server 2.2.10	Apache Software Foundation Apache HTTP Server 2.2.11
Apache Software Foundation Apache HTTP Server 2.2.12	Apache Software Foundation Apache HTTP Server 2.2.13	Apache Software Foundation Apache HTTP Server 2.2.14
Apache Software Foundation Apache HTTP Server 2.2.15	Apache Software Foundation Apache HTTP Server 2.2.16	Apache Software Foundation Apache HTTP Server 2.2.17
Apple Mac OS X 10.6.0	FreeBSD	Google Android Operating System
NetBSD 5.1	OpenBSD 4.8	Oracle Solaris 10

References

http://cvsweb.netbsd.org/bsdweb.cgi/src/lib/libc/gen/fnmatch.c##rev1.22

http://cxib.net/stuff/apache.fnmatch.phps

http://cxib.net/stuff/apr_fnmatch.txts

http://httpd.apache.org/security/vulnerabilities_22.html

http://lists.apple.com/archives/Security-announce/2011//Oct/msg00003.html

http://lists.opensuse.org/opensuse-security-announce/2011-11/msg00011.html

http://marc.info/?l=bugtraq&m=131551295528105&w=2

http://marc.info/?l=bugtraq&m=131731002122529&w=2

http://marc.info/?l=bugtraq&m=132033751509019&w=2

http://marc.info/?l=bugtraq&m=134987041210674&w=2

http://secunia.com/advisories/48308

http://securityreason.com/achievement_securityalert/98

http://securityreason.com/securityalert/8246

http://securitytracker.com/id?1025527

http://support.apple.com/kb/HT5002

http://svn.apache.org/viewvc/apr/apr/branches/1.4.x/strings/apr_fnmatch.c?r1=731029&r2=1098902

http://svn.apache.org/viewvc?view=revision&revision=1098188

http://svn.apache.org/viewvc?view=revision&revision=1098799

http://www.apache.org/dist/apr/Announcement1.x.html

http://www.apache.org/dist/apr/CHANGES-APR-1.4
http://www.apache.org/dist/httpd/Announcement2.2.html
http://www.debian.org/security/2011/dsa-2237
http://www.mail-archive.com/dev@apr.apache.org/msg23960.html
http://www.mail-archive.com/dev@apr.apache.org/msg23961.html
http://www.mail-archive.com/dev@apr.apache.org/msg23976.html
http://www.mandriva.com/security/advisories?name=MDVSA-2011:084
http://www.mandriva.com/security/advisories?name=MDVSA-2013:150
http://www.openbsd.org/cgi-bin/cvsweb/src/lib/libc/gen/fnmatch.c##rev1.15
http://www.oracle.com/technetwork/topics/security/cpujul2012-392727.html
http://www.oracle.com/technetwork/topics/security/cpujuly2013-1899826.html
http://www.redhat.com/support/errata/RHSA-2011-0507.html
http://www.redhat.com/support/errata/RHSA-2011-0896.html
http://www.redhat.com/support/errata/RHSA-2011-0897.html
https://bugzilla.redhat.com/show_bug.cgi?id=703390

Summary

Multiple cross-site scripting (XSS) vulnerabilities in the balancer_handler function in the manager interface in mod_proxy_balancer.c in the mod_proxy_balancer module in the Apache HTTP Server 2.2.x before 2.2.24-dev and 2.4.x before 2.4.4 allow remote attackers to inject arbitrary web script or HTML via a crafted string.

CVE-2012-4558 Information	
CVSS Score	4.3
CWE	CWE-79
Vulnerability impact	
Confidentiality	NONE
Integrity	PARTIAL
Availability	NONE
Access methodology information	
Vector	NETWORK
Complexity	MEDIUM
Authentication	NONE

Vulnerable configs

Apache Software Foundation Apache HTTP Server 2.2	Apache Software Foundation Apache HTTP Server 2.2.0	Apache Software Foundation Apache HTTP Server 2.2.1
Apache Software Foundation Apache HTTP Server 2.2.2	Apache Software Foundation Apache HTTP Server 2.2.3	Apache Software Foundation Apache HTTP Server 2.2.4
Apache Software Foundation Apache HTTP Server 2.2.6	Apache Software Foundation Apache HTTP Server 2.2.8	Apache Software Foundation Apache HTTP Server 2.2.9
Apache Software Foundation Apache HTTP Server 2.2.10	Apache Software Foundation Apache HTTP Server 2.2.11	Apache Software Foundation Apache HTTP Server 2.2.12
Apache Software Foundation Apache HTTP Server 2.2.13	Apache Software Foundation Apache HTTP Server 2.2.14	Apache Software Foundation Apache HTTP Server 2.2.15
Apache Software Foundation Apache HTTP Server 2.2.16	Apache Software Foundation Apache HTTP Server 2.2.17	Apache Software Foundation Apache HTTP Server 2.2.18
Apache Software Foundation Apache HTTP Server 2.2.19	Apache Software Foundation Apache HTTP Server 2.2.20	Apache HTTP Server 2.2.21
Apache Software Foundation Apache HTTP Server 2.2.22	Apache Software Foundation Apache HTTP Server 2.2.23	Apache Software Foundation Apache HTTP Server 2.4.1
Apache Software Foundation Apache HTTP Server 2.4.2	Apache Software Foundation Apache HTTP Server 2.4.0	Apache Software Foundation Apache HTTP Server 2.4.3

References

http://httpd.apache.org/security/vulnerabilities_22.html

http://httpd.apache.org/security/vulnerabilities_24.html

http://lists.apple.com/archives/security-announce/2013/Sep/msg00002.html

http://lists.fedoraproject.org/pipermail/package-announce/2013-April/101196.html

http://marc.info/?l=bugtraq&m=136612293908376&w=2
http://rhn.redhat.com/errata/RHSA-2013-0815.html
http://rhn.redhat.com/errata/RHSA-2013-1207.html
http://rhn.redhat.com/errata/RHSA-2013-1208.html
http://rhn.redhat.com/errata/RHSA-2013-1209.html
http://support.apple.com/kb/HT5880
http://svn.apache.org/viewvc/httpd/httpd/trunk/modules/proxy/mod_proxy_balancer.c?r1=1404653&r2=1
http://www.debian.org/security/2013/dsa-2637
http://www.oracle.com/technetwork/topics/security/cpujan2014-1972949.html
http://www.securityfocus.com/bid/58165
http://www.securityfocus.com/bid/64758

Summary

protocol.c in the Apache HTTP Server 2.2.x through 2.2.21 does not properly restrict header information during construction of Bad Request (aka 400) error documents, which allows remote attackers to obtain the values of HTTPOnly cookies via vectors involving a (1) long or (2) malformed header in conjunction with crafted web script.

CVE-2012-0053 Information	
CVSS Score	4.3
CWE	CWE-264
Vulnerability impact	
Confidentiality	PARTIAL
Integrity	NONE
Availability	NONE
Access methodology information	
Vector	NETWORK
Complexity	MEDIUM
Authentication	NONE

Vulnerable configs

Apache Software Foundation Apache HTTP Server 2.2	Apache Software Foundation Apache HTTP Server 2.2.0	Apache Software Foundation Apache HTTP Server 2.2.1
Apache Software Foundation Apache HTTP Server 2.2.2	Apache Software Foundation Apache HTTP Server 2.2.3	Apache Software Foundation Apache HTTP Server 2.2.4
Apache Software Foundation Apache HTTP Server 2.2.6	Apache Software Foundation Apache HTTP Server 2.2.8	Apache Software Foundation Apache HTTP Server 2.2.9
Apache Software Foundation Apache HTTP Server 2.2.10	Apache Software Foundation Apache HTTP Server 2.2.11	Apache Software Foundation Apache HTTP Server 2.2.12
Apache Software Foundation Apache HTTP Server 2.2.13	Apache Software Foundation Apache HTTP Server 2.2.14	Apache Software Foundation Apache HTTP Server 2.2.15
Apache Software Foundation Apache HTTP Server 2.2.16	Apache Software Foundation Apache HTTP Server 2.2.17	Apache Software Foundation Apache HTTP Server 2.2.18
Apache Software Foundation Apache HTTP Server 2.2.19	Apache Software Foundation Apache HTTP Server 2.2.20	Apache HTTP Server 2.2.21

References

http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=c03360041
http://httpd.apache.org/security/vulnerabilities_22.html
http://kb.juniper.net/JSA10585
http://lists.apple.com/archives/security-announce/2012/Sep/msg00004.html
http://lists.opensuse.org/opensuse-security-announce/2012-02/msg00026.html

http://lists.opensuse.org/opensuse-security-announce/2012-03/msg00002.html
http://marc.info/?l=bugtraq&m=133294460209056&w=2
http://marc.info/?l=bugtraq&m=133494237717847&w=2
http://marc.info/?l=bugtraq&m=133951357207000&w=2
http://marc.info/?l=bugtraq&m=136441204617335&w=2
http://rhn.redhat.com/errata/RHSA-2012-0128.html
http://rhn.redhat.com/errata/RHSA-2012-0542.html
http://rhn.redhat.com/errata/RHSA-2012-0543.html
http://support.apple.com/kb/HT5501
http://svn.apache.org/viewvc?view=revision&revision=1235454
http://www.debian.org/security/2012/dsa-2405
http://www.mandriva.com/security/advisories?name=MDVSA-2012:012
http://www.mandriva.com/security/advisories?name=MDVSA-2013:150
http://www.oracle.com/technetwork/topics/security/cpujan2015-1972971.html
http://www.oracle.com/technetwork/topics/security/cpujul2012-392727.html
http://www.securityfocus.com/bid/51706
https://bugzilla.redhat.com/show_bug.cgi?id=785069

Summary

The mod_proxy module in the Apache HTTP Server 2.0.x through 2.0.64 and 2.2.x before 2.2.18, when the Revision 1179239 patch is in place, does not properly interact with use of (1) RewriteRule and (2) ProxyPassMatch pattern matches for configuration of a reverse proxy, which allows remote attackers to send requests to intranet servers by using the HTTP/0.9 protocol with a malformed URI containing an initial @ (at sign) character. NOTE: this vulnerability exists because of an incomplete fix for CVE-2011-3368.

CVE-2011-3639 Information	
CVSS Score	4.3
CWE	CWE-20
Vulnerability impact	
Confidentiality	NONE
Integrity	PARTIAL
Availability	NONE
Access methodology information	
Vector	NETWORK
Complexity	MEDIUM
Authentication	NONE

Vulnerable configs

cpe:2.3:a:apache:http_server:2.0.11
cpe:2.3:a:apache:http_server:2.0.12
cpe:2.3:a:apache:http_server:2.0.13
cpe:2.3:a:apache:http_server:2.0.14
cpe:2.3:a:apache:http_server:2.0.15
cpe:2.3:a:apache:http_server:2.0.16
cpe:2.3:a:apache:http_server:2.0.17
cpe:2.3:a:apache:http_server:2.0.18
cpe:2.3:a:apache:http_server:2.0.19
cpe:2.3:a:apache:http_server:2.0.20
cpe:2.3:a:apache:http_server:2.0.21
cpe:2.3:a:apache:http_server:2.0.22
cpe:2.3:a:apache:http_server:2.0.23
cpe:2.3:a:apache:http_server:2.0.24
cpe:2.3:a:apache:http_server:2.0.25
cpe:2.3:a:apache:http_server:2.0.26
cpe:2.3:a:apache:http_server:2.0.27
Apache Software Foundation Apache HTTP Server 2.0.28
cpe:2.3:a:apache:http_server:2.0.29
cpe:2.3:a:apache:http_server:2.0.30
cpe:2.3:a:apache:http_server:2.0.31
Apache Software Foundation Apache HTTP Server 2.0.32
cpe:2.3:a:apache:http_server:2.0.33
cpe:2.3:a:apache:http_server:2.0.34
Apache Software Foundation Apache HTTP Server 2.0.35
Apache Software Foundation Apache HTTP Server 2.0.36
Apache Software Foundation Apache HTTP Server 2.0.37
Apache Software Foundation Apache HTTP Server 2.0.38
Apache Software Foundation Apache HTTP Server 2.0.39
Apache Software Foundation Apache HTTP Server 2.0.40
Apache Software Foundation Apache HTTP Server 2.0.41
Apache Software Foundation Apache HTTP Server 2.0.42
Apache Software Foundation Apache HTTP Server 2.0.43
Apache Software Foundation Apache HTTP Server 2.0.44
Apache Software Foundation Apache HTTP Server 2.0.45
Apache Software Foundation Apache HTTP Server 2.0.46
Apache Software Foundation Apache HTTP Server 2.0.47
Apache Software Foundation Apache HTTP Server 2.0.48
Apache Software Foundation Apache HTTP Server 2.0.49
Apache Software Foundation Apache HTTP Server 2.0.50
Apache Software Foundation Apache HTTP Server 2.0.51
Apache Software Foundation Apache HTTP Server 2.0.52
Apache Software Foundation Apache HTTP Server 2.0.53
Apache Software Foundation Apache HTTP Server 2.0.54
Apache Software Foundation Apache HTTP Server 2.0.55
Apache Software Foundation Apache HTTP Server 2.0.56
Apache Software Foundation Apache HTTP Server 2.0.57
Apache Software Foundation Apache HTTP Server 2.0.58
Apache Software Foundation HTTP Server 2.0.59
Apache Software Foundation HTTP Server 2.0.61
Apache Software Foundation Apache HTTP Server 2.0.63
Apache Software Foundation Apache HTTP Server 2.2.0
Apache Software Foundation Apache HTTP Server 2.2.1
Apache Software Foundation Apache HTTP Server 2.2.2
Apache Software Foundation Apache HTTP Server 2.2.3
Apache Software Foundation Apache HTTP Server 2.2.4
Apache Software Foundation Apache HTTP Server 2.2.6
Apache Software Foundation Apache HTTP Server 2.2.8
Apache Software Foundation Apache HTTP Server 2.2.9
Apache Software Foundation Apache HTTP Server 2.2.10
Apache Software Foundation Apache HTTP Server 2.2.11
Apache Software Foundation Apache HTTP Server 2.2.12
Apache Software Foundation Apache HTTP Server 2.2.13
Apache Software Foundation Apache HTTP Server 2.2.14
Apache Software Foundation Apache HTTP Server 2.2.15
Apache Software Foundation Apache HTTP Server 2.2.16
Apache Software Foundation Apache HTTP Server 2.2.17
cpe:2.3:a:apache:http_server2.0a1
cpe:2.3:a:apache:http_server2.0a2
cpe:2.3:a:apache:http_server2.0a3
cpe:2.3:a:apache:http_server2.0a4
cpe:2.3:a:apache:http_server2.0a5

cpe:2.3:a:apache:http_server2.0a6 cpe:2.3:a:apache:http_server2.0a7 cpe:2.3:a:apache:http_server2.0a8
cpe:2.3:a:apache:http_server2.0a9

References

http://rhn.redhat.com/errata/RHSA-2012-0128.html

http://svn.apache.org/viewvc?view=revision&revision=1188745

http://www.debian.org/security/2012/dsa-2405

https://bugzilla.redhat.com/show_bug.cgi?id=752080

Summary

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.

CVE-2008-2939 Information	
CVSS Score	4.3
CWE	CWE-79
Vulnerability impact	
Confidentiality	NONE
Integrity	PARTIAL
Availability	NONE
Access methodology information	
Vector	NETWORK
Complexity	MEDIUM
Authentication	NONE

Vulnerable configs

Apache Software Foundation Apache HTTP Server
Apache Software Foundation Apache HTTP Server 2.0.63
Apache Software Foundation Apache HTTP Server 2.2.0
Apache Software Foundation Apache HTTP Server 2.2.1
Apache Software Foundation Apache HTTP Server 2.2.2
Apache Software Foundation Apache HTTP Server 2.2.3
Apache Software Foundation Apache HTTP Server 2.2.4
Apache Software Foundation Apache HTTP Server 2.2.6
Apache Software Foundation Apache HTTP Server 2.2.8
Apache Software Foundation Apache HTTP Server 2.2.9
Apple Mac OS X 10.5.6
Canonical Ubuntu Linux 6.06 LTS (Long-Term Support)
Canonical Ubuntu Linux 7.10
Canonical Ubuntu Linux 8.04 LTS (Long-Term Support)
OpenSUSE 10.2
OpenSUSE 10.3
OpenSUSE 11.0

References

http://lists.apple.com/archives/security-announce/2009/May/msg00002.html
http://lists.opensuse.org/opensuse-security-announce/2008-11/msg00000.html
http://marc.info/?l=bugtraq&m=123376588623823&w=2
http://marc.info/?l=bugtraq&m=125631037611762&w=2
http://rhn.redhat.com/errata/RHSA-2008-0967.html
http://sunsolve.sun.com/search/document.do?assetkey=1-26-247666-1

http://support.apple.com/kb/HT3549
http://svn.apache.org/viewvc?view=rev&revision=682868
http://svn.apache.org/viewvc?view=rev&revision=682870
http://svn.apache.org/viewvc?view=rev&revision=682871
http://wiki.rpath.com/Advisories:rPSA-2008-0327
http://wiki.rpath.com/wiki/Advisories:rPSA-2008-0328
http://www-1.ibm.com/support/docview.wss?uid=swg1PK70197
http://www-1.ibm.com/support/docview.wss?uid=swg1PK70937
http://www.kb.cert.org/vuls/id/663763
http://www.mandriva.com/security/advisories?name=MDVSA-2008:194
http://www.mandriva.com/security/advisories?name=MDVSA-2008:195
http://www.mandriva.com/security/advisories?name=MDVSA-2009:124
http://www.rapid7.com/advisories/R7-0033
http://www.redhat.com/support/errata/RHSA-2008-0966.html
http://www.securityfocus.com/archive/1/495180/100/0/threaded
http://www.securityfocus.com/archive/1/498566/100/0/threaded
http://www.securityfocus.com/archive/1/498567/100/0/threaded
http://www.securityfocus.com/bid/30560
http://www.securitytracker.com/id?1020635
http://www.ubuntu.com/usn/USN-731-1
http://www.us-cert.gov/cas/techalerts/TA09-133A.html
http://www.vupen.com/english/advisories/2008/2315
http://www.vupen.com/english/advisories/2008/2461
http://www.vupen.com/english/advisories/2009/0320
http://www.vupen.com/english/advisories/2009/1297
https://exchange.xforce.ibmcloud.com/vulnerabilities/44223

Summary

mod_dav.c in the Apache HTTP Server before 2.2.25 does 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 Information	
CVSS Score	4.3
CWE	CWE-264
Vulnerability impact	
Confidentiality	NONE
Integrity	NONE
Availability	PARTIAL
Access methodology information	
Vector	NETWORK
Complexity	MEDIUM
Authentication	NONE

Vulnerable configs

Apache Software Foundation Apache HTTP Server 2.2.24
Apache Software Foundation Apache HTTP Server 2.2.19
Apache Software Foundation Apache HTTP Server 2.2.1
Apache Software Foundation Apache HTTP Server 2.2.6
Apache Software Foundation Apache HTTP Server 2.2.12
Apache Software Foundation Apache HTTP Server 2.2.0
Apache Software Foundation Apache HTTP Server 2.2.11
Apache Software Foundation Apache HTTP Server 2.2.9
Apache Software Foundation Apache HTTP Server 2.2.10
Apache Software Foundation Apache HTTP Server 2.2.8
Apache Software Foundation Apache HTTP Server 2.2.20
Apache Software Foundation Apache HTTP Server 2.2.22
Apache Software Foundation Apache HTTP Server 2.2.23
Apache Software Foundation Apache HTTP Server 2.2.16
Apache Software Foundation Apache HTTP Server 2.2.15
Apache HTTP Server 2.2.21
Apache Software Foundation Apache HTTP Server 2.2.2
Apache Software Foundation Apache HTTP Server 2.2.4
Apache Software Foundation Apache HTTP Server 2.2.17
Apache Software Foundation Apache HTTP Server 2.2.18
Apache Software Foundation Apache HTTP Server 2.2.13
Apache Software Foundation Apache HTTP Server 2.2.3
Apache Software Foundation Apache HTTP Server 2.2.14

References

http://lists.opensuse.org/opensuse-updates/2013-08/msg00026.html
http://lists.opensuse.org/opensuse-updates/2013-08/msg00029.html
http://lists.opensuse.org/opensuse-updates/2013-08/msg00030.html
http://rhn.redhat.com/errata/RHSA-2013-1156.html
http://rhn.redhat.com/errata/RHSA-2013-1207.html

http://rhn.redhat.com/errata/RHSA-2013-1208.html
http://rhn.redhat.com/errata/RHSA-2013-1209.html
http://support.apple.com/kb/HT6150
http://svn.apache.org/viewvc/httpd/httpd/trunk/modules/dav/main/mod_dav.c?r1=1482522&r2=1485668
http://svn.apache.org/viewvc/httpd/httpd/trunk/modules/dav/main/mod_dav.c?view=log
http://tools.cisco.com/security/center/content/CiscoSecurityNotice/CVE-2013-1896
http://www-01.ibm.com/support/docview.wss?uid=swg21644047
http://www.apache.org/dist/httpd/Announcement2.2.html
http://www.securityfocus.com/bid/61129
http://www.ubuntu.com/usn/USN-1903-1
https://h20566.www2.hp.com/portal/site/hpsc/template.PAGE/public/kb/docDisplay/?spf_p.tpst=kbDocD
navigationalState\%3DdocId\%253Demr_na-c03922406-1\%257CdocLocale\%253D\%257CcalledBy\%253
https://httpd.apache.org/security/vulnerabilities_24.html

Summary

Possible CRLF injection allowing HTTP response splitting attacks for sites which use mod_userdir. This issue was mitigated by changes made in 2.4.25 and 2.2.32 which prohibit CR or LF injection into the "Location" or other outbound header key or value. Fixed in Apache HTTP Server 2.4.25 (Affected 2.4.1-2.4.23). Fixed in Apache HTTP Server 2.2.32 (Affected 2.2.0-2.2.31).

CVE-2016-4975 Information	
CVSS Score	4.3
CWE	CWE-93

Vulnerable configs

Apache Software Foundation Apache HTTP Server 2.2.0
Apache Software Foundation Apache HTTP Server 2.2.2
Apache Software Foundation Apache HTTP Server 2.2.3
Apache Software Foundation Apache HTTP Server 2.2.4
Apache Software Foundation Apache HTTP Server 2.2.6
Apache Software Foundation Apache HTTP Server 2.2.8
Apache Software Foundation Apache HTTP Server 2.2.9
Apache Software Foundation Apache HTTP Server 2.2.10
Apache Software Foundation Apache HTTP Server 2.2.11
Apache Software Foundation Apache HTTP Server 2.2.12
Apache Software Foundation Apache HTTP Server 2.2.13
Apache Software Foundation Apache HTTP Server 2.2.14
Apache Software Foundation Apache HTTP Server 2.2.15
Apache Software Foundation Apache HTTP Server 2.2.16
Apache Software Foundation Apache HTTP Server 2.2.17
Apache Software Foundation Apache HTTP Server 2.2.18
Apache Software Foundation Apache HTTP Server 2.2.19
Apache Software Foundation Apache HTTP Server 2.2.20
Apache HTTP Server 2.2.21
Apache Software Foundation Apache HTTP Server 2.2.22
Apache Software Foundation Apache HTTP Server 2.2.23
Apache Software Foundation Apache HTTP Server 2.2.24
Apache Software Foundation Apache HTTP Server 2.2.25
Apache Software Foundation Apache HTTP Server 2.2.26
Apache Software Foundation Apache HTTP Server 2.2.27
Apache Software Foundation Apache HTTP Server 2.2.29
Apache Software Foundation Apache HTTP Server 2.2.31
Apache Software Foundation Apache HTTP Server 2.4.1
Apache Software Foundation Apache HTTP Server 2.4.2
Apache Software Foundation Apache HTTP Server 2.4.3
Apache Software Foundation Apache HTTP Server 2.4.4
Apache Software Foundation Apache HTTP Server 2.4.6
Apache Software Foundation Apache HTTP Server 2.4.7
Apache Software Foundation Apache HTTP Server 2.4.9
Apache Software Foundation Apache HTTP Server 2.4.10
Apache Software Foundation Apache HTTP Server 2.4.12
Apache Software Foundation Apache HTTP Server 2.4.16
Apache Software Foundation Apache HTTP Server 2.4.17
Apache Software Foundation Apache HTTP Server 2.4.18
Apache Software Foundation HTTP Server 2.4.20
Apache Software Foundation HTTP Server 2.4.23

References

http://www.securityfocus.com/bid/105093
https://httpd.apache.org/security/vulnerabilities_22.html##CVE-2016-4975
https://httpd.apache.org/security/vulnerabilities_24.html##CVE-2016-4975
https://security.netapp.com/advisory/ntap-20180926-0006/
https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbux03908en_us

Summary

Multiple cross-site scripting (XSS) vulnerabilities in the Apache HTTP Server 2.2.x before 2.2.24-dev and 2.4.x before 2.4.4 allow remote attackers to inject arbitrary web script or HTML via vectors involving hostnames and URIs in the (1) mod_imagemap, (2) mod_info, (3) mod_ldap, (4) mod_proxy_ftp, and (5) mod_status modules.

CVE-2012-3499 Information	
CVSS Score	4.3
CWE	CWE-79
Vulnerability impact	
Confidentiality	NONE
Integrity	PARTIAL
Availability	NONE
Access methodology information	
Vector	NETWORK
Complexity	MEDIUM
Authentication	NONE

Vulnerable configs

Apache Software Foundation Apache HTTP Server 2.2
Apache Software Foundation Apache HTTP Server 2.2.0
Apache Software Foundation Apache HTTP Server 2.2.1
Apache Software Foundation Apache HTTP Server 2.2.2
Apache Software Foundation Apache HTTP Server 2.2.3
Apache Software Foundation Apache HTTP Server 2.2.4
Apache Software Foundation Apache HTTP Server 2.2.6
Apache Software Foundation Apache HTTP Server 2.2.8
Apache Software Foundation Apache HTTP Server 2.2.9
Apache Software Foundation Apache HTTP Server 2.2.10
Apache Software Foundation Apache HTTP Server 2.2.11
Apache Software Foundation Apache HTTP Server 2.2.12
Apache Software Foundation Apache HTTP Server 2.2.13
Apache Software Foundation Apache HTTP Server 2.2.14
Apache Software Foundation Apache HTTP Server 2.2.15
Apache Software Foundation Apache HTTP Server 2.2.16
Apache Software Foundation Apache HTTP Server 2.2.17
Apache Software Foundation Apache HTTP Server 2.2.18
Apache Software Foundation Apache HTTP Server 2.2.19
Apache Software Foundation Apache HTTP Server 2.2.20
Apache HTTP Server 2.2.21
Apache Software Foundation Apache HTTP Server 2.2.22
Apache Software Foundation Apache HTTP Server 2.2.23
Apache Software Foundation Apache HTTP Server 2.4.1
Apache Software Foundation Apache HTTP Server 2.4.2
Apache Software Foundation Apache HTTP Server 2.4.0
Apache Software Foundation Apache HTTP Server 2.4.3

References

http://httpd.apache.org/security/vulnerabilities_22.html
http://httpd.apache.org/security/vulnerabilities_24.html
http://lists.apple.com/archives/security-announce/2013/Sep/msg00002.html
http://lists.fedoraproject.org/pipermail/package-announce/2013-April/101196.html

http://marc.info/?l=bugtraq&m=136612293908376&w=2
http://rhn.redhat.com/errata/RHSA-2013-0815.html
http://rhn.redhat.com/errata/RHSA-2013-1207.html
http://rhn.redhat.com/errata/RHSA-2013-1208.html
http://rhn.redhat.com/errata/RHSA-2013-1209.html
http://support.apple.com/kb/HT5880
http://svn.apache.org/viewvc/httpd/httpd/trunk/modules/generators/mod_info.c?r1=1225799&r2=141373
http://svn.apache.org/viewvc/httpd/httpd/trunk/modules/generators/mod_status.c?r1=1389564&r2=1413
http://svn.apache.org/viewvc/httpd/httpd/trunk/modules/ldap/util_ldap_cache_mgr.c?r1=1209766&r2=14
http://svn.apache.org/viewvc/httpd/httpd/trunk/modules/mappers/mod_imagemap.c?r1=1398480&r2=14
http://svn.apache.org/viewvc/httpd/httpd/trunk/modules/proxy/mod_proxy_ftp.c?r1=1404625&r2=141373
http://www.debian.org/security/2013/dsa-2637
http://www.fujitsu.com/global/support/software/security/products-f/interstage-201303e.html
http://www.oracle.com/technetwork/topics/security/cpujan2014-1972949.html
http://www.securityfocus.com/bid/58165
http://www.securityfocus.com/bid/64758

Summary

The ap_read_request function in server/protocol.c in the Apache HTTP Server 2.2.x before 2.2.15, when a multithreaded MPM is used, does not properly handle headers in subrequests in certain circumstances involving a parent request that has a body, which might allow remote attackers to obtain sensitive information via a crafted request that triggers access to memory locations associated with an earlier request.

CVE-2010-0434 Information	
CVSS Score	4.3
CWE	CWE-200
Vulnerability impact	
Confidentiality	PARTIAL
Integrity	NONE
Availability	NONE
Access methodology information	
Vector	NETWORK
Complexity	MEDIUM
Authentication	NONE

Vulnerable configs

Apache Software Foundation Apache HTTP Server		Apache Software Foundation Apache HTTP Server 2.2
Apache Software Foundation Apache HTTP Server 2.2.0	Apache Software Foundation Apache HTTP Server 2.2.1	Apache Software Foundation Apache HTTP Server 2.2.2
Apache Software Foundation Apache HTTP Server 2.2.3	Apache Software Foundation Apache HTTP Server 2.2.4	Apache Software Foundation Apache HTTP Server 2.2.6
Apache Software Foundation Apache HTTP Server 2.2.8	Apache Software Foundation Apache HTTP Server 2.2.9	Apache Software Foundation Apache HTTP Server 2.2.11
Apache Software Foundation Apache HTTP Server 2.2.12	Apache Software Foundation Apache HTTP Server 2.2.13	Apache Software Foundation Apache HTTP Server 2.2.14

References

http://httpd.apache.org/security/vulnerabilities_22.html
http://lists.apple.com/archives/security-announce/2010//Nov/msg00000.html
http://lists.fedoraproject.org/pipermail/package-announce/2010-April/039957.html
http://lists.fedoraproject.org/pipermail/package-announce/2010-May/040652.html
http://lists.opensuse.org/opensuse-security-announce/2010-04/msg00006.html

http://lists.vmware.com/pipermail/security-announce/2010/000105.html
http://marc.info/?l=bugtraq&m=127557640302499&w=2
http://support.apple.com/kb/HT4435
http://svn.apache.org/viewvc/httpd/httpd/branches/2.2.x/server/protocol.c?r1=917617&r2=917867&pathr
http://svn.apache.org/viewvc?view=revision&revision=917867
http://svn.apache.org/viewvc?view=revision&revision=918427
http://www-01.ibm.com/support/docview.wss?uid=swg1PM08939
http://www-01.ibm.com/support/docview.wss?uid=swg1PM12247
http://www-01.ibm.com/support/docview.wss?uid=swg1PM15829
http://www.debian.org/security/2010/dsa-2035
http://www.oracle.com/technetwork/topics/security/cpujuly2013-1899826.html
http://www.redhat.com/support/errata/RHSA-2010-0168.html
http://www.redhat.com/support/errata/RHSA-2010-0175.html
http://www.securityfocus.com/bid/38494
http://www.vmware.com/security/advisories/VMSA-2010-0014.html
http://www.vupen.com/english/advisories/2010/0911
http://www.vupen.com/english/advisories/2010/0994
http://www.vupen.com/english/advisories/2010/1001
http://www.vupen.com/english/advisories/2010/1057
http://www.vupen.com/english/advisories/2010/1411
https://bugzilla.redhat.com/show_bug.cgi?id=570171
https://exchange.xforce.ibmcloud.com/vulnerabilities/56625
https://issues.apache.org/bugzilla/show_bug.cgi?id=48359

Summary

Apache HTTP Server mod_cluster before version httpd 2.4.23 is vulnerable to an Improper Input Validation in the protocol parsing logic in the load balancer resulting in a Segmentation Fault in the serving httpd process.

CVE-2016-8612 Information	
CVSS Score	3.3
CWE	CWE-20

Vulnerable configs

Apache Software Foundation Apache HTTP Server
Apache Software Foundation Apache HTTP Server 0.8.11
Apache Software Foundation Apache HTTP Server 0.8.14
Apache Software Foundation Apache HTTP Server 1.0
Apache Software Foundation Apache HTTP Server 1.0.2
Apache Software Foundation Apache HTTP Server 1.0.3
Apache Software Foundation Apache HTTP Server 1.0.5
Apache Software Foundation Apache HTTP Server 1.1
Apache Software Foundation Apache HTTP Server 1.1.1
Apache Software Foundation Apache 1.2
Apache Software Foundation Apache HTTP Server 1.2.4
Apache Software Foundation Apache HTTP Server 1.2.5
Apache Software Foundation Apache HTTP Server 1.2.6
Apache Software Foundation Apache 1.29
Apache Software Foundation Apache HTTP Server 1.3
Apache Software Foundation Apache HTTP Server 1.3.0
Apache Software Foundation Apache HTTP Server 1.3.1
Apache Software Foundation Apache HTTP Server 1.3.1.1
Apache Software Foundation Apache HTTP Server 1.3.2
Apache Software Foundation Apache HTTP Server 1.3.3
Apache Software Foundation Apache HTTP Server 1.3.4
Apache Software Foundation Apache HTTP Server 1.3.5
Apache Software Foundation Apache HTTP Server 1.3.6
Apache Software Foundation Apache HTTP Server 1.3.7
Apache Software Foundation Apache HTTP Server 1.3.8
Apache Software Foundation Apache HTTP Server 1.3.9
Apache Software Foundation Apache 1.3.10
Apache Software Foundation Apache HTTP Server 1.3.11
Apache Software Foundation Apache HTTP Server 1.3.12
Apache Software Foundation Apache 1.3.13
Apache Software Foundation Apache HTTP Server 1.3.14
Apache Software Foundation Apache 1.3.15
Apache Software Foundation Apache 1.3.16
Apache Software Foundation Apache HTTP Server 1.3.17
Apache Software Foundation Apache HTTP Server 1.3.18
Apache Software Foundation Apache HTTP Server 1.3.19
Apache Software Foundation Apache HTTP Server 1.3.20
Apache Software Foundation Apache HTTP Server 1.3.22
Apache Software Foundation Apache HTTP Server 1.3.23
Apache Software Foundation Apache HTTP Server 1.3.24
Apache Software Foundation Apache HTTP Server 1.3.25
Apache Software Foundation Apache HTTP Server 1.3.26
Apache Software Foundation Apache HTTP Server 1.3.27
Apache Software Foundation Apache HTTP Server 1.3.28
Apache Software Foundation Apache HTTP Server 1.3.29
Apache Software Foundation Apache HTTP Server 1.3.30
Apache Software Foundation Apache HTTP Server 1.3.31
Apache Software Foundation Apache HTTP Server 1.3.32
Apache Software Foundation Apache HTTP Server 1.3.33
Apache Software Foundation Apache HTTP Server 1.3.34
Apache Software Foundation Apache HTTP Server 1.3.35
Apache Software Foundation Apache HTTP Server 1.3.36
Apache Software Foundation Apache HTTP Server 1.3.37
Apache Software Foundation Apache HTTP Server 1.3.38
Apache Software Foundation Apache HTTP Server 1.3.39
Apache Software Foundation Apache HTTP Server 1.3.41
Apache Software Foundation Apache HTTP Server 1.3.42
Apache Software Foundation Apache HTTP Server 1.3.65
Apache Software Foundation Apache HTTP Server 1.3.68
Apache Software Foundation Apache HTTP Server 1.4.0
Apache Software Foundation Apache HTTP Server 1.99
Apache Software Foundation Apache HTTP Server 2.0
Apache Software Foundation Apache HTTP Server 2.0.0
Apache Software Foundation Apache HTTP Server 2.0.9a
Apache Software Foundation Apache HTTP Server 2.0.28
Apache Software Foundation Apache HTTP Server 2.0.28 Beta
Apache Software Foundation Apache HTTP Server 2.0.32
Apache Software Foundation Apache HTTP Server 2.0.32 Beta
Apache Software Foundation Apache HTTP Server 2.0.34 Beta
Apache Software Foundation Apache HTTP Server 2.0.35
Apache Software Foundation Apache HTTP Server 2.0.36
Apache Software Foundation Apache HTTP Server 2.0.37
Apache Software Foundation Apache HTTP Server 2.0.38
Apache Software Foundation Apache HTTP Server 2.0.39
Apache Software Foundation Apache HTTP Server 2.0.40
Apache Software Foundation Apache HTTP Server 2.0.41
Apache Software Foundation Apache HTTP Server 2.0.42
Apache Software Foundation Apache HTTP Server 2.0.43
Apache Software Foundation Apache HTTP Server 2.0.44
Apache Software Foundation Apache HTTP Server 2.0.45
Apache Software Foundation Apache HTTP Server 2.0.46
Apache Software Foundation Apache HTTP Server 2.0.47
Apache Software Foundation Apache HTTP Server 2.0.48
Apache Software Foundation Apache HTTP Server 2.0.49
Apache Software Foundation Apache HTTP Server 2.0.50
Apache Software Foundation Apache HTTP Server 2.0.51
Apache Software Foundation Apache HTTP Server 2.0.52
Apache Software Foundation Apache HTTP Server 2.0.53
Apache Software Foundation Apache HTTP Server 2.0.54
Apache Software Foundation Apache HTTP Server 2.0.55
Apache Software Foundation Apache HTTP Server 2.0.56
Apache Software Foundation Apache HTTP Server 2.0.57
Apache Software Foundation Apache HTTP Server 2.0.58
Apache Software Foundation HTTP Server 2.0.59
Apache Software Foundation Apache HTTP Server 2.0.60 dev
Apache Software Foundation HTTP Server 2.0.61
Apache Software Foundation Apache HTTP Server 2.0.63
Apache Software Foundation Apache HTTP Server 2.0.64
Apache Software Foundation Apache HTTP Server 2.0.65
Apache Software Foundation Apache HTTP Server 2.1
Apache Software Foundation Apache HTTP Server 2.1.0
Apache Software Foundation Apache HTTP Server 2.1.1
Apache Software Foundation Apache HTTP Server 2.1.2
Apache Software Foundation Apache HTTP Server 2.1.3
Apache Software Foundation Apache HTTP Server 2.1.4
Apache Software Foundation Apache HTTP Server 2.1.5
Apache Software Foundation Apache HTTP Server 2.1.6
Apache Software Foundation Apache HTTP Server 2.1.7
Apache Software Foundation Apache HTTP Server 2.1.8
Apache Software Foundation Apache HTTP Server 2.1.9
Apache Software Foundation Apache HTTP Server 2.2
Apache Software Foundation Apache HTTP Server 2.2.0
Apache Software Foundation Apache HTTP Server 2.2.1
Apache Software Foundation Apache HTTP Server 2.2.2
Apache Software Foundation Apache HTTP Server 2.2.3
Apache Software Foundation Apache HTTP Server 2.2.4
Apache Software Foundation Apache HTTP Server
Apache Software Foundation Apache HTTP Server 2.2.6
Apache Software Foundation Apache HTTP Server 2.2.8
Apache Software Foundation Apache HTTP Server 2.2.9
Apache Software Foundation Apache HTTP Server 2.2.10
Apache Software Foundation Apache HTTP Server 2.2.11
Apache Software Foundation Apache HTTP Server 2.2.12
Apache Software Foundation Apache HTTP Server 2.2.13
Apache Software Foundation Apache HTTP Server 2.2.14
Apache Software Foundation Apache HTTP Server 2.2.15
Apache Software Foundation Apache HTTP Server 2.2.16
Apache Software Foundation Apache HTTP Server 2.2.17
Apache Software Foundation Apache HTTP Server 2.2.18
Apache Software Foundation Apache HTTP Server 2.2.19
Apache Software Foundation Apache HTTP Server 2.2.20
Apache HTTP Server 2.2.21
Apache Software Foundation Apache HTTP Server 2.2.22
Apache Software Foundation Apache HTTP Server 2.2.23
Apache Software Foundation Apache HTTP Server 2.2.24
Apache Software Foundation Apache HTTP Server 2.2.25
Apache Software Foundation Apache HTTP Server 2.2.26
Apache Software Foundation Apache HTTP Server 2.2.27
Apache Software Foundation Apache HTTP Server 2.2.29
Apache Software Foundation Apache HTTP Server 2.2.31
Apache Software Foundation Apache HTTP Server 2.2.32
Apache Software Foundation Apache HTTP Server 2.2.33
Apache Software Foundation Apache HTTP Server 2.2.34
Apache Software Foundation Apache HTTP Server 2.3.0
Apache Software Foundation Apache HTTP Server 2.3.1
Apache Software Foundation Apache HTTP Server 2.3.2
Apache Software Foundation Apache HTTP Server 2.3.3
Apache Software Foundation Apache HTTP Server 2.3.4
Apache Software Foundation Apache HTTP Server 2.3.5
Apache Software Foundation Apache HTTP Server 2.3.6
Apache Software Foundation Apache HTTP Server 2.3.7
Apache Software Foundation Apache HTTP Server 2.3.8
Apache Software Foundation Apache HTTP Server 2.3.9
Apache Software Foundation Apache HTTP Server 2.3.10
Apache Software Foundation Apache HTTP Server 2.3.11
Apache Software Foundation Apache HTTP Server 2.3.12
Apache Software Foundation Apache HTTP Server 2.3.13
Apache Software Foundation Apache HTTP Server 2.3.14
Apache Software Foundation Apache HTTP Server 2.3.15
Apache Software Foundation Apache HTTP Server 2.3.16
Apache Software Foundation Apache HTTP Server 2.4.0
Apache Software Foundation Apache HTTP Server 2.4.1
Apache Software Foundation Apache HTTP Server 2.4.2
Apache Software Foundation Apache HTTP Server 2.4.3
Apache Software Foundation Apache HTTP Server 2.4.4
Apache Software Foundation Apache HTTP Server 2.4.6
Apache Software Foundation Apache HTTP Server 2.4.7
Apache Software Foundation Apache HTTP Server 2.4.8
Apache Software Foundation Apache HTTP Server 2.4.9
Apache Software Foundation Apache HTTP Server 2.4.10
Apache Software Foundation Apache HTTP Server 2.4.12
Apache Software Foundation Apache HTTP Server 2.4.14
Apache Software Foundation Apache HTTP Server 2.4.16
Apache Software Foundation Apache HTTP Server 2.4.17
Apache Software Foundation Apache HTTP Server 2.4.18
Apache Software Foundation HTTP Server 2.4.19
Apache Software Foundation HTTP Server 2.4.20
Apache Software Foundation Apache HTTP Server 2.4.21
Apache Software Foundation Apache HTTP Server 2.4.22
cpe:2.3:o:redhat:enterprise_linux:6.0
Red Hat Enterprise Linux (RHEL) 7.0 (7)

References

http://rhn.redhat.com/errata/RHSA-2016-2957.html
http://www.securityfocus.com/bid/94939
https://access.redhat.com/errata/RHSA-2017:0193
https://access.redhat.com/errata/RHSA-2017:0194
https://bugzilla.redhat.com/show_bug.cgi?id=1387605
https://security.netapp.com/advisory/ntap-20180601-0005/

Summary

Multiple cross-site scripting (XSS) vulnerabilities in the make_variant_list function in mod_negotiation.c in the mod_negotiation module in the Apache HTTP Server 2.4.x before 2.4.3, when the MultiViews option is enabled, allow remote attackers to inject arbitrary web script or HTML via a crafted filename that is not properly handled during construction of a variant list.

CVE-2012-2687 Information	
CVSS Score	2.6
CWE	CWE-79
Vulnerability impact	
Confidentiality	NONE
Integrity	PARTIAL
Availability	NONE
Access methodology information	
Vector	NETWORK
Complexity	HIGH
Authentication	NONE

Vulnerable configs

Apache Software Foundation Apache HTTP Server 2.4.1
Apache Software Foundation Apache HTTP Server 2.4.2
Apache Software Foundation Apache HTTP Server 2.4.0
Apache Software Foundation Apache HTTP Server 2.2.22
Apache Software Foundation Apache HTTP Server 2.2.23
Apache Software Foundation Apache HTTP Server 2.2.19
Apache Software Foundation Apache HTTP Server 2.2.1
Apache Software Foundation Apache HTTP Server 2.2.16
Apache Software Foundation Apache HTTP Server 2.2.15
Apache Software Foundation Apache HTTP Server 2.2.6
Apache HTTP Server 2.2.21
Apache Software Foundation Apache HTTP Server 2.2.12
Apache Software Foundation Apache HTTP Server 2.2.2
Apache Software Foundation Apache HTTP Server 2.2.4
Apache Software Foundation Apache HTTP Server 2.2.17
Apache Software Foundation Apache HTTP Server 2.2.0
Apache Software Foundation Apache HTTP Server 2.2.18
Apache Software Foundation Apache HTTP Server 2.2.11
Apache Software Foundation Apache HTTP Server 2.2.9
Apache Software Foundation Apache HTTP Server 2.2.13
Apache Software Foundation Apache HTTP Server 2.2.10
Apache Software Foundation Apache HTTP Server 2.2.8
Apache Software Foundation Apache HTTP Server 2.2.3
Apache Software Foundation Apache HTTP Server 2.2.20
Apache Software Foundation Apache HTTP Server 2.2.14

References

http://httpd.apache.org/security/vulnerabilities_24.html
http://lists.apple.com/archives/security-announce/2013/Sep/msg00002.html
http://lists.opensuse.org/opensuse-updates/2013-02/msg00009.html
http://lists.opensuse.org/opensuse-updates/2013-02/msg00011.html
http://lists.opensuse.org/opensuse-updates/2013-02/msg00012.html

http://mail-archives.apache.org/mod_mbox/www-announce/201208.mbox/\%3C0BFFEA9B-801B-4BAA-9534-56F640268E30@apache.org\%3E
http://marc.info/?l=bugtraq&m=136612293908376&w=2
http://rhn.redhat.com/errata/RHSA-2012-1591.html
http://rhn.redhat.com/errata/RHSA-2012-1592.html
http://rhn.redhat.com/errata/RHSA-2012-1594.html
http://rhn.redhat.com/errata/RHSA-2013-0130.html
http://support.apple.com/kb/HT5880
http://www-01.ibm.com/support/docview.wss?uid=nas2a2b50a0ca011b37c86257a96003c9a4f
http://www.apache.org/dist/httpd/CHANGES_2.4.3
http://www.fujitsu.com/global/support/software/security/products-f/interstage-201303e.html
http://www.oracle.com/technetwork/topics/security/cpujuly2013-1899826.html
http://www.securityfocus.com/bid/55131
http://www.ubuntu.com/usn/USN-1627-1
http://www.xerox.com/download/security/security-bulletin/16287-4d6b7b0c81f7b/cert_XRX13-003_v1.0.pdf

Summary

The ap_pregsub function in server/util.c in the Apache HTTP Server 2.0.x through 2.0.64 and 2.2.x through 2.2.21, when the mod_setenvif module is enabled, does not restrict the size of values of environment variables, which allows local users to cause a denial of service (memory consumption or NULL pointer dereference) via a .htaccess file with a crafted SetEnvIf directive, in conjunction with a crafted HTTP request header, related to (1) the "len +=" statement and (2) the apr_pcalloc function call, a different vulnerability than CVE-2011-3607.

CVE-2011-4415 Information	
CVSS Score	1.2
CWE	CWE-20
Vulnerability impact	
Confidentiality	NONE
Integrity	NONE
Availability	PARTIAL
Access methodology information	
Vector	LOCAL
Complexity	HIGH
Authentication	NONE

Vulnerable configs

Apache Software Foundation HTTP Server 2.0.61
Apache Software Foundation Apache HTTP Server 2.0.58 Apache Software Foundation Apache HTTP Server 2.0.55 Apache Software Foundation Apache HTTP Server 2.0.54
Apache Software Foundation Apache HTTP Server 2.0.57 Apache Software Foundation Apache HTTP Server 2.0.56 Apache Software Foundation Apache HTTP Server 2.0.51
Apache Software Foundation Apache HTTP Server 2.0.50 Apache Software Foundation Apache HTTP Server 2.0.53 Apache Software Foundation Apache HTTP Server 2.0.52
Apache Software Foundation Apache HTTP Server 2.0.47 Apache Software Foundation Apache HTTP Server 2.0.46 Apache Software Foundation Apache HTTP Server 2.0.49
Apache Software Foundation Apache HTTP Server 2.0.48 Apache Software Foundation Apache HTTP Server 2.0.43 Apache Software Foundation Apache HTTP Server 2.0.42
Apache Software Foundation Apache HTTP Server 2.0.45 Apache Software Foundation Apache HTTP Server 2.0.44 Apache Software Foundation HTTP Server 2.0.59
Apache Software Foundation Apache HTTP Server 2.0.63 Apache Software Foundation Apache HTTP Server 2.0.9a Apache Software Foundation Apache HTTP Server 2.0.60 dev
Apache Software Foundation Apache HTTP Server 2.0 Apache Software Foundation Apache HTTP Server 2.0.28 Beta Apache Software Foundation Apache HTTP Server 2.0.28
Apache Software Foundation Apache HTTP Server 2.0.32 Beta Apache Software Foundation Apache HTTP Server 2.0.32 Apache Software Foundation Apache HTTP Server 2.0.35
Apache Software Foundation Apache HTTP Server 2.0.34 Beta Apache Software Foundation Apache HTTP Server 2.0.37 Apache Software Foundation Apache HTTP Server 2.0.36
Apache Software Foundation Apache HTTP Server 2.0.39 Apache Software Foundation Apache HTTP Server 2.0.38 Apache Software Foundation Apache HTTP Server 2.0.41
Apache Software Foundation Apache HTTP Server 2.0.40 Apache Software Foundation Apache HTTP Server 2.0.64 Apache Software Foundation Apache HTTP Server 2.2.1
Apache Software Foundation Apache HTTP Server 2.2.6 Apache Software Foundation Apache HTTP Server 2.2.11 Apache Software Foundation Apache HTTP Server 2.2.9
Apache Software Foundation Apache HTTP Server 2.2.10 Apache Software Foundation Apache HTTP Server 2.2.8 Apache Software Foundation Apache HTTP Server 2.2.13
Apache Software Foundation Apache HTTP Server 2.2.3 Apache Software Foundation Apache HTTP Server 2.2.12 Apache Software Foundation Apache HTTP Server 2.2.0
Apache Software Foundation Apache HTTP Server 2.2.16 Apache Software Foundation Apache HTTP Server 2.2.15 Apache Software Foundation Apache HTTP Server 2.2.2
Apache Software Foundation Apache HTTP Server 2.2.4 Apache Software Foundation Apache HTTP Server 2.2.18 Apache Software Foundation Apache HTTP Server 2.2.14
Apache Software Foundation Apache HTTP Server 2.2.19 Apache Software Foundation Apache HTTP Server 2.2.20 Apache HTTP Server 2.2.21

References

http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=c03360041
http://www.gossamer-threads.com/lists/apache/dev/403775
http://www.halfdog.net/Security/2011/ApacheModSetEnvIfIntegerOverflow/
http://www.halfdog.net/Security/2011/ApacheModSetEnvIfIntegerOverflow/DemoExploit.html

Summary

http/modules/ngx_http_proxy_module.c in nginx 1.1.4 through 1.2.8 and 1.3.0 through 1.4.0, when proxy_pass is used with untrusted HTTP servers, allows remote attackers to cause a denial of service (crash) and obtain sensitive information from worker process memory via a crafted proxy response, a similar vulnerability to CVE-2013-2028.

CVE-2013-2070 Information	
CVSS Score	5.8
CWE	CWE-264
Vulnerability impact	
Confidentiality	PARTIAL
Integrity	NONE
Availability	PARTIAL
Access methodology information	
Vector	NETWORK
Complexity	MEDIUM
Authentication	NONE

Vulnerable configs

cpe:2.3:a:igor_sysoev:nginx:1.2.1	cpe:2.3:a:igor_sysoev:nginx:1.2.2	cpe:2.3:a:igor_sysoev:nginx:1.2.3
cpe:2.3:a:igor_sysoev:nginx:1.2.4	cpe:2.3:a:igor_sysoev:nginx:1.2.5	cpe:2.3:a:igor_sysoev:nginx:1.2.6
cpe:2.3:a:igor_sysoev:nginx:1.2.7	cpe:2.3:a:igor_sysoev:nginx:1.2.8	Nginx 1.1.4
Nginx 1.1.6	Nginx 1.1.7	Nginx 1.1.8
Nginx 1.1.9	Nginx 1.1.10	Nginx 1.1.11
Nginx 1.1.12	Nginx 1.1.13	Nginx 1.1.15
Nginx 1.1.16	Nginx 1.1.17	Nginx 1.1.18
Nginx 1.1.19	Nginx 1.2.0	Nginx 1.3.0
Nginx 1.3.1	Nginx 1.3.2	Nginx 1.3.3
Nginx 1.3.4	Nginx 1.3.5	Nginx 1.3.6
Nginx 1.3.7	Nginx 1.3.8	Nginx 1.3.9
Nginx 1.3.10	Nginx 1.3.11	Nginx 1.3.12
Nginx 1.3.13	Nginx 1.3.14	Nginx 1.3.15
Nginx 1.3.16		Nginx 1.4.0

References

http://lists.fedoraproject.org/pipermail/package-announce/2013-May/105950.html
http://mailman.nginx.org/pipermail/nginx-announce/2013/000114.html
http://nginx.org/download/patch.2013.proxy.txt

http://seclists.org/oss-sec/2013/q2/291
http://security.gentoo.org/glsa/glsa-201310-04.xml
http://www.debian.org/security/2013/dsa-2721
http://www.openwall.com/lists/oss-security/2013/05/13/3
http://www.securityfocus.com/bid/59824
https://bugzilla.redhat.com/show_bug.cgi?id=962525
https://exchange.xforce.ibmcloud.com/vulnerabilities/84172

Summary

http/modules/ngx_http_proxy_module.c in nginx 1.1.4 through 1.2.8 and 1.3.0 through 1.4.0, when proxy_pass is used with untrusted HTTP servers, allows remote attackers to cause a denial of service (crash) and obtain sensitive information from worker process memory via a crafted proxy response, a similar vulnerability to CVE-2013-2028.

CVE-2013-2070 Information	
CVSS Score	5.8
CWE	CWE-264
Vulnerability impact	
Confidentiality	PARTIAL
Integrity	NONE
Availability	PARTIAL
Access methodology information	
Vector	NETWORK
Complexity	MEDIUM
Authentication	NONE

Vulnerable configs

cpe:2.3:a:igor_sysoev:nginx:1.2.1		
cpe:2.3:a:igor_sysoev:nginx:1.2.2	cpe:2.3:a:igor_sysoev:nginx:1.2.3	cpe:2.3:a:igor_sysoev:nginx:1.2.4
cpe:2.3:a:igor_sysoev:nginx:1.2.5	cpe:2.3:a:igor_sysoev:nginx:1.2.6	cpe:2.3:a:igor_sysoev:nginx:1.2.7
cpe:2.3:a:igor_sysoev:nginx:1.2.8	Nginx 1.1.4	Nginx 1.1.6
Nginx 1.1.7	Nginx 1.1.8	Nginx 1.1.9
Nginx 1.1.10	Nginx 1.1.11	Nginx 1.1.12
Nginx 1.1.13	Nginx 1.1.15	Nginx 1.1.16
Nginx 1.1.17	Nginx 1.1.18	Nginx 1.1.19
Nginx 1.2.0	Nginx 1.3.0	Nginx 1.3.1
Nginx 1.3.2	Nginx 1.3.3	Nginx 1.3.4
Nginx 1.3.5	Nginx 1.3.6	Nginx 1.3.7
Nginx 1.3.8	Nginx 1.3.9	Nginx 1.3.10
Nginx 1.3.11	Nginx 1.3.12	Nginx 1.3.13
Nginx 1.3.14	Nginx 1.3.15	Nginx 1.3.16
Nginx 1.4.0		

References

http://lists.fedoraproject.org/pipermail/package-announce/2013-May/105950.html
http://mailman.nginx.org/pipermail/nginx-announce/2013/000114.html

http://nginx.org/download/patch.2013.proxy.txt
http://seclists.org/oss-sec/2013/q2/291
http://security.gentoo.org/glsa/glsa-201310-04.xml
http://www.debian.org/security/2013/dsa-2721
http://www.openwall.com/lists/oss-security/2013/05/13/3
http://www.securityfocus.com/bid/59824
https://bugzilla.redhat.com/show_bug.cgi?id=962525
https://exchange.xforce.ibmcloud.com/vulnerabilities/84172

Summary

lighttpd before 1.4.33 does not check the return value of the (1) setuid, (2) setgid, or (3) setgroups functions, which might cause lighttpd to run as root if it is restarted and allows remote attackers to gain privileges, as demonstrated by multiple calls to the clone function that cause setuid to fail when the user process limit is reached.

CVE-2013-4559 Information	
CVSS Score	7.6
CWE	CWE-264
Vulnerability impact	
Confidentiality	COMPLETE
Integrity	COMPLETE
Availability	COMPLETE
Access methodology information	
Vector	NETWORK
Complexity	HIGH
Authentication	NONE

Vulnerable configs

lighttpd 1.4.9
lighttpd 1.4.7
lighttpd 1.4.4
lighttpd 1.4.30
lighttpd 1.4.28
lighttpd lighttpd 1.4.25
lighttpd lighttpd 1.4.22
lighttpd lighttpd 1.4.19
lighttpd 1.4.16
lighttpd 1.4.13
lighttpd 1.4.10
Debian GNU/Linux 6.0
lighttpd 1.4.6
lighttpd 1.4.32
lighttpd 1.4.3
Lighttpd 1.4.27
lighttpd lighttpd 1.4.24
lighttpd lighttpd 1.4.21
lighttpd 1.4.18
lighttpd 1.4.15
lighttpd 1.4.12
Debian Linux 7.0
lighttpd 1.4.8
lighttpd 1.4.5
lighttpd 1.4.31
lighttpd 1.4.29
lighttpd lighttpd 1.4.26
lighttpd lighttpd 1.4.23
lighttpd lighttpd 1.4.20
lighttpd lighttpd 1.4.17
lighttpd lighttpd 1.4.14
lighttpd 1.4.11
Debian Linux 7.1

References

http://download.lighttpd.net/lighttpd/security/lighttpd_sa_2013_02.txt
http://lists.opensuse.org/opensuse-updates/2014-01/msg00049.html
http://marc.info/?l=bugtraq&m=141576815022399&w=2
http://www.openwall.com/lists/oss-security/2013/11/12/4

https://www.debian.org/security/2013/dsa-2795

Summary

SQL injection vulnerability in mod_mysql_vhost.c in lighttpd before 1.4.35 allows remote attackers to execute arbitrary SQL commands via the host name, related to request_check_hostname.

CVE-2014-2323 Information	
CVSS Score	7.5
CWE	CWE-89
Vulnerability impact	
Confidentiality	PARTIAL
Integrity	PARTIAL
Availability	PARTIAL
Access methodology information	
Vector	NETWORK
Complexity	LOW
Authentication	NONE

Vulnerable configs

lighttpd 1.4.34
lighttpd 1.4.10
lighttpd 1.4.13
lighttpd 1.4.16
lighttpd lighttpd 1.4.19
lighttpd lighttpd 1.4.22
lighttpd lighttpd 1.4.25
lighttpd 1.4.28
lighttpd 1.4.30
lighttpd 1.4.33
lighttpd 1.4.6
lighttpd 1.4.9
lighttpd 1.4.11
lighttpd lighttpd 1.4.14
lighttpd lighttpd 1.4.17
lighttpd lighttpd 1.4.20
lighttpd lighttpd 1.4.23
lighttpd lighttpd 1.4.26
lighttpd 1.4.29
lighttpd 1.4.31
lighttpd 1.4.4
lighttpd 1.4.7
lighttpd 1.3.16
lighttpd 1.4.12
lighttpd 1.4.15
lighttpd 1.4.18
lighttpd lighttpd 1.4.21
lighttpd lighttpd 1.4.24
Lighttpd 1.4.27
lighttpd 1.4.3
lighttpd 1.4.32
lighttpd 1.4.5
lighttpd 1.4.8

References

http://download.lighttpd.net/lighttpd/security/lighttpd_sa_2014_01.txt
http://lists.opensuse.org/opensuse-security-announce/2014-03/msg00023.html
http://lists.opensuse.org/opensuse-security-announce/2014-04/msg00002.html
http://lists.opensuse.org/opensuse-security-announce/2014-04/msg00006.html
http://marc.info/?l=bugtraq&m=141576815022399&w=2
http://seclists.org/oss-sec/2014/q1/561

http://seclists.org/oss-sec/2014/q1/564
http://www.debian.org/security/2014/dsa-2877
http://www.lighttpd.net/2014/3/12/1.4.35/

Summary

mod_userdir in lighttpd before 1.4.20, when a case-insensitive operating system or filesystem is used, performs case-sensitive comparisons on filename components in configuration options, which might allow remote attackers to bypass intended access restrictions, as demonstrated by a request for a .PHP file when there is a configuration rule for .php files.

CVE-2008-4360 Information	
CVSS Score	7.5
CWE	CWE-200
Vulnerability impact	
Confidentiality	COMPLETE
Integrity	NONE
Availability	NONE
Access methodology information	
Vector	NETWORK
Complexity	LOW
Authentication	NONE

Vulnerable configs

lighttpd 1.3.16
lighttpd 1.4.3
lighttpd 1.4.4
lighttpd 1.4.5
lighttpd 1.4.6
lighttpd 1.4.7
lighttpd 1.4.8
lighttpd 1.4.9
lighttpd 1.4.10
lighttpd 1.4.11
lighttpd 1.4.12
lighttpd 1.4.13
lighttpd lighttpd 1.4.14
lighttpd 1.4.15
lighttpd 1.4.16
lighttpd lighttpd 1.4.17
lighttpd 1.4.18
lighttpd lighttpd 1.4.19
Debian GNU/Linux 4.0

References

http://lists.opensuse.org/opensuse-security-announce/2008-11/msg00002.html
http://openwall.com/lists/oss-security/2008/09/30/1
http://openwall.com/lists/oss-security/2008/09/30/2
http://openwall.com/lists/oss-security/2008/09/30/3
http://security.gentoo.org/glsa/glsa-200812-04.xml
http://trac.lighttpd.net/trac/changeset/2283

http://trac.lighttpd.net/trac/changeset/2308
http://trac.lighttpd.net/trac/ticket/1589
http://wiki.rpath.com/Advisories:rPSA-2008-0309
http://wiki.rpath.com/wiki/Advisories:rPSA-2008-0309
http://www.debian.org/security/2008/dsa-1645
http://www.lighttpd.net/security/lighttpd-1.4.x_userdir_lowercase.patch
http://www.lighttpd.net/security/lighttpd_sa_2008_06.txt
http://www.securityfocus.com/archive/1/497932/100/0/threaded
http://www.securityfocus.com/bid/31600
http://www.vupen.com/english/advisories/2008/2741
https://exchange.xforce.ibmcloud.com/vulnerabilities/45689

Summary

lighttpd before 1.4.20 compares URIs to patterns in the (1) url.redirect and (2) url.rewrite configuration settings before performing URL decoding, which might allow remote attackers to bypass intended access restrictions, and obtain sensitive information or possibly modify data.

CVE-2008-4359 Information	
CVSS Score	7.5
CWE	CWE-200
Vulnerability impact	
Confidentiality	PARTIAL
Integrity	PARTIAL
Availability	PARTIAL
Access methodology information	
Vector	NETWORK
Complexity	LOW
Authentication	NONE

Vulnerable configs

lighttpd 1.3.16
lighttpd 1.4.3
lighttpd 1.4.4
lighttpd 1.4.5
lighttpd 1.4.6
lighttpd 1.4.7
lighttpd 1.4.8
lighttpd 1.4.9
lighttpd 1.4.10
lighttpd 1.4.11
lighttpd 1.4.12
lighttpd 1.4.13
lighttpd lighttpd 1.4.14
lighttpd 1.4.15
lighttpd 1.4.16
lighttpd lighttpd 1.4.17
lighttpd 1.4.18
lighttpd lighttpd 1.4.19
Debian GNU/Linux 4.0

References

http://lists.opensuse.org/opensuse-security-announce/2008-11/msg00002.html
http://openwall.com/lists/oss-security/2008/09/30/1
http://openwall.com/lists/oss-security/2008/09/30/2
http://openwall.com/lists/oss-security/2008/09/30/3
http://security.gentoo.org/glsa/glsa-200812-04.xml

http://trac.lighttpd.net/trac/changeset/2278
http://trac.lighttpd.net/trac/changeset/2307
http://trac.lighttpd.net/trac/changeset/2309
http://trac.lighttpd.net/trac/changeset/2310
http://trac.lighttpd.net/trac/ticket/1720
http://wiki.rpath.com/Advisories:rPSA-2008-0309
http://wiki.rpath.com/wiki/Advisories:rPSA-2008-0309
http://www.debian.org/security/2008/dsa-1645
http://www.lighttpd.net/security/lighttpd-1.4.x_rewrite_redirect_decode_url.patch
http://www.lighttpd.net/security/lighttpd_sa_2008_05.txt
http://www.securityfocus.com/archive/1/497932/100/0/threaded
http://www.securityfocus.com/bid/31599
http://www.vupen.com/english/advisories/2008/2741
https://exchange.xforce.ibmcloud.com/vulnerabilities/45690

Summary

Multiple directory traversal vulnerabilities in (1) mod_evhost and (2) mod_simple_vhost in lighttpd before 1.4.35 allow remote attackers to read arbitrary files via a .. (dot dot) in the host name, related to request_check_hostname.

CVE-2014-2324 Information	
CVSS Score	5.0
CWE	CWE-22
Vulnerability impact	
Confidentiality	PARTIAL
Integrity	NONE
Availability	NONE
Access methodology information	
Vector	NETWORK
Complexity	LOW
Authentication	NONE

Vulnerable configs

lighttpd 1.4.34
lighttpd 1.4.11
lighttpd lighttpd 1.4.14
lighttpd lighttpd 1.4.17
lighttpd lighttpd 1.4.20
lighttpd lighttpd 1.4.23
lighttpd lighttpd 1.4.26
lighttpd 1.4.29
lighttpd 1.4.31
lighttpd 1.4.4
lighttpd 1.4.7
lighttpd 1.3.16
lighttpd 1.4.12
lighttpd 1.4.15
lighttpd 1.4.18
lighttpd lighttpd 1.4.21
lighttpd lighttpd 1.4.24
Lighttpd 1.4.27
lighttpd 1.4.3
lighttpd 1.4.32
lighttpd 1.4.5
lighttpd 1.4.8
lighttpd 1.4.10
lighttpd 1.4.13
lighttpd 1.4.16
lighttpd lighttpd 1.4.19
lighttpd lighttpd 1.4.22
lighttpd lighttpd 1.4.25
lighttpd 1.4.28
lighttpd 1.4.30
lighttpd 1.4.33
lighttpd 1.4.6
lighttpd 1.4.9

References

http://download.lighttpd.net/lighttpd/security/lighttpd_sa_2014_01.txt
http://lists.opensuse.org/opensuse-security-announce/2014-03/msg00023.html
http://lists.opensuse.org/opensuse-security-announce/2014-04/msg00002.html
http://lists.opensuse.org/opensuse-security-announce/2014-04/msg00006.html
http://marc.info/?l=bugtraq&m=141576815022399&w=2

http://seclists.org/oss-sec/2014/q1/561
http://seclists.org/oss-sec/2014/q1/564
http://www.debian.org/security/2014/dsa-2877
http://www.lighttpd.net/2014/3/12/1.4.35/
http://www.securityfocus.com/bid/66157

Summary

lighttpd before 1.4.26, and 1.5.x, allocates a buffer for each read operation that occurs for a request, which allows remote attackers to cause a denial of service (memory consumption) by breaking a request into small pieces that are sent at a slow rate.

CVE-2010-0295 Information	
CVSS Score	5.0
CWE	CWE-399
Vulnerability impact	
Confidentiality	NONE
Integrity	NONE
Availability	PARTIAL
Access methodology information	
Vector	NETWORK
Complexity	LOW
Authentication	NONE

Vulnerable configs

lighttpd 1.4.18
lighttpd 1.4.4
lighttpd 1.4.7
lighttpd lighttpd 1.4.19
lighttpd 1.4.15
lighttpd 1.4.12
cpe:2.3:a:lighttpd:lighttpd:1.4.0
cpe:2.3:a:lighttpd:lighttpd:1.3.6
cpe:2.3:a:lighttpd:lighttpd:1.3.3
lighttpd 1.3.15
lighttpd 1.3.12
cpe:2.3:a:lighttpd:lighttpd:1.3.1
cpe:2.3:a:lighttpd:lighttpd:1.2.7
cpe:2.3:a:lighttpd:lighttpd:1.2.3
cpe:2.3:a:lighttpd:lighttpd:1.2.0
cpe:2.3:a:lighttpd:lighttpd:1.1.7
cpe:2.3:a:lighttpd:lighttpd:1.1.4
cpe:2.3:a:lighttpd:lighttpd:1.1.1
cpe:2.3:a:lighttpd:lighttpd:1.0.2
lighttpd lighttpd 1.4.22
lighttpd lighttpd 1.4.25
lighttpd 1.4.2
lighttpd 1.4.5
lighttpd 1.4.8
lighttpd lighttpd 1.4.17
lighttpd lighttpd 1.4.14
lighttpd 1.4.11
cpe:2.3:a:lighttpd:lighttpd:1.3.9
cpe:2.3:a:lighttpd:lighttpd:1.3.5
cpe:2.3:a:lighttpd:lighttpd:1.3.2
lighttpd 1.3.14
lighttpd 1.3.11
cpe:2.3:a:lighttpd:lighttpd:1.3.0
cpe:2.3:a:lighttpd:lighttpd:1.2.6
cpe:2.3:a:lighttpd:lighttpd:1.2.2
cpe:2.3:a:lighttpd:lighttpd:1.1.9
cpe:2.3:a:lighttpd:lighttpd:1.1.6
cpe:2.3:a:lighttpd:lighttpd:1.1.3
cpe:2.3:a:lighttpd:lighttpd:1.1.0
lighttpd lighttpd 1.4.20
lighttpd lighttpd 1.4.23
lighttpd 1.4.3
lighttpd 1.4.6
lighttpd 1.4.9
lighttpd 1.4.16
lighttpd 1.4.13
lighttpd 1.4.10
cpe:2.3:a:lighttpd:lighttpd:1.3.8
cpe:2.3:a:lighttpd:lighttpd:1.3.4
lighttpd 1.3.16
lighttpd 1.3.13
cpe:2.3:a:lighttpd:lighttpd:1.3.10
cpe:2.3:a:lighttpd:lighttpd:1.2.8
cpe:2.3:a:lighttpd:lighttpd:1.2.5
cpe:2.3:a:lighttpd:lighttpd:1.2.1
cpe:2.3:a:lighttpd:lighttpd:1.1.8
cpe:2.3:a:lighttpd:lighttpd:1.1.5
cpe:2.3:a:lighttpd:lighttpd:1.1.2
cpe:2.3:a:lighttpd:lighttpd:1.0.3
lighttpd lighttpd 1.4.21
lighttpd lighttpd 1.4.24
lighttpd 1.5.0

References

http://blogs.sun.com/security/entry/cve_2010_0295_vulnerability_in

http://download.lighttpd.net/lighttpd/security/lighttpd-1.4.x_fix_slow_request_dos.patch
http://download.lighttpd.net/lighttpd/security/lighttpd-1.5_fix_slow_request_dos.patch
http://download.lighttpd.net/lighttpd/security/lighttpd_sa_2010_01.txt
http://lists.fedoraproject.org/pipermail/package-announce/2010-May/041264.html
http://lists.fedoraproject.org/pipermail/package-announce/2010-May/041296.html
http://lists.fedoraproject.org/pipermail/package-announce/2010-May/041307.html
http://lists.opensuse.org/opensuse-security-announce/2010-02/msg00003.html
http://redmine.lighttpd.net/issues/2147
http://redmine.lighttpd.net/projects/lighttpd/repository/revisions/2710
http://redmine.lighttpd.net/projects/lighttpd/repository/revisions/2711
http://security.gentoo.org/glsa/glsa-201006-17.xml
http://www.debian.org/security/2010/dsa-1987
http://www.openwall.com/lists/oss-security/2010/02/01/8
http://www.securityfocus.com/bid/38036
http://www.vupen.com/english/advisories/2011/0172
https://exchange.xforce.ibmcloud.com/vulnerabilities/56038

Summary

An issue was discovered in mod_alias_physical_handler in mod_alias.c in lighttpd before 1.4.50. There is potential ../ path traversal of a single directory above an alias target, with a specific mod_alias configuration where the matched alias lacks a trailing '/' character, but the alias target filesystem path does have a trailing '/' character.

CVE-2018-19052 Information	
CVSS Score	5.0
CWE	CWE-22

Vulnerable configs

lighttpd 1.3.11		
lighttpd 1.3.12	lighttpd 1.3.13	lighttpd 1.3.14
lighttpd 1.3.15	lighttpd 1.3.16	lighttpd 1.4.1
lighttpd 1.4.2	lighttpd 1.4.3	lighttpd 1.4.4
lighttpd 1.4.5	lighttpd 1.4.6	lighttpd 1.4.7
lighttpd 1.4.8	lighttpd 1.4.9	lighttpd 1.4.10
lighttpd 1.4.11	lighttpd 1.4.12	lighttpd 1.4.13
lighttpd lighttpd 1.4.14	lighttpd 1.4.15	lighttpd 1.4.16
lighttpd lighttpd 1.4.17	lighttpd 1.4.18	lighttpd lighttpd 1.4.19
lighttpd lighttpd 1.4.20	lighttpd lighttpd 1.4.21	lighttpd lighttpd 1.4.22
lighttpd lighttpd 1.4.23	lighttpd lighttpd 1.4.24	lighttpd lighttpd 1.4.25
lighttpd lighttpd 1.4.26	Lighttpd 1.4.27	lighttpd 1.4.28
lighttpd 1.4.29	lighttpd 1.4.30	lighttpd 1.4.31
lighttpd 1.4.32	lighttpd 1.4.33	lighttpd 1.4.34
lighttpd lighttpd 1.4.35	lighttpd 1.4.36	lighttpd 1.4.37
lighttpd 1.4.38	lighttpd 1.4.39	lighttpd 1.4.40
lighttpd 1.4.41	lighttpd 1.4.42	lighttpd 1.4.43
lighttpd 1.4.44	lighttpd 1.4.45	lighttpd 1.4.46
lighttpd 1.4.47	lighttpd 1.4.48	lighttpd 1.4.49
SUSE Linux Enterprise Server (SLES) 11 Service Pack 3	SUSE Linux Enterprise Server (SLES) 11 Service Pack 4	SUSE Linux Enterprise Server (SLES) 12
SUSE Linux Enterprise Server (SLES) 12 Service Pack 1	SUSE Linux Enterprise Server (SLES) 12 Service Pack 2	SUSE Linux Enterprise Server (SLES) 12 Service Pack 3
cpe:2.3:o:suse:suse_linux_enterprise_server:12:sp4		

References

https://github.com/lighttpd/lighttpd1.4/commit/2105dae0f9d7a964375ce681e53cb165375f84c1

Summary

Memory leak in the http_request_parse function in request.c in lighttpd before 1.4.20 allows remote attackers to cause a denial of service (memory consumption) via a large number of requests with duplicate request headers.

CVE-2008-4298 Information	
CVSS Score	5.0
CWE	CWE-399
Vulnerability impact	
Confidentiality	NONE
Integrity	NONE
Availability	PARTIAL
Access methodology information	
Vector	NETWORK
Complexity	LOW
Authentication	NONE

Vulnerable configs

cpe:2.3:a:lighttpd:lighttpd:1.1.1
cpe:2.3:a:lighttpd:lighttpd:1.1.2
cpe:2.3:a:lighttpd:lighttpd:1.1.3
cpe:2.3:a:lighttpd:lighttpd:1.1.4
cpe:2.3:a:lighttpd:lighttpd:1.1.5
cpe:2.3:a:lighttpd:lighttpd:1.1.6
cpe:2.3:a:lighttpd:lighttpd:1.1.7
cpe:2.3:a:lighttpd:lighttpd:1.1.8
cpe:2.3:a:lighttpd:lighttpd:1.1.9
cpe:2.3:a:lighttpd:lighttpd:1.2.1
cpe:2.3:a:lighttpd:lighttpd:1.2.2
cpe:2.3:a:lighttpd:lighttpd:1.2.3
cpe:2.3:a:lighttpd:lighttpd:1.2.4
cpe:2.3:a:lighttpd:lighttpd:1.2.5
cpe:2.3:a:lighttpd:lighttpd:1.2.6
cpe:2.3:a:lighttpd:lighttpd:1.2.7
cpe:2.3:a:lighttpd:lighttpd:1.2.8
cpe:2.3:a:lighttpd:lighttpd:1.3.0
cpe:2.3:a:lighttpd:lighttpd:1.3.1
cpe:2.3:a:lighttpd:lighttpd:1.3.2
cpe:2.3:a:lighttpd:lighttpd:1.3.3
cpe:2.3:a:lighttpd:lighttpd:1.3.4
cpe:2.3:a:lighttpd:lighttpd:1.3.5
cpe:2.3:a:lighttpd:lighttpd:1.3.6
cpe:2.3:a:lighttpd:lighttpd:1.3.7
cpe:2.3:a:lighttpd:lighttpd:1.3.8
cpe:2.3:a:lighttpd:lighttpd:1.3.9
cpe:2.3:a:lighttpd:lighttpd:1.3.10
lighttpd 1.3.11
lighttpd 1.3.12
lighttpd 1.3.13
lighttpd 1.3.14
lighttpd 1.3.15
lighttpd 1.3.16
cpe:2.3:a:lighttpd:lighttpd:1.4.0
lighttpd 1.4.1
lighttpd 1.4.2
lighttpd 1.4.3
lighttpd 1.4.4
lighttpd 1.4.5
lighttpd 1.4.6
lighttpd 1.4.7
lighttpd 1.4.8
lighttpd 1.4.9
lighttpd 1.4.10
lighttpd 1.4.11
lighttpd 1.4.12
lighttpd 1.4.13
lighttpd lighttpd 1.4.14
lighttpd 1.4.15
lighttpd 1.4.16
lighttpd lighttpd 1.4.17
lighttpd 1.4.18
lighttpd lighttpd 1.4.19

References

http://bugs.gentoo.org/show_bug.cgi?id=238180
http://lists.opensuse.org/opensuse-security-announce/2008-11/msg00002.html

http://security.gentoo.org/glsa/glsa-200812-04.xml
http://trac.lighttpd.net/trac/changeset/2305
http://trac.lighttpd.net/trac/ticket/1774
http://wiki.rpath.com/Advisories:rPSA-2008-0309
http://wiki.rpath.com/wiki/Advisories:rPSA-2008-0309
http://www.debian.org/security/2008/dsa-1645
http://www.lighttpd.net/security/lighttpd_sa_2008_07.txt
http://www.openwall.com/lists/oss-security/2008/09/26/5
http://www.securityfocus.com/archive/1/497932/100/0/threaded
http://www.securityfocus.com/bid/31434
http://www.vupen.com/english/advisories/2008/2741
https://exchange.xforce.ibmcloud.com/vulnerabilities/45471

Summary

Integer signedness error in the base64_decode function in the HTTP authentication functionality (http_auth.c) in lighttpd 1.4 before 1.4.30 and 1.5 before SVN revision 2806 allows remote attackers to cause a denial of service (segmentation fault) via crafted base64 input that triggers an out-of-bounds read with a negative index.

CVE-2011-4362 Information	
CVSS Score	5.0
CWE	CWE-189
Vulnerability impact	
Confidentiality	NONE
Integrity	NONE
Availability	PARTIAL
Access methodology information	
Vector	NETWORK
Complexity	LOW
Authentication	NONE

Vulnerable configs

lighttpd 1.4.3
lighttpd 1.4.4
lighttpd 1.4.5
lighttpd 1.4.6
lighttpd 1.4.7
lighttpd 1.4.8
lighttpd 1.4.9
lighttpd 1.4.10
lighttpd 1.4.11
lighttpd 1.4.12
lighttpd 1.4.13
lighttpd lighttpd 1.4.14
lighttpd 1.4.15
lighttpd 1.4.16
lighttpd lighttpd 1.4.17
lighttpd 1.4.18
lighttpd lighttpd 1.4.19
lighttpd lighttpd 1.4.20
lighttpd lighttpd 1.4.21
lighttpd lighttpd 1.4.22
lighttpd lighttpd 1.4.23
lighttpd lighttpd 1.4.24
lighttpd lighttpd 1.4.25
lighttpd lighttpd 1.4.26
Lighttpd 1.4.27
lighttpd 1.4.28
lighttpd 1.4.29
lighttpd 1.5.0
Debian GNU/Linux 5.0
Debian GNU/Linux 6.0
Debian Linux 7.0

References

http://archives.neohapsis.com/archives/bugtraq/2011-12/0167.html
http://blog.pi3.com.pl/?p=277
http://download.lighttpd.net/lighttpd/security/lighttpd_sa_2011_01.txt
http://redmine.lighttpd.net/issues/2370

http://www.debian.org/security/2011/dsa-2368
http://www.exploit-db.com/exploits/18295
http://www.openwall.com/lists/oss-security/2011/11/29/13
http://www.openwall.com/lists/oss-security/2011/11/29/8
http://www.securitytracker.com/id?1026359
https://bugzilla.redhat.com/show_bug.cgi?id=758624
https://exchange.xforce.ibmcloud.com/vulnerabilities/71536

Summary

The connection_state_machine function (connections.c) in lighttpd 1.4.19 and earlier, and 1.5.x before 1.5.0, allows remote attackers to cause a denial of service (active SSL connection loss) by triggering an SSL error, such as disconnecting before a download has finished, which causes all active SSL connections to be lost.

CVE-2008-1531 Information	
CVSS Score	4.3
CWE	Unknown
Vulnerability impact	
Confidentiality	NONE
Integrity	NONE
Availability	PARTIAL
Access methodology information	
Vector	NETWORK
Complexity	MEDIUM
Authentication	NONE

Vulnerable configs

lighttpd lighttpd 1.4.19
Debian GNU/Linux 4.0

References

http://lists.opensuse.org/opensuse-security-announce/2008-05/msg00000.html
http://security.gentoo.org/glsa/glsa-200804-08.xml
http://trac.lighttpd.net/trac/changeset/2136
http://trac.lighttpd.net/trac/changeset/2139
http://trac.lighttpd.net/trac/changeset/2140
http://trac.lighttpd.net/trac/ticket/285##comment:18
http://trac.lighttpd.net/trac/ticket/285##comment:21
http://wiki.rpath.com/wiki/Advisories:rPSA-2008-0132

http://www.debian.org/security/2008/dsa-1540
http://www.securityfocus.com/archive/1/490323/100/0/threaded
http://www.securityfocus.com/bid/28489
http://www.vupen.com/english/advisories/2008/1063/references
https://bugs.gentoo.org/show_bug.cgi?id=214892
https://exchange.xforce.ibmcloud.com/vulnerabilities/41545
https://issues.rpath.com/browse/RPL-2407
https://www.redhat.com/archives/fedora-package-announce/2008-April/msg00562.html
https://www.redhat.com/archives/fedora-package-announce/2008-April/msg00587.html

Summary

Use-after-free vulnerability in lighttpd before 1.4.33 allows remote attackers to cause a denial of service (segmentation fault and crash) via unspecified vectors that trigger FAMMonitorDirectory failures.

CVE-2013-4560 Information	
CVSS Score	2.6
CWE	CWE-399
Vulnerability impact	
Confidentiality	NONE
Integrity	NONE
Availability	PARTIAL
Access methodology information	
Vector	NETWORK
Complexity	HIGH
Authentication	NONE

Vulnerable configs

lighttpd 1.4.9
lighttpd 1.4.8
lighttpd 1.4.7
lighttpd 1.4.6
lighttpd 1.4.5
lighttpd 1.4.4
lighttpd 1.4.32
lighttpd 1.4.31
lighttpd 1.4.30
lighttpd 1.4.3
lighttpd 1.4.29
lighttpd 1.4.28
Lighttpd 1.4.27
lighttpd lighttpd 1.4.26
lighttpd lighttpd 1.4.25
lighttpd lighttpd 1.4.24
lighttpd lighttpd 1.4.23
lighttpd lighttpd 1.4.22
lighttpd lighttpd 1.4.21
lighttpd lighttpd 1.4.20
lighttpd lighttpd 1.4.19
lighttpd 1.4.18
lighttpd lighttpd 1.4.17
lighttpd 1.4.16
lighttpd 1.4.15
lighttpd lighttpd 1.4.14
lighttpd 1.4.13
lighttpd 1.4.12
lighttpd 1.4.11
lighttpd 1.4.10
Debian Linux 7.0
Debian Linux 7.1
Debian GNU/Linux 6.0

References

http://download.lighttpd.net/lighttpd/security/lighttpd_sa_2013_03.txt
http://lists.opensuse.org/opensuse-updates/2014-01/msg00049.html
http://marc.info/?l=bugtraq&m=141576815022399&w=2
http://www.openwall.com/lists/oss-security/2013/11/12/4
https://www.debian.org/security/2013/dsa-2795

Summary

The configuration file for the FastCGI PHP support for lighttpd before 1.4.28 on Debian GNU/Linux creates a socket file with a predictable name in /tmp, which allows local users to hijack the PHP control socket and perform unauthorized actions such as forcing the use of a different version of PHP via a symlink attack or a race condition.

CVE-2013-1427 Information	
CVSS Score	1.9
CWE	CWE-310
Vulnerability impact	
Confidentiality	NONE
Integrity	PARTIAL
Availability	NONE
Access methodology information	
Vector	LOCAL
Complexity	MEDIUM
Authentication	NONE

Vulnerable configs

Lighttpd 1.4.27
lighttpd lighttpd 1.4.25
lighttpd lighttpd 1.4.22
lighttpd lighttpd 1.4.19
lighttpd 1.4.16
lighttpd 1.4.13
lighttpd 1.4.8
lighttpd 1.4.5
lighttpd 1.3.16
lighttpd lighttpd 1.4.24
lighttpd lighttpd 1.4.21
lighttpd 1.4.18
lighttpd 1.4.15
lighttpd 1.4.10
lighttpd 1.4.7
lighttpd 1.4.4
lighttpd lighttpd 1.4.26
lighttpd lighttpd 1.4.23
lighttpd lighttpd 1.4.20
lighttpd 1.4.11
lighttpd 1.4.12
lighttpd 1.4.9
lighttpd 1.4.6
lighttpd 1.4.3
Debian Linux

References

http://www.debian.org/security/2013/dsa-2649
http://www.securityfocus.com/bid/58528
https://exchange.xforce.ibmcloud.com/vulnerabilities/82897

3 RAW SCRIPTS INFORMATION

```
NMAP Script run: vulners NMAP Script Result:
 cpe:/a:openbsd:openssh:4.7p1:
       CVE-2010-4478         7.5           https://vulners.com/cve/CVE
           -2010-4478
       CVE-2016-10708        5.0           https://vulners.com/cve/CVE
           -2016-10708
       CVE-2017-15906        5.0           https://vulners.com/cve/CVE
           -2017-15906
       CVE-2010-4755         4.0           https://vulners.com/cve/CVE
           -2010-4755
       CVE-2008-5161         2.6           https://vulners.com/cve/CVE
           -2008-5161

NMAP Script run: http-server-header NMAP Script Result: Apache/2.2.8 (Ubuntu)
    DAV/2 mod_fastcgi/2.4.6 PHP/5.2.4-2ubuntu5 with Suhosin-Patch mod_ssl/2.2.8
     OpenSSL/0.9.8g NMAP Script run: vulners NMAP Script Result:
 cpe:/a:apache:http_server:2.2.8:
       CVE-2010-0425         10.0          https://vulners.com/cve/CVE
           -2010-0425
       CVE-2011-3192         7.8           https://vulners.com/cve/CVE
           -2011-3192
       CVE-2013-2249         7.5           https://vulners.com/cve/CVE
           -2013-2249
       CVE-2017-7679         7.5           https://vulners.com/cve/CVE
           -2017-7679
       CVE-2009-1890         7.1           https://vulners.com/cve/CVE
           -2009-1890
       CVE-2009-1891         7.1           https://vulners.com/cve/CVE
           -2009-1891
       CVE-2012-0883         6.9           https://vulners.com/cve/CVE
           -2012-0883
       CVE-2013-1862         5.1           https://vulners.com/cve/CVE
           -2013-1862
       CVE-2014-0231         5.0           https://vulners.com/cve/CVE
           -2014-0231
```

```
CVE-2013-6438        5.0          https://vulners.com/cve/CVE
    -2013-6438
CVE-2011-3368        5.0          https://vulners.com/cve/CVE
    -2011-3368
CVE-2008-2364        5.0          https://vulners.com/cve/CVE
    -2008-2364
CVE-2014-0098        5.0          https://vulners.com/cve/CVE
    -2014-0098
CVE-2007-6750        5.0          https://vulners.com/cve/CVE
    -2007-6750
CVE-2010-1452        5.0          https://vulners.com/cve/CVE
    -2010-1452
CVE-2010-0408        5.0          https://vulners.com/cve/CVE
    -2010-0408
CVE-2009-2699        5.0          https://vulners.com/cve/CVE
    -2009-2699
CVE-2009-1195        4.9          https://vulners.com/cve/CVE
    -2009-1195
CVE-2012-0031        4.6          https://vulners.com/cve/CVE
    -2012-0031
CVE-2011-3607        4.4          https://vulners.com/cve/CVE
    -2011-3607
CVE-2011-4317        4.3          https://vulners.com/cve/CVE
    -2011-4317
CVE-2011-3348        4.3          https://vulners.com/cve/CVE
    -2011-3348
CVE-2011-0419        4.3          https://vulners.com/cve/CVE
    -2011-0419
CVE-2012-4558        4.3          https://vulners.com/cve/CVE
    -2012-4558
CVE-2012-0053        4.3          https://vulners.com/cve/CVE
    -2012-0053
CVE-2011-3639        4.3          https://vulners.com/cve/CVE
    -2011-3639
CVE-2008-2939        4.3          https://vulners.com/cve/CVE
    -2008-2939
```

```
      CVE-2013-1896        4.3           https://vulners.com/cve/CVE
          -2013-1896
      CVE-2016-4975        4.3           https://vulners.com/cve/CVE
          -2016-4975
      CVE-2012-3499        4.3           https://vulners.com/cve/CVE
          -2012-3499
      CVE-2010-0434        4.3           https://vulners.com/cve/CVE
          -2010-0434
      CVE-2016-8612        3.3           https://vulners.com/cve/CVE
          -2016-8612
      CVE-2012-2687        2.6           https://vulners.com/cve/CVE
          -2012-2687
      CVE-2011-4415        1.2           https://vulners.com/cve/CVE
          -2011-4415

NMAP Script run: http-server-header NMAP Script Result: Apache/2.2.8 (Ubuntu)
   DAV/2 mod_fastcgi/2.4.6 PHP/5.2.4-2ubuntu5 with Suhosin-Patch mod_ssl/2.2.8
    OpenSSL/0.9.8g NMAP Script run: vulners NMAP Script Result:
 cpe:/a:apache:http_server:2.2.8:
      CVE-2010-0425        10.0          https://vulners.com/cve/CVE
          -2010-0425
      CVE-2011-3192        7.8           https://vulners.com/cve/CVE
          -2011-3192
      CVE-2013-2249        7.5           https://vulners.com/cve/CVE
          -2013-2249
      CVE-2017-7679        7.5           https://vulners.com/cve/CVE
          -2017-7679
      CVE-2009-1890        7.1           https://vulners.com/cve/CVE
          -2009-1890
      CVE-2009-1891        7.1           https://vulners.com/cve/CVE
          -2009-1891
      CVE-2012-0883        6.9           https://vulners.com/cve/CVE
          -2012-0883
      CVE-2013-1862        5.1           https://vulners.com/cve/CVE
          -2013-1862
      CVE-2014-0231        5.0           https://vulners.com/cve/CVE
          -2014-0231
```

```
CVE-2013-6438       5.0         https://vulners.com/cve/CVE
    -2013-6438
CVE-2011-3368       5.0         https://vulners.com/cve/CVE
    -2011-3368
CVE-2008-2364       5.0         https://vulners.com/cve/CVE
    -2008-2364
CVE-2014-0098       5.0         https://vulners.com/cve/CVE
    -2014-0098
CVE-2007-6750       5.0         https://vulners.com/cve/CVE
    -2007-6750
CVE-2010-1452       5.0         https://vulners.com/cve/CVE
    -2010-1452
CVE-2010-0408       5.0         https://vulners.com/cve/CVE
    -2010-0408
CVE-2009-2699       5.0         https://vulners.com/cve/CVE
    -2009-2699
CVE-2009-1195       4.9         https://vulners.com/cve/CVE
    -2009-1195
CVE-2012-0031       4.6         https://vulners.com/cve/CVE
    -2012-0031
CVE-2011-3607       4.4         https://vulners.com/cve/CVE
    -2011-3607
CVE-2011-4317       4.3         https://vulners.com/cve/CVE
    -2011-4317
CVE-2011-3348       4.3         https://vulners.com/cve/CVE
    -2011-3348
CVE-2011-0419       4.3         https://vulners.com/cve/CVE
    -2011-0419
CVE-2012-4558       4.3         https://vulners.com/cve/CVE
    -2012-4558
CVE-2012-0053       4.3         https://vulners.com/cve/CVE
    -2012-0053
CVE-2011-3639       4.3         https://vulners.com/cve/CVE
    -2011-3639
CVE-2008-2939       4.3         https://vulners.com/cve/CVE
    -2008-2939
```

```
      CVE-2013-1896        4.3           https://vulners.com/cve/CVE
          -2013-1896
      CVE-2016-4975        4.3           https://vulners.com/cve/CVE
          -2016-4975
      CVE-2012-3499        4.3           https://vulners.com/cve/CVE
          -2012-3499
      CVE-2010-0434        4.3           https://vulners.com/cve/CVE
          -2010-0434
      CVE-2016-8612        3.3           https://vulners.com/cve/CVE
          -2016-8612
      CVE-2012-2687        2.6           https://vulners.com/cve/CVE
          -2012-2687
      CVE-2011-4415        1.2           https://vulners.com/cve/CVE
          -2011-4415



NMAP Script run: fingerprint-strings NMAP Script Result:
 GenericLines, beast2:
   *** bWAPP Movie Service ***
   Matching movies: 0



NMAP Script run: http-server-header NMAP Script Result: nginx/1.4.0 NMAP Script
    run: vulners NMAP Script Result:
 nginx 1.4.0:
      CVE-2013-2070        5.8           https://vulners.com/cve/CVE
          -2013-2070
NMAP Script run: http-server-header NMAP Script Result: nginx/1.4.0 NMAP Script
    run: vulners NMAP Script Result:
 nginx 1.4.0:
      CVE-2013-2070        5.8           https://vulners.com/cve/CVE
          -2013-2070
NMAP Script run: http-server-header NMAP Script Result: lighttpd/1.4.19 NMAP
   Script run: vulners NMAP Script Result:
```

```
cpe:/a:lighttpd:lighttpd:1.4.19:
        CVE-2013-4559           7.6             https://vulners.com/cve/CVE
            -2013-4559
        CVE-2014-2323           7.5             https://vulners.com/cve/CVE
            -2014-2323
        CVE-2008-4360           7.5             https://vulners.com/cve/CVE
            -2008-4360
        CVE-2008-4359           7.5             https://vulners.com/cve/CVE
            -2008-4359
        CVE-2014-2324           5.0             https://vulners.com/cve/CVE
            -2014-2324
        CVE-2010-0295           5.0             https://vulners.com/cve/CVE
            -2010-0295
        CVE-2018-19052          5.0             https://vulners.com/cve/CVE
            -2018-19052
        CVE-2008-4298           5.0             https://vulners.com/cve/CVE
            -2008-4298
        CVE-2011-4362           5.0             https://vulners.com/cve/CVE
            -2011-4362
        CVE-2008-1531           4.3             https://vulners.com/cve/CVE
            -2008-1531
        CVE-2013-4560           2.6             https://vulners.com/cve/CVE
            -2013-4560
        CVE-2013-1427           1.9             https://vulners.com/cve/CVE
            -2013-1427
```

189