Service: ssh 3.9p1

CVE ID: CVE-2007-1365

Publish Date: 2007-03-10 21:19:00

Exploit Exists: No

Summary: Buffer overflow in kern/uipc_mbuf2.c in OpenBSD 3.9 and 4.0 allows remote attackers to execute arbitrary code via fragmented IPv6 packets due to "incorrect mbuf handling for ICMP6 packets." NOTE: this was originally reported as a denial of service.

CVSS Severity: HIGH

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

EPSS Score: 0.44190)

Overflow: Yes

Code Execution: Yes

Denial of Service: Yes

Memory Corruption: No

Sql Injection: No

Xss: No

Directory Traversal: No

File Inclusion: No

Csrf: No

Xxe: No

Ssrf: No

Open Redirect: No

Input Validation: No

Bypass Something: No

Gain Privilege: No

Information Leak: No

CVE ID: CVE-2007-1351

Publish Date: 2007-04-06 01:19:00

Exploit Exists: No

Summary: Integer overflow in the bdfReadCharacters function in bdfread.c in (1) X.Org libXfont before 20070403 and (2) freetype 2.3.2 and earlier allows remote authenticated users to execute arbitrary code via crafted BDF fonts, which result in a heap overflow.

CVSS Severity: HIGH

Attack Vector: AV:N/AC:M/Au:S/C:C/I:C/A:C

EPSS Score: 0.05034)

Overflow: Yes

Code Execution: Yes

Denial of Service: No

Memory Corruption: No

Sql Injection: No

Xss: No

Directory Traversal: No

File Inclusion: No

Csrf: No

Xxe: No

Ssrf: No

Open Redirect: No

Input Validation: No

Bypass Something: No

Gain Privilege: No

Information Leak: No

CVE ID: CVE-2006-4924

Publish Date: 2006-09-27 01:07:00

Exploit Exists: No

Summary: sshd in OpenSSH before 4.4, when using the version 1 SSH protocol, allows remote attackers to cause a denial of service (CPU consumption) via an SSH packet that contains duplicate blocks, which is not properly handled by the CRC compensation attack detector.

CVSS Severity: HIGH

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

EPSS Score: 0.94601)

Overflow: No

Code Execution: No

Denial of Service: Yes

Memory Corruption: No

Sql Injection: No

Xss: No

Directory Traversal: No

File Inclusion: No

Csrf: No

Xxe: No

Ssrf: No

Open Redirect: No

Input Validation: No

Bypass Something: No

Gain Privilege: No

Information Leak: No

CVE ID: CVE-2010-4478

Publish Date: 2010-12-06 22:30:32

Exploit Exists: No

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.

CVSS Severity: HIGH

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

EPSS Score: 0.02241)

Overflow: No

Code Execution: No

Denial of Service: No

Memory Corruption: No

Sql Injection: No

Xss: No

Directory Traversal: No

File Inclusion: No

Csrf: No

Xxe: No

Ssrf: No

Open Redirect: No

Input Validation: No

Bypass Something: Yes

Gain Privilege: Yes

Information Leak: No

CVE ID: CVE-2012-1577

Publish Date: 2019-12-10 19:15:14

Exploit Exists: No

Summary: lib/libc/stdlib/random.c in OpenBSD returns 0 when seeded with 0.

CVSS Severity: HIGH

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

EPSS Score: 0.01346)

Overflow: No

Code Execution: No

Denial of Service: No

Memory Corruption: No

Sql Injection: No

Xss: No

Directory Traversal: No

File Inclusion: No

Csrf: No

Xxe: No

Ssrf: No

Open Redirect: No

Input Validation: No

Bypass Something: No

Gain Privilege: No

Information Leak: No

CVE ID: CVE-2008-4609

Publish Date: 2008-10-20 17:59:26

Exploit Exists: No

Summary: The TCP implementation in (1) Linux, (2) platforms based on BSD Unix, (3) Microsoft Windows, (4) Cisco products, and probably other operating systems allows remote attackers to cause a denial of service (connection queue exhaustion) via multiple vectors that manipulate information in the TCP state table, as demonstrated by sockstress.

CVSS Severity: HIGH

Attack Vector: AV:N/AC:M/Au:N/C:N/I:N/A:C

EPSS Score: 0.04547)

Overflow: No

Code Execution: No

Denial of Service: Yes

Memory Corruption: No

Sql Injection: No

Xss: No

Directory Traversal: No

File Inclusion: No

Csrf: No

Xxe: No

Ssrf: No

Open Redirect: No

Input Validation: No

Bypass Something: No

Gain Privilege: No

Information Leak: No

CVE ID: CVE-2020-15778

Publish Date: 2020-07-24 14:15:12

Exploit Exists: No

Summary: scp in OpenSSH through 8.3p1 allows command injection in the scp.c toremote function, as demonstrated by backtick characters in the destination argument. NOTE: the vendor reportedly has stated that they intentionally omit validation of "anomalous argument transfers" because that could "stand a great chance of breaking existing workflows."

CVSS Severity: MEDIUM

Attack Vector: AV:N/AC:M/Au:N/C:P/I:P/A:P

EPSS Score: 0.00289)

Overflow: No

Code Execution: No

Denial of Service: No

Memory Corruption: No

Sql Injection: No

Xss: No

Directory Traversal: No

File Inclusion: No

Csrf: No

Xxe: No

Ssrf: No

Open Redirect: No

Input Validation: No

Bypass Something: No

Gain Privilege: No

Information Leak: No

CVE ID: CVE-2004-1653

Publish Date: 2004-08-31 04:00:00

Exploit Exists: No

Summary: The default configuration for OpenSSH enables AllowTcpForwarding, which could allow remote authenticated users to perform a port bounce, when configured with an anonymous access program such as AnonCVS.

CVSS Severity: MEDIUM

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

EPSS Score: 0.01041)

Overflow: No

Code Execution: No

Denial of Service: No

Memory Corruption: No

Sql Injection: No

Xss: No

Directory Traversal: No

File Inclusion: No

Csrf: No

Xxe: No

Ssrf: No

Open Redirect: No

Input Validation: No

Bypass Something: No

Gain Privilege: No

Information Leak: No

CVE ID: CVE-2007-0085

Publish Date: 2007-01-05 11:28:00

Exploit Exists: No

Summary: Unspecified vulnerability in sys/dev/pci/vga_pci.c in the VGA graphics driver for wscons in OpenBSD 3.9 and 4.0, when the kernel is compiled with the PCIAGP option and a non-AGP device is

being used, allows local users to gain privileges via unspecified vectors, possibly related to agp_ioctl NULL pointer reference.

CVSS Severity: MEDIUM

Attack Vector: AV:L/AC:H/Au:S/C:C/I:C/A:C

EPSS Score: 0.00043)

Overflow: No

Code Execution: No

Denial of Service: No

Memory Corruption: No

Sql Injection: No

Xss: No

Directory Traversal: No

File Inclusion: No

Csrf: No

Xxe: No

Ssrf: No

Open Redirect: No

Input Validation: No

Bypass Something: No

Gain Privilege: No

Information Leak: No

CVE ID: CVE-2011-2168

Publish Date: 2011-05-24 23:55:05

Exploit Exists: No

Summary: Multiple integer overflows in the glob implementation in libc in OpenBSD before 4.9 might allow context-dependent attackers to have an unspecified impact via a crafted string, related to the GLOB_APPEND and GLOB_DOOFFS flags, a different issue than CVE-2011-0418.

CVSS Severity: MEDIUM

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

EPSS Score: 0.00268)

Overflow: No

Code Execution: No

Denial of Service: No

Memory Corruption: No

Sql Injection: No

Xss: No

Directory Traversal: No

File Inclusion: No

Csrf: No

Xxe: No

Ssrf: No

Open Redirect: No

Input Validation: No

Bypass Something: No

Gain Privilege: No

Information Leak: No

CVE ID: CVE-2010-5107

Publish Date: 2013-03-07 20:55:01

Exploit Exists: No

Summary: The default configuration of OpenSSH through 6.1 enforces a fixed time limit between establishing a TCP connection and completing a login, which makes it easier for remote attackers to cause a denial of service (connection-slot exhaustion) by periodically making many new TCP connections.

CVSS Severity: MEDIUM

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

EPSS Score: 0.07870)

Overflow: No

Code Execution: No

Denial of Service: Yes

Memory Corruption: No

Sql Injection: No

Xss: No

Directory Traversal: No

File Inclusion: No

Csrf: No

Xxe: No

Ssrf: No

Open Redirect: No

Input Validation: No

Bypass Something: No

Gain Privilege: No

Information Leak: No

CVE ID: CVE-2008-4109

Publish Date: 2008-09-18 15:04:27

Exploit Exists: No

Summary: A certain Debian patch for OpenSSH before 4.3p2-9etch3 on etch; before 4.6p1-1 on sid and lenny; and on other distributions such as SUSE uses functions that are not async-signal-safe in the signal handler for login timeouts, which allows remote attackers to cause a denial of service (connection slot exhaustion) via multiple login attempts. NOTE: this issue exists because of an incorrect fix for CVE-2006-5051.

CVSS Severity: MEDIUM

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

EPSS Score: 0.04479)

Overflow: No

Code Execution: No

Denial of Service: Yes

Memory Corruption: No

Sql Injection: No

Xss: No

Directory Traversal: No

File Inclusion: No

Csrf: No

Xxe: No

Ssrf: No

Open Redirect: No

Input Validation: No

Bypass Something: No

Gain Privilege: No

Information Leak: No

CVE ID: CVE-2007-2243

Publish Date: 2007-04-25 16:19:00

Exploit Exists: No

Summary: OpenSSH 4.6 and earlier, when ChallengeResponseAuthentication is enabled, allows remote attackers to determine the existence of user accounts by attempting to authenticate via S/KEY, which displays a different response if the user account exists, a similar issue to CVE-2001-1483.

CVSS Severity: MEDIUM

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

EPSS Score: 0.00954)

Overflow: No

Code Execution: No

Denial of Service: No

Memory Corruption: No

Sql Injection: No

Xss: No

Directory Traversal: No

File Inclusion: No

Csrf: No

Xxe: No

Ssrf: No

Open Redirect: No

Input Validation: No

Bypass Something: Yes

Gain Privilege: Yes

Information Leak: No

CVE ID: CVE-2006-5052

Publish Date: 2006-09-27 23:07:00

Exploit Exists: No

Summary: Unspecified vulnerability in portable OpenSSH before 4.4, when running on some platforms, allows remote attackers to determine the validity of usernames via unknown vectors involving a GSSAPI "authentication abort."

CVSS Severity: MEDIUM

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

EPSS Score: 0.02249)

Overflow: No

Code Execution: No

Denial of Service: No

Memory Corruption: No

Sql Injection: No

Xss: No

Directory Traversal: No

File Inclusion: No

Csrf: No

Xxe: No

Ssrf: No

Open Redirect: No

Input Validation: No

Bypass Something: No

Gain Privilege: No

Information Leak: No

CVE ID: CVE-2005-2798

Publish Date: 2005-09-06 17:03:00

Exploit Exists: No

Summary: sshd in OpenSSH before 4.2, when GSSAPIDelegateCredentials is enabled, allows GSSAPI credentials to be delegated to clients who log in using non-GSSAPI methods, which could cause those credentials to be exposed to untrusted users or hosts.

CVSS Severity: MEDIUM

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

EPSS Score: 0.01362)

Overflow: No

Code Execution: No

Denial of Service: No

Memory Corruption: No

Sql Injection: No

Xss: No

Directory Traversal: No

File Inclusion: No

Csrf: No

Xxe: No

Ssrf: No

Open Redirect: No

Input Validation: No

Bypass Something: No

Gain Privilege: No

Information Leak: No

CVE ID: CVE-2009-0537

Publish Date: 2009-03-09 21:30:00

Exploit Exists: No

Summary: Integer overflow in the fts_build function in fts.c in libc in (1) OpenBSD 4.4 and earlier and (2) Microsoft Interix 6.0 build 10.0.6030.0 allows context-dependent attackers to cause a denial of service (application crash) via a deep directory tree, related to the fts_level structure member, as demonstrated by (a) du, (b) rm, (c) chmod, and (d) chgrp on OpenBSD; and (e) SearchIndexer.exe on Vista Enterprise.

CVSS Severity: MEDIUM

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

EPSS Score: 0.00156)

Overflow: Yes

Code Execution: No

Denial of Service: Yes

Memory Corruption: No

Sql Injection: No

Xss: No

Directory Traversal: No

File Inclusion: No

Csrf: No

Xxe: No

Ssrf: No

Open Redirect: No

Input Validation: No

Bypass Something: No

Gain Privilege: No

Information Leak: No

CVE ID: CVE-2006-0225

Publish Date: 2006-01-25 11:03:00

Exploit Exists: No

Summary: scp in OpenSSH 4.2p1 allows attackers to execute arbitrary commands via filenames that contain shell metacharacters or spaces, which are expanded twice.

CVSS Severity: MEDIUM

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

EPSS Score: 0.00111)

Overflow: No

Code Execution: No

Denial of Service: No

Memory Corruption: No

Sql Injection: No

Xss: No

Directory Traversal: No

File Inclusion: No

Csrf: No

Xxe: No

Ssrf: No

Open Redirect: No

Input Validation: No

Bypass Something: No

Gain Privilege: No

Information Leak: No

CVE ID: CVE-2016-20012

Publish Date: 2021-09-15 20:15:07

Exploit Exists: No

Summary: OpenSSH through 8.7 allows remote attackers, who have a suspicion that a certain combination of username and public key is known to an SSH server, to test whether this suspicion is correct. This occurs because a challenge is sent only when that combination could be valid for a login session. NOTE: the vendor does not recognize user enumeration as a vulnerability for this product

CVSS Severity: MEDIUM

Attack Vector: AV:N/AC:M/Au:N/C:P/I:N/A:N

EPSS Score: 0.00477)

Overflow: No

Code Execution: No

Denial of Service: No

Memory Corruption: No

Sql Injection: No

Xss: No

Directory Traversal: No

File Inclusion: No

Csrf: No

Xxe: No

Ssrf: No

Open Redirect: No

Input Validation: No

Bypass Something: No

Gain Privilege: No

Information Leak: No

CVE ID: CVE-2010-4755

Publish Date: 2011-03-02 20:00:01

Exploit Exists: No

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.

CVSS Severity: MEDIUM

Attack Vector: AV:N/AC:L/Au:S/C:N/I:N/A:P

EPSS Score: 0.01098)

Overflow: No

Code Execution: No

Denial of Service: Yes

Memory Corruption: No

Sql Injection: No

Xss: No

Directory Traversal: No

File Inclusion: No

Csrf: No

Xxe: No

Ssrf: No

Open Redirect: No

Input Validation: No

Bypass Something: No

Gain Privilege: No

Information Leak: No

CVE ID: CVE-2007-1352

Publish Date: 2007-04-06 01:19:00

Exploit Exists: No

Summary: Integer overflow in the FontFileInitTable function in X.Org libXfont before 20070403 allows remote authenticated users to execute arbitrary code via a long first line in the fonts.dir file, which results in a heap overflow.

CVSS Severity: LOW

Attack Vector: AV:A/AC:M/Au:S/C:N/I:P/A:P

EPSS Score: 0.02921)

Overflow: Yes

Code Execution: Yes

Denial of Service: No

Memory Corruption: No

Sql Injection: No

Xss: No

Directory Traversal: No

File Inclusion: No

Csrf: No

Xxe: No

Ssrf: No

Open Redirect: No

Input Validation: No

Bypass Something: No

Gain Privilege: No

Information Leak: No

CVE ID: CVE-2012-0814

Publish Date: 2012-01-27 19:55:01

Exploit Exists: No

Summary: The auth_parse_options function in auth-options.c in sshd in OpenSSH before 5.7 provides debug messages containing authorized_keys command options, which allows remote authenticated users to obtain potentially sensitive information by reading these messages, as demonstrated by the shared user account required by Gitolite. NOTE: this can cross privilege boundaries because a user account may intentionally have no shell or filesystem access, and therefore may have no supported way to read an authorized_keys file in its own home directory.

CVSS Severity: LOW

Attack Vector: AV:N/AC:M/Au:S/C:P/I:N/A:N

EPSS Score: 0.00285)

Overflow: No

Code Execution: No

Denial of Service: No

Memory Corruption: No

Sql Injection: No

Xss: No

Directory Traversal: No

File Inclusion: No

Csrf: No

Xxe: No

Ssrf: No

Open Redirect: No

Input Validation: No

Bypass Something: No

Gain Privilege: No

Information Leak: No

CVE ID: CVE-2011-5000

Publish Date: 2012-04-05 14:55:04

Exploit Exists: No

Summary: The ssh_gssapi_parse_ename function in gss-serv.c in OpenSSH 5.8 and earlier, when gssapi-with-mic authentication is enabled, allows remote authenticated users to cause a denial of service (memory consumption) via a large value in a certain length field. NOTE: there may be limited scenarios in which this issue is relevant.

CVSS Severity: LOW

Attack Vector: AV:N/AC:M/Au:S/C:N/I:N/A:P

EPSS Score: 0.00353)

Overflow: No

Code Execution: No

Denial of Service: Yes

Memory Corruption: No

Sql Injection: No

Xss: No

Directory Traversal: No

File Inclusion: No

Csrf: No

Xxe: No

Ssrf: No

Open Redirect: No

Input Validation: No

Bypass Something: No

Gain Privilege: No

Information Leak: No

CVE ID: CVE-2023-51767

Publish Date: 2023-12-24 07:15:07

Exploit Exists: No

Summary: OpenSSH through 9.6, when common types of DRAM are used, might allow row hammer attacks (for authentication bypass) because the integer value of authenticated in mm_answer_authpassword does not resist flips of a single bit. NOTE: this is applicable to a certain threat model of attacker-victim co-location in which the attacker has user privileges.

CVSS Severity: HIGH

Attack Vector: CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H

EPSS Score: 0.00051)

Overflow: No

Code Execution: No

Denial of Service: No

Memory Corruption: No

Sql Injection: No

Xss: No

Directory Traversal: No

File Inclusion: No

Csrf: No

Xxe: No

Ssrf: No

Open Redirect: No

Input Validation: No

Bypass Something: No

Gain Privilege: No

Information Leak: No

CVE ID: CVE-2011-4327

Publish Date: 2014-02-03 03:55:04

Exploit Exists: No

Summary: ssh-keysign.c in ssh-keysign in OpenSSH before 5.8p2 on certain platforms executes ssh-rand-helper with unintended open file descriptors, which allows local users to obtain sensitive key information via the ptrace system call.

CVSS Severity: LOW

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

EPSS Score: 0.00042)

Overflow: No

Code Execution: No

Denial of Service: No

Memory Corruption: No

Sql Injection: No

Xss: No

Directory Traversal: No

File Inclusion: No

Csrf: No

Xxe: No

Ssrf: No

Open Redirect: No

Input Validation: No

Bypass Something: No

Gain Privilege: No

Information Leak: Yes

CVE ID: CVE-2008-3259

Publish Date: 2008-07-22 16:41:00

Exploit Exists: No

Summary: OpenSSH before 5.1 sets the SO_REUSEADDR socket option when the X11UseLocalhost configuration setting is disabled, which allows local users on some platforms to hijack the X11 forwarding port via a bind to a single IP address, as demonstrated on the HP-UX platform.

CVSS Severity: LOW

Attack Vector: AV:L/AC:H/Au:N/C:P/I:N/A:N

EPSS Score: 0.00042)

Overflow: No

Code Execution: No

Denial of Service: No

Memory Corruption: No

Sql Injection: No

Xss: No

Directory Traversal: No

File Inclusion: No

Csrf: No

Xxe: No

Ssrf: No

Open Redirect: No

Input Validation: No

Bypass Something: No

Gain Privilege: No

Information Leak: Yes

CVE ID: CVE-2005-2666

Publish Date: 2005-08-23 04:00:00

Exploit Exists: No

Summary: SSH, as implemented in OpenSSH before 4.0 and possibly other implementations, stores hostnames, IP addresses, and keys in plaintext in the known_hosts file, which makes it easier for an attacker that has compromised an SSH user's account to generate a list of additional targets that are more likely to have the same password or key.

CVSS Severity: LOW

Attack Vector: AV:L/AC:H/Au:N/C:P/I:N/A:N

EPSS Score: 0.00071)

Overflow: No

Code Execution: No

Denial of Service: No

Memory Corruption: No

Sql Injection: No

Xss: No

Directory Traversal: No

File Inclusion: No

Csrf: No

Xxe: No

Ssrf: No

Open Redirect: No

Input Validation: No

Bypass Something: No

Gain Privilege: No

Information Leak: No

Service: http 2.0.52

CVE ID: CVE-2005-2700

Publish Date: 2005-09-06 23:03:00

Exploit Exists: No

Summary: ssl_engine_kernel.c in mod_ssl before 2.8.24, when using "SSLVerifyClient optional" in the global virtual host configuration, does not properly enforce "SSLVerifyClient require" in a per-location context, which allows remote attackers to bypass intended access restrictions.

CVSS Severity: HIGH

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

EPSS Score: 0.00214)

Overflow: No

Code Execution: No

Denial of Service: No

Memory Corruption: No

Sql Injection: No

Xss: No

Directory Traversal: No

File Inclusion: No

Csrf: No

Xxe: No

Ssrf: No

Open Redirect: No

Input Validation: No

Bypass Something: No

Gain Privilege: No

Information Leak: No

CVE ID: CVE-2011-3192

Publish Date: 2011-08-29 15:55:02

Exploit Exists: Yes

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.

CVSS Severity: HIGH

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

EPSS Score: 0.96165)

Overflow: No

Code Execution: No

Denial of Service: Yes

Memory Corruption: No

Sql Injection: No

Xss: No

Directory Traversal: No

File Inclusion: No

Csrf: No

Xxe: No

Ssrf: No

Open Redirect: No

Input Validation: No

Bypass Something: No

Gain Privilege: No

Information Leak: No

CVE ID: CVE-2006-3747

Publish Date: 2006-07-28 18:02:00

Exploit Exists: Yes

Summary: Off-by-one error in the ldap scheme handling in the Rewrite module (mod_rewrite) in Apache 1.3 from 1.3.28, 2.0.46 and other versions before 2.0.59, and 2.2, when RewriteEngine is enabled, allows remote attackers to cause a denial of service (application crash) and possibly execute arbitrary code via crafted URLs that are not properly handled using certain rewrite rules.

CVSS Severity: HIGH

Attack Vector: AV:N/AC:H/Au:N/C:C/I:C/A:C

EPSS Score: 0.97401)

Overflow: No

Code Execution: Yes

Denial of Service: Yes

Memory Corruption: No

Sql Injection: No

Xss: No

Directory Traversal: No

File Inclusion: No

Csrf: No

Xxe: No

Ssrf: No

Open Redirect: No

Input Validation: No

Bypass Something: No

Gain Privilege: No

Information Leak: No

CVE ID: CVE-2005-1344

Publish Date: 2005-05-02 04:00:00

Exploit Exists: No

Summary: Buffer overflow in htdigest in Apache 2.0.52 may allow attackers to execute arbitrary code via a long realm argument. NOTE: since htdigest is normally only locally accessible and not setuid or setgid, there are few attack vectors which would lead to an escalation of privileges, unless htdigest is executed from a CGI program. Therefore this may not be a vulnerability.

CVSS Severity: HIGH

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

EPSS Score: 0.00401)

Overflow: Yes

Code Execution: Yes

Denial of Service: No

Memory Corruption: No

Sql Injection: No

Xss: No

Directory Traversal: No

File Inclusion: No

Csrf: No

Xxe: No

Ssrf: No

Open Redirect: No

Input Validation: No

Bypass Something: No

Gain Privilege: No

Information Leak: No

CVE ID: CVE-2004-0885

Publish Date: 2004-11-03 05:00:00

Exploit Exists: No

Summary: The mod_ssl module in Apache 2.0.35 through 2.0.52, when using the "SSLCipherSuite" directive in directory or location context, allows remote clients to bypass intended restrictions by using any cipher suite that is allowed by the virtual host configuration.

CVSS Severity: HIGH

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

EPSS Score: 0.00180)

Overflow: No

Code Execution: No

Denial of Service: No

Memory Corruption: No

Sql Injection: No

Xss: No

Directory Traversal: No

File Inclusion: No

Csrf: No

Xxe: No

Ssrf: No

Open Redirect: No

Input Validation: No

Bypass Something: No

Gain Privilege: No

Information Leak: No

CVE ID: CVE-2009-1891

Publish Date: 2009-07-10 15:30:00

Exploit Exists: No

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).

CVSS Severity: HIGH

Attack Vector: AV:N/AC:M/Au:N/C:N/I:N/A:C

EPSS Score: 0.00492)

Overflow: No

Code Execution: No

Denial of Service: Yes

Memory Corruption: No

Sql Injection: No

Xss: No

Directory Traversal: No

File Inclusion: No

Csrf: No

Xxe: No

Ssrf: No

Open Redirect: No

Input Validation: No

Bypass Something: No

Gain Privilege: No

Information Leak: No

CVE ID: CVE-2006-4154

Publish Date: 2006-10-16 19:07:00

Exploit Exists: No

Summary: Format string vulnerability in the mod_tcl module 1.0 for Apache 2.x allows context-dependent attackers to execute arbitrary code via format string specifiers that are not properly handled in a set_var function call in (1) tcl_cmds.c and (2) tcl_core.c.

CVSS Severity: MEDIUM

Attack Vector: AV:N/AC:M/Au:N/C:P/I:P/A:P

EPSS Score: 0.84746)

Overflow: No

Code Execution: Yes

Denial of Service: No

Memory Corruption: No

Sql Injection: No

Xss: No

Directory Traversal: No

File Inclusion: No

Csrf: No

Xxe: No

Ssrf: No

Open Redirect: No

Input Validation: No

Bypass Something: No

Gain Privilege: No

Information Leak: No

CVE ID: CVE-2005-3357

Publish Date: 2005-12-31 05:00:00

Exploit Exists: No

Summary: mod_ssl in Apache 2.0 up to 2.0.55, when configured with an SSL vhost with access control and a custom error 400 error page, allows remote attackers to cause a denial of service (application crash) via a non-SSL request to an SSL port, which triggers a NULL pointer dereference.

CVSS Severity: MEDIUM

Attack Vector: AV:N/AC:H/Au:N/C:N/I:N/A:C

EPSS Score: 0.97267)

Overflow: No

Code Execution: No

Denial of Service: Yes

Memory Corruption: Yes

Sql Injection: No

Xss: No

Directory Traversal: No

File Inclusion: No

Csrf: No

Xxe: No

Ssrf: No

Open Redirect: No

Input Validation: No

Bypass Something: No

Gain Privilege: No

Information Leak: No

CVE ID: CVE-2013-1862

Publish Date: 2013-06-10 17:55:02

Exploit Exists: No

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.

CVSS Severity: MEDIUM

Attack Vector: AV:N/AC:H/Au:N/C:P/I:P/A:P

EPSS Score: 0.38256)

Overflow: No

Code Execution: No

Denial of Service: No

Memory Corruption: No

Sql Injection: No

Xss: No

Directory Traversal: No

File Inclusion: No

Csrf: No

Xxe: No

Ssrf: No

Open Redirect: No

Input Validation: No

Bypass Something: No

Gain Privilege: No

Information Leak: No

CVE ID: CVE-2023-31122

Publish Date: 2023-10-23 07:15:11

Exploit Exists: No

Summary: Out-of-bounds Read vulnerability in mod_macro of Apache HTTP Server.This issue affects Apache HTTP Server: through 2.4.57.

CVSS Severity: CRITICAL

Attack Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:H

EPSS Score: 0.00759)

Overflow: No

Code Execution: No

Denial of Service: No

Memory Corruption: No

Sql Injection: No

Xss: No

Directory Traversal: No

File Inclusion: No

Csrf: No

Xxe: No

Ssrf: No

Open Redirect: No

Input Validation: No

Bypass Something: No

Gain Privilege: No

Information Leak: No

CVE ID: CVE-2011-3368

Publish Date: 2011-10-05 22:55:03

Exploit Exists: Yes

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.

CVSS Severity: MEDIUM

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

EPSS Score: 0.97321)

Overflow: No

Code Execution: No

Denial of Service: No

Memory Corruption: No

Sql Injection: No

Xss: No

Directory Traversal: No

File Inclusion: No

Csrf: No

Xxe: No

Ssrf: No

Open Redirect: No

Input Validation: Yes

Bypass Something: No

Gain Privilege: No

Information Leak: No

CVE ID: CVE-2010-1623

Publish Date: 2010-10-04 21:00:04

Exploit Exists: No

Summary: Memory leak in the apr_brigade_split_line function in buckets/apr_brigade.c in the Apache Portable Runtime Utility library (aka APR-util) before 1.3.10, as used in the mod_reqtimeout module in the Apache HTTP Server and other software, allows remote attackers to cause a denial of service (memory consumption) via unspecified vectors related to the destruction of an APR bucket.

CVSS Severity: MEDIUM

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

EPSS Score: 0.42531)

Overflow: Yes

Code Execution: No

Denial of Service: Yes

Memory Corruption: No

Sql Injection: No

Xss: No

Directory Traversal: No

File Inclusion: No

Csrf: No

Xxe: No

Ssrf: No

Open Redirect: No

Input Validation: No

Bypass Something: No

Gain Privilege: No

Information Leak: No

CVE ID: CVE-2010-1452

Publish Date: 2010-07-28 20:00:01

Exploit Exists: No

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.

CVSS Severity: MEDIUM

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

EPSS Score: 0.22992)

Overflow: No

Code Execution: No

Denial of Service: Yes

Memory Corruption: No

Sql Injection: No

Xss: No

Directory Traversal: No

File Inclusion: No

Csrf: No

Xxe: No

Ssrf: No

Open Redirect: No

Input Validation: No

Bypass Something: No

Gain Privilege: No

Information Leak: No

CVE ID: CVE-2009-3720

Publish Date: 2009-11-03 16:30:13

Exploit Exists: No

Summary: The updatePosition function in lib/xmltok_impl.c in libexpat in Expat 2.0.1, as used in Python, PyXML, w3c-libwww, and other software, allows context-dependent attackers to cause a denial of service (application crash) via an XML document with crafted UTF-8 sequences that trigger a buffer over-read, a different vulnerability than CVE-2009-2625.

CVSS Severity: MEDIUM

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

EPSS Score: 0.03228)

Overflow: No

Code Execution: No

Denial of Service: Yes

Memory Corruption: No

Sql Injection: No

Xss: No

Directory Traversal: No

File Inclusion: No

Csrf: No

Xxe: No

Ssrf: No

Open Redirect: No

Input Validation: No

Bypass Something: No

Gain Privilege: No

Information Leak: No

CVE ID: CVE-2009-3560

Publish Date: 2009-12-04 21:30:01

Exploit Exists: No

Summary: The big2_toUtf8 function in lib/xmltok.c in libexpat in Expat 2.0.1, as used in the XML-Twig module for Perl, allows context-dependent attackers to cause a denial of service (application crash) via an XML document with malformed UTF-8 sequences that trigger a buffer over-read, related to the doProlog function in lib/xmlparse.c, a different vulnerability than CVE-2009-2625 and CVE-2009-3720.

CVSS Severity: MEDIUM

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

EPSS Score: 0.01275)

Overflow: Yes

Code Execution: No

Denial of Service: Yes

Memory Corruption: No

Sql Injection: No

Xss: No

Directory Traversal: No

File Inclusion: No

Csrf: No

Xxe: No

Ssrf: No

Open Redirect: No

Input Validation: No

Bypass Something: No

Gain Privilege: No

Information Leak: No

CVE ID: CVE-2009-3095

Publish Date: 2009-09-08 18:30:01

Exploit Exists: No

Summary: The mod_proxy_ftp module in the Apache HTTP Server allows remote attackers to bypass intended access restrictions and send arbitrary commands to an FTP server via vectors related to the embedding of these commands in the Authorization HTTP header, as demonstrated by a certain module in VulnDisco Pack Professional 8.11.

CVSS Severity: MEDIUM

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

EPSS Score: 0.00946)

Overflow: No

Code Execution: No

Denial of Service: No

Memory Corruption: No

Sql Injection: No

Xss: No

Directory Traversal: No

File Inclusion: No

Csrf: No

Xxe: No

Ssrf: No

Open Redirect: No

Input Validation: No

Bypass Something: No

Gain Privilege: No

Information Leak: No

CVE ID: CVE-2008-2364

Publish Date: 2008-06-13 18:41:00

Exploit Exists: No

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.

CVSS Severity: MEDIUM

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

EPSS Score: 0.00700)

Overflow: No

Code Execution: No

Denial of Service: Yes

Memory Corruption: No

Sql Injection: No

Xss: No

Directory Traversal: No

File Inclusion: No

Csrf: No

Xxe: No

Ssrf: No

Open Redirect: No

Input Validation: No

Bypass Something: No

Gain Privilege: No

Information Leak: No

CVE ID: CVE-2007-6750

Publish Date: 2011-12-27 18:55:01

Exploit Exists: Yes

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.

CVSS Severity: MEDIUM

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

EPSS Score: 0.01696)

Overflow: No

Code Execution: No

Denial of Service: Yes

Memory Corruption: No

Sql Injection: No

Xss: No

Directory Traversal: No

File Inclusion: No

Csrf: No

Xxe: No

Ssrf: No

Open Redirect: No

Input Validation: No

Bypass Something: No

Gain Privilege: No

Information Leak: No

CVE ID: CVE-2007-3847

Publish Date: 2007-08-23 22:17:00

Exploit Exists: No

Summary: The date handling code in modules/proxy/proxy_util.c (mod_proxy) in Apache 2.3.0, when using a threaded MPM, allows remote origin servers to cause a denial of service (caching forward proxy process crash) via crafted date headers that trigger a buffer over-read.

CVSS Severity: MEDIUM

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

EPSS Score: 0.00715)

Overflow: No

Code Execution: No

Denial of Service: Yes

Memory Corruption: No

Sql Injection: No

Xss: No

Directory Traversal: No

File Inclusion: No

Csrf: No

Xxe: No

Ssrf: No

Open Redirect: No

Input Validation: No

Bypass Something: No

Gain Privilege: No

Information Leak: No

CVE ID: CVE-2007-1863

Publish Date: 2007-06-27 17:30:00

Exploit Exists: No

Summary: cache_util.c in the mod_cache module in Apache HTTP Server (httpd), when caching is enabled and a threaded Multi-Processing Module (MPM) is used, allows remote attackers to cause a denial of service (child processing handler crash) via a request with the (1) s-maxage, (2) max-age, (3) min-fresh, or (4) max-stale Cache-Control headers without a value.

CVSS Severity: MEDIUM

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

EPSS Score: 0.87682)

Overflow: No

Code Execution: No

Denial of Service: Yes

Memory Corruption: No

Sql Injection: No

Xss: No

Directory Traversal: No

File Inclusion: No

Csrf: No

Xxe: No

Ssrf: No

Open Redirect: No

Input Validation: No

Bypass Something: No

Gain Privilege: No

Information Leak: No

CVE ID: CVE-2005-2970

Publish Date: 2005-10-25 17:06:00

Exploit Exists: No

Summary: Memory leak in the worker MPM (worker.c) for Apache 2, in certain circumstances, allows remote attackers to cause a denial of service (memory consumption) via aborted connections, which prevents the memory for the transaction pool from being reused for other connections.

CVSS Severity: MEDIUM

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

EPSS Score: 0.00794)

Overflow: No

Code Execution: No

Denial of Service: Yes

Memory Corruption: No

Sql Injection: No

Xss: No

Directory Traversal: No

File Inclusion: No

Csrf: No

Xxe: No

Ssrf: No

Open Redirect: No

Input Validation: No

Bypass Something: No

Gain Privilege: No

Information Leak: No

CVE ID: CVE-2005-2728

Publish Date: 2005-08-30 11:45:00

Exploit Exists: No

Summary: The byte-range filter in Apache 2.0 before 2.0.54 allows remote attackers to cause a denial of service (memory consumption) via an HTTP header with a large Range field.

CVSS Severity: MEDIUM

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

EPSS Score: 0.93963)

Overflow: No

Code Execution: No

Denial of Service: Yes

Memory Corruption: No

Sql Injection: No

Xss: No

Directory Traversal: No

File Inclusion: No

Csrf: No

Xxe: No

Ssrf: No

Open Redirect: No

Input Validation: No

Bypass Something: No

Gain Privilege: No

Information Leak: No

CVE ID: CVE-2005-1268

Publish Date: 2005-08-05 04:00:00

Exploit Exists: No

Summary: Off-by-one error in the mod_ssl Certificate Revocation List (CRL) verification callback in Apache, when configured to use a CRL, allows remote attackers to cause a denial of service (child process crash) via a CRL that causes a buffer overflow of one null byte.

CVSS Severity: MEDIUM

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

EPSS Score: 0.00886)

Overflow: Yes

Code Execution: No

Denial of Service: Yes

Memory Corruption: No

Sql Injection: No

Xss: No

Directory Traversal: No

File Inclusion: No

Csrf: No

Xxe: No

Ssrf: No

Open Redirect: No

Input Validation: No

Bypass Something: No

Gain Privilege: No

Information Leak: No

CVE ID: CVE-2004-0942

Publish Date: 2005-02-09 05:00:00

Exploit Exists: No

Summary: Apache webserver 2.0.52 and earlier allows remote attackers to cause a denial of service (CPU consumption) via an HTTP GET request with a MIME header containing multiple lines with a large number of space characters.

CVSS Severity: MEDIUM

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

EPSS Score: 0.96511)

Overflow: No

Code Execution: No

Denial of Service: Yes

Memory Corruption: No

Sql Injection: No

Xss: No

Directory Traversal: No

File Inclusion: No

Csrf: No

Xxe: No

Ssrf: No

Open Redirect: No

Input Validation: No

Bypass Something: No

Gain Privilege: No

Information Leak: No

CVE ID: CVE-2007-3304

Publish Date: 2007-06-20 22:30:00

Exploit Exists: No

Summary: Apache httpd 1.3.37, 2.0.59, and 2.2.4 with the Prefork MPM module, allows local users to cause a denial of service by modifying the worker_score and process_score arrays to reference an arbitrary process ID, which is sent a SIGUSR1 signal from the master process, aka "SIGUSR1 killer."

CVSS Severity: MEDIUM

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

EPSS Score: 0.00044)

Overflow: No

Code Execution: No

Denial of Service: Yes

Memory Corruption: No

Sql Injection: No

Xss: No

Directory Traversal: No

File Inclusion: No

Csrf: No

Xxe: No

Ssrf: No

Open Redirect: No

Input Validation: No

Bypass Something: No

Gain Privilege: No

Information Leak: No

CVE ID: CVE-2012-0031

Publish Date: 2012-01-18 20:55:03

Exploit Exists: No

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.

CVSS Severity: MEDIUM

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

EPSS Score: 0.00043)

Overflow: No

Code Execution: No

Denial of Service: Yes

Memory Corruption: No

Sql Injection: No

Xss: No

Directory Traversal: No

File Inclusion: No

Csrf: No

Xxe: No

Ssrf: No

Open Redirect: No

Input Validation: No

Bypass Something: No

Gain Privilege: No

Information Leak: No

CVE ID: CVE-2011-3607

Publish Date: 2011-11-08 11:55:06

Exploit Exists: No

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.

CVSS Severity: MEDIUM

Attack Vector: AV:L/AC:M/Au:N/C:P/I:P/A:P

EPSS Score: 0.00062)

Overflow: Yes

Code Execution: No

Denial of Service: No

Memory Corruption: No

Sql Injection: No

Xss: No

Directory Traversal: No

File Inclusion: No

Csrf: No

Xxe: No

Ssrf: No

Open Redirect: No

Input Validation: No

Bypass Something: No

Gain Privilege: No

Information Leak: No

CVE ID: CVE-2012-0053

Publish Date: 2012-01-28 04:05:01

Exploit Exists: No

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.

CVSS Severity: MEDIUM

Attack Vector: AV:N/AC:M/Au:N/C:P/I:N/A:N

EPSS Score: 0.73964)

Overflow: No

Code Execution: No

Denial of Service: No

Memory Corruption: No

Sql Injection: No

Xss: No

Directory Traversal: No

File Inclusion: No

Csrf: No

Xxe: No

Ssrf: No

Open Redirect: No

Input Validation: No

Bypass Something: No

Gain Privilege: No

Information Leak: No

CVE ID: CVE-2011-4317

Publish Date: 2011-11-30 04:05:59

Exploit Exists: No

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.

CVSS Severity: MEDIUM

Attack Vector: AV:N/AC:M/Au:N/C:N/I:P/A:N

EPSS Score: 0.93695)

Overflow: No

Code Execution: No

Denial of Service: No

Memory Corruption: No

Sql Injection: No

Xss: No

Directory Traversal: No

File Inclusion: No

Csrf: No

Xxe: No

Ssrf: No

Open Redirect: No

Input Validation: Yes

Bypass Something: No

Gain Privilege: No

Information Leak: No

CVE ID: CVE-2011-3639

Publish Date: 2011-11-30 04:05:58

Exploit Exists: No

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.

CVSS Severity: MEDIUM

Attack Vector: AV:N/AC:M/Au:N/C:N/I:P/A:N

EPSS Score: 0.03505)

Overflow: No

Code Execution: No

Denial of Service: No

Memory Corruption: No

Sql Injection: No

Xss: No

Directory Traversal: No

File Inclusion: No

Csrf: No

Xxe: No

Ssrf: No

Open Redirect: No

Input Validation: Yes

Bypass Something: No

Gain Privilege: No

Information Leak: No

CVE ID: CVE-2010-0434

Publish Date: 2010-03-05 19:30:01

Exploit Exists: No

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.

CVSS Severity: MEDIUM

Attack Vector: AV:N/AC:M/Au:N/C:P/I:N/A:N

EPSS Score: 0.00316)

Overflow: No

Code Execution: No

Denial of Service: No

Memory Corruption: No

Sql Injection: No

Xss: No

Directory Traversal: No

File Inclusion: No

Csrf: No

Xxe: No

Ssrf: No

Open Redirect: No

Input Validation: No

Bypass Something: No

Gain Privilege: No

Information Leak: Yes

CVE ID: CVE-2008-2939

Publish Date: 2008-08-06 18:41:00

Exploit Exists: No

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.

CVSS Severity: MEDIUM

Attack Vector: AV:N/AC:M/Au:N/C:N/I:P/A:N

EPSS Score: 0.05366)

Overflow: No

Code Execution: No

Denial of Service: No

Memory Corruption: No

Sql Injection: No

Xss: Yes

Directory Traversal: No

File Inclusion: No

Csrf: No

Xxe: No

Ssrf: No

Open Redirect: No

Input Validation: No

Bypass Something: No

Gain Privilege: No

Information Leak: No

CVE ID: CVE-2008-2168

Publish Date: 2008-05-13 21:20:00

Exploit Exists: No

Summary: Cross-site scripting (XSS) vulnerability in Apache 2.2.6 and earlier allows remote attackers to inject arbitrary web script or HTML via UTF-7 encoded URLs that are not properly handled when displaying the 403 Forbidden error page.

CVSS Severity: MEDIUM

Attack Vector: AV:N/AC:M/Au:N/C:N/I:P/A:N

EPSS Score: 0.02221)

Overflow: No

Code Execution: No

Denial of Service: No

Memory Corruption: No

Sql Injection: No

Xss: Yes

Directory Traversal: No

File Inclusion: No

Csrf: No

Xxe: No

Ssrf: No

Open Redirect: No

Input Validation: No

Bypass Something: No

Gain Privilege: No

Information Leak: No

CVE ID: CVE-2008-0005

Publish Date: 2008-01-12 00:46:00

Exploit Exists: No

Summary: mod_proxy_ftp in Apache 2.2.x before 2.2.7-dev, 2.0.x before 2.0.62-dev, and 1.3.x before 1.3.40-dev does not define a charset, which allows remote attackers to conduct cross-site scripting (XSS) attacks using UTF-7 encoding.

CVSS Severity: MEDIUM

Attack Vector: AV:N/AC:M/Au:N/C:N/I:P/A:N

EPSS Score: 0.01494)

Overflow: No

Code Execution: No

Denial of Service: No

Memory Corruption: No

Sql Injection: No

Xss: Yes

Directory Traversal: No

File Inclusion: No

Csrf: No

Xxe: No

Ssrf: No

Open Redirect: No

Input Validation: No

Bypass Something: No

Gain Privilege: No

Information Leak: No

CVE ID: CVE-2007-6388

Publish Date: 2008-01-08 18:46:00

Exploit Exists: No

Summary: Cross-site scripting (XSS) vulnerability in mod_status in the Apache HTTP Server 2.2.0 through 2.2.6, 2.0.35 through 2.0.61, and 1.3.2 through 1.3.39, when the server-status page is enabled, allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.

CVSS Severity: MEDIUM

Attack Vector: AV:N/AC:M/Au:N/C:N/I:P/A:N

EPSS Score: 0.81803)

Overflow: No

Code Execution: No

Denial of Service: No

Memory Corruption: No

Sql Injection: No

Xss: Yes

Directory Traversal: No

File Inclusion: No

Csrf: No

Xxe: No

Ssrf: No

Open Redirect: No

Input Validation: No

Bypass Something: No

Gain Privilege: No

Information Leak: No

CVE ID: CVE-2007-6203

Publish Date: 2007-12-03 22:46:00

Exploit Exists: No

Summary: Apache HTTP Server 2.0.x and 2.2.x does not sanitize the HTTP Method specifier header from an HTTP request when it is reflected back in a "413 Request Entity Too Large" error message, which might allow cross-site scripting (XSS) style attacks using web client components that can send

arbitrary headers in requests, as demonstrated via an HTTP request containing an invalid Content-length value, a similar issue to CVE-2006-3918.

CVSS Severity: MEDIUM

Attack Vector: AV:N/AC:M/Au:N/C:N/I:P/A:N

EPSS Score: 0.97200)

Overflow: No

Code Execution: No

Denial of Service: No

Memory Corruption: No

Sql Injection: No

Xss: Yes

Directory Traversal: No

File Inclusion: No

Csrf: No

Xxe: No

Ssrf: No

Open Redirect: No

Input Validation: No

Bypass Something: No

Gain Privilege: No

Information Leak: No

CVE ID: CVE-2007-5000

Publish Date: 2007-12-13 18:46:00

Exploit Exists: No

Summary: Cross-site scripting (XSS) vulnerability in the (1) mod_imap module in the Apache HTTP Server 1.3.0 through 1.3.39 and 2.0.35 through 2.0.61 and the (2) mod_imagemap module in the Apache HTTP Server 2.2.0 through 2.2.6 allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.

CVSS Severity: MEDIUM

Attack Vector: AV:N/AC:M/Au:N/C:N/I:P/A:N

EPSS Score: 0.64572)

Overflow: No

Code Execution: No

Denial of Service: No

Memory Corruption: No

Sql Injection: No

Xss: Yes

Directory Traversal: No

File Inclusion: No

Csrf: No

Xxe: No

Ssrf: No

Open Redirect: No

Input Validation: No

Bypass Something: No

Gain Privilege: No

Information Leak: No

CVE ID: CVE-2007-4465

Publish Date: 2007-09-14 00:17:00

Exploit Exists: No

Summary: Cross-site scripting (XSS) vulnerability in mod_autoindex.c in the Apache HTTP Server before 2.2.6, when the charset on a server-generated page is not defined, allows remote attackers to inject arbitrary web script or HTML via the P parameter using the UTF-7 charset. NOTE: it could be argued that this issue is due to a design limitation of browsers that attempt to perform automatic content type detection.

CVSS Severity: MEDIUM

Attack Vector: AV:N/AC:M/Au:N/C:N/I:P/A:N

EPSS Score: 0.01700)

Overflow: No

Code Execution: No

Denial of Service: No

Memory Corruption: No

Sql Injection: No

Xss: Yes

Directory Traversal: No

File Inclusion: No

Csrf: No

Xxe: No

Ssrf: No

Open Redirect: No

Input Validation: No

Bypass Something: No

Gain Privilege: No

Information Leak: No

CVE ID: CVE-2006-5752

Publish Date: 2007-06-27 17:30:00

Exploit Exists: No

Summary: Cross-site scripting (XSS) vulnerability in mod_status.c in the mod_status module in Apache HTTP Server (httpd), when ExtendedStatus is enabled and a public server-status page is used, allows remote attackers to inject arbitrary web script or HTML via unspecified vectors involving charsets with browsers that perform "charset detection" when the content-type is not specified.

CVSS Severity: MEDIUM

Attack Vector: AV:N/AC:M/Au:N/C:N/I:P/A:N

EPSS Score: 0.07835)

Overflow: No

Code Execution: No

Denial of Service: No

Memory Corruption: No

Sql Injection: No

Xss: Yes

Directory Traversal: No

File Inclusion: No

Csrf: No

Xxe: No

Ssrf: No

Open Redirect: No

Input Validation: No

Bypass Something: No

Gain Privilege: No

Information Leak: No

CVE ID: CVE-2005-3352

Publish Date: 2005-12-13 20:03:00

Exploit Exists: No

Summary: Cross-site scripting (XSS) vulnerability in the mod_imap module of Apache httpd before 1.3.35-dev and Apache httpd 2.0.x before 2.0.56-dev allows remote attackers to inject arbitrary web script or HTML via the Referer when using image maps.

CVSS Severity: MEDIUM

Attack Vector: AV:N/AC:M/Au:N/C:N/I:P/A:N

EPSS Score: 0.01623)

Overflow: No

Code Execution: No

Denial of Service: No

Memory Corruption: No

Sql Injection: No

Xss: Yes

Directory Traversal: No

File Inclusion: No

Csrf: No

Xxe: No

Ssrf: No

Open Redirect: No

Input Validation: No

Bypass Something: No

Gain Privilege: No

Information Leak: No

CVE ID: CVE-2005-2088

Publish Date: 2005-07-05 04:00:00

Exploit Exists: No

Summary: The Apache HTTP server before 1.3.34, and 2.0.x before 2.0.55, when acting as an HTTP proxy, allows remote attackers to poison the web cache, bypass web application firewall protection, and conduct XSS attacks via an HTTP request with both a "Transfer-Encoding: chunked" header and a Content-Length header, which causes Apache to incorrectly handle and forward the body of the request in a way that causes the receiving server to process it as a separate HTTP request, aka "HTTP Request Smuggling."

CVSS Severity: MEDIUM

Attack Vector: AV:N/AC:M/Au:N/C:N/I:P/A:N

EPSS Score: 0.96340)

Overflow: No

Code Execution: No

Denial of Service: No

Memory Corruption: No

Sql Injection: No

Xss: Yes

Directory Traversal: No

File Inclusion: No

Csrf: No

Xxe: No

Ssrf: No

Open Redirect: No

Input Validation: No

Bypass Something: No

Gain Privilege: No

Information Leak: No

CVE ID: CVE-2016-8612

Publish Date: 2018-03-09 20:29:00

Exploit Exists: No

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.

CVSS Severity: LOW

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

EPSS Score: 0.00114)

Overflow: No

Code Execution: No

Denial of Service: No

Memory Corruption: Yes

Sql Injection: No

Xss: No

Directory Traversal: No

File Inclusion: No

Csrf: No

Xxe: No

Ssrf: No

Open Redirect: No

Input Validation: Yes

Bypass Something: No

Gain Privilege: No

Information Leak: No

CVE ID: CVE-2023-45802

Publish Date: 2023-10-23 07:15:11

Exploit Exists: No

Summary: When a HTTP/2 stream was reset (RST frame) by a client, there was a time window were the request's memory resources were not reclaimed immediately. Instead, de-allocation was deferred to connection close. A client could send new requests and resets, keeping the connection busy and open and causing the memory footprint to keep on growing. On connection close, all resources were reclaimed, but the process might run out of memory before that. This was found by the reporter during testing of CVE-2023-44487 (HTTP/2 Rapid Reset Exploit) with their own test client. During "normal" HTTP/2 use, the probability to hit this bug is very low. The kept memory would not become noticeable before the connection closes or times out. Users are recommended to upgrade to version 2.4.58, which fixes the issue.

CVSS Severity: MEDIUM

Attack Vector: CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H

EPSS Score: 0.00177)

Overflow: No

Code Execution: No

Denial of Service: No

Memory Corruption: No

Sql Injection: No

Xss: No

Directory Traversal: No

File Inclusion: No

Csrf: No

Xxe: No

Ssrf: No

Open Redirect: No

Input Validation: No

Bypass Something: No

Gain Privilege: No

Information Leak: No

CVE ID: CVE-2009-3094

Publish Date: 2009-09-08 18:30:01

Exploit Exists: No

Summary: The ap_proxy_ftp_handler function in modules/proxy/proxy_ftp.c in the mod_proxy_ftp module in the Apache HTTP Server 2.0.63 and 2.2.13 allows remote FTP servers to cause a denial of service (NULL pointer dereference and child process crash) via a malformed reply to an EPSV command.

CVSS Severity: LOW

Attack Vector: AV:N/AC:H/Au:N/C:N/I:N/A:P

EPSS Score: 0.00151)

Overflow: No

Code Execution: No

Denial of Service: Yes

Memory Corruption: Yes

Sql Injection: No

Xss: No

Directory Traversal: No

File Inclusion: No

Csrf: No

Xxe: No

Ssrf: No

Open Redirect: No

Input Validation: No

Bypass Something: No

Gain Privilege: No

Information Leak: No

CVE ID: CVE-2011-4415

Publish Date: 2011-11-08 11:55:06

Exploit Exists: No

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.

CVSS Severity: LOW

Attack Vector: AV:L/AC:H/Au:N/C:N/I:N/A:P

EPSS Score: 0.00042)

Overflow: No

Code Execution: No

Denial of Service: Yes

Memory Corruption: Yes

Sql Injection: No

Xss: No

Directory Traversal: No

File Inclusion: No

Csrf: No

Xxe: No

Ssrf: No

Open Redirect: No

Input Validation: Yes

Bypass Something: No

Gain Privilege: No

Information Leak: No

Service: rpcbind 2

No CVEs associated with this service.

Service: https

No CVEs associated with this service.

Service: ipp 1.1

No CVEs associated with this service.

Service: status 1

No CVEs associated with this service.

Service: mysql

No CVEs associated with this service.