Vulnerability Report 07/10/18

# Software: httpd 1.3

## CVEs from Vulners

### CVE-1999-0067

## CVEs from CPE

No vulnerability found in CPE.

# Software: tomcat 5.0.25

## CVEs from Vulners

### CVE-2007-2450

## CVEs from CPE

### CVE-2006-7195 --> Score: 4.3

Cross-site scripting (XSS) vulnerability in implicit-objects.jsp in Apache Tomcat 5.0.0 through 5.0.30 and 5.5.0 through 5.5.17 allows remote attackers to inject arbitrary web script or HTML via certain header values.

### CVE-2007-1355 --> Score: 4.3

Multiple cross-site scripting (XSS) vulnerabilities in the appdev/sample/web/hello.jsp example application in Tomcat 4.0.0 through 4.0.6, 4.1.0 through 4.1.36, 5.0.0 through 5.0.30, 5.5.0 through 5.5.23, and 6.0.0 through 6.0.10 allow remote attackers to inject arbitrary web script or HTML via the test parameter and unspecified vectors.

### CVE-2007-1858 --> Score: 2.6

The default SSL cipher configuration in Apache Tomcat 4.1.28 through 4.1.31, 5.0.0 through 5.0.30, and 5.5.0 through 5.5.17 uses certain insecure ciphers, including the anonymous cipher, which allows remote attackers to obtain sensitive information or have other, unspecified impacts.

### CVE-2006-7196 --> Score: 4.3

Cross-site scripting (XSS) vulnerability in the calendar application example in Apache Tomcat 4.0.0 through 4.0.6, 4.1.0 through 4.1.31, 5.0.0 through 5.0.30, and 5.5.0 through 5.5.15 allows remote attackers to inject arbitrary web script or HTML via the time parameter to cal2.jsp and possibly unspecified other vectors. NOTE: this may be related to CVE-2006-0254.1.

### CVE-2007-2449 --> Score: 4.3

Multiple cross-site scripting (XSS) vulnerabilities in certain JSP files in the examples web application in Apache Tomcat 4.0.0 through 4.0.6, 4.1.0 through 4.1.36, 5.0.0 through 5.0.30, 5.5.0 through 5.5.24, and 6.0.0 through 6.0.13 allow remote attackers to inject arbitrary web script or HTML via the portion of the URI after the ';' character, as demonstrated by a URI containing a "snp/snoop.jsp;" sequence.

### CVE-2013-6357 --> Score: 6.8

\*\* DISPUTED \*\* Cross-site request forgery (CSRF) vulnerability in the Manager application in Apache Tomcat 5.5.25 and earlier allows remote attackers to hijack the authentication of administrators for requests that manipulate application deployment via the POST method, as demonstrated by a /manager/html/undeploy?path= URI. NOTE: the vendor disputes the significance of this report, stating that "the Apache Tomcat Security team has not accepted any reports of CSRF attacks against the Manager application ... as they require a reckless system administrator."

### CVE-2007-3382 --> Score: 4.3

Apache Tomcat 6.0.0 to 6.0.13, 5.5.0 to 5.5.24, 5.0.0 to 5.0.30, 4.1.0 to 4.1.36, and 3.3 to 3.3.2 treats single quotes ("'") as delimiters in cookies, which might cause sensitive information such as session IDs to be leaked and allow remote attackers to conduct session hijacking attacks.

### CVE-2007-2450 --> Score: 3.5

Multiple cross-site scripting (XSS) vulnerabilities in the (1) Manager and (2) Host Manager web applications in Apache Tomcat 4.0.0 through 4.0.6, 4.1.0 through 4.1.36, 5.0.0 through 5.0.30, 5.5.0 through 5.5.24, and 6.0.0 through 6.0.13 allow remote authenticated users to inject arbitrary web script or HTML via a parameter name to manager/html/upload, and other unspecified vectors.

### CVE-2007-3385 --> Score: 4.3

Apache Tomcat 6.0.0 to 6.0.13, 5.5.0 to 5.5.24, 5.0.0 to 5.0.30, 4.1.0 to 4.1.36, and 3.3 to 3.3.2 does not properly handle the \" character sequence in a cookie value, which might cause sensitive information such as session IDs to be leaked to remote attackers and enable session hijacking attacks.

### CVE-2009-3548 --> Score: 7.5

The Windows installer for Apache Tomcat 6.0.0 through 6.0.20, 5.5.0 through 5.5.28, and possibly earlier versions uses a blank default password for the administrative user, which allows remote attackers to gain privileges.

### CVE-2008-5519 --> Score: 2.6

The JK Connector (aka mod\_jk) 1.2.0 through 1.2.26 in Apache Tomcat allows remote attackers to obtain sensitive information via an arbitrary request from an HTTP client, in opportunistic circumstances involving (1) a request from a different client that included a Content-Length header but no POST data or (2) a rapid series of requests, related to noncompliance with the AJP protocol's requirements for requests containing Content-Length headers.

### CVE-2013-4590 --> Score: 4.3

Apache Tomcat before 6.0.39, 7.x before 7.0.50, and 8.x before 8.0.0-RC10 allows attackers to obtain "Tomcat internals" information by leveraging the presence of an untrusted web application with a context.xml, web.xml, \*.jspx, \*.tagx, or \*.tld XML document containing an external entity declaration in conjunction with an entity reference, related to an XML External Entity (XXE) issue.

### CVE-2013-4322 --> Score: 4.3

Apache Tomcat before 6.0.39, 7.x before 7.0.50, and 8.x before 8.0.0-RC10 processes chunked transfer coding without properly handling (1) a large total amount of chunked data or (2) whitespace characters in an HTTP header value within a trailer field, which allows remote attackers to cause a denial of service by streaming data. NOTE: this vulnerability exists because of an incomplete fix for CVE-2012-3544.

### CVE-2012-5568 --> Score: 5.0

Apache Tomcat through 7.0.x allows remote attackers to cause a denial of service (daemon outage) via partial HTTP requests, as demonstrated by Slowloris.

### CVE-2013-4286 --> Score: 5.8

Apache Tomcat before 6.0.39, 7.x before 7.0.47, and 8.x before 8.0.0-RC3, when an HTTP connector or AJP connector is used, does not properly handle certain inconsistent HTTP request headers, which allows remote attackers to trigger incorrect identification of a request's length and conduct request-smuggling attacks via (1) multiple Content-Length headers or (2) a Content-Length header and a "Transfer-Encoding: chunked" header. NOTE: this vulnerability exists because of an incomplete fix for CVE-2005-2090.

# Software: tomcat 6.0.32

## CVEs from Vulners

No vulnerability found in CPE.

## CVEs from CPE

### CVE-2011-3375 --> Score: 5.0

Apache Tomcat 6.0.30 through 6.0.33 and 7.x before 7.0.22 does not properly perform certain caching and recycling operations involving request objects, which allows remote attackers to obtain unintended read access to IP address and HTTP header information in opportunistic circumstances by reading TCP data.

### CVE-2011-2729 --> Score: 5.0

native/unix/native/jsvc-unix.c in jsvc in the Daemon component 1.0.3 through 1.0.6 in Apache Commons, as used in Apache Tomcat 5.5.32 through 5.5.33, 6.0.30 through 6.0.32, and 7.0.x before 7.0.20 on Linux, does not drop capabilities, which allows remote attackers to bypass read permissions for files via a request to an application.

### CVE-2013-2067 --> Score: 6.8

java/org/apache/catalina/authenticator/FormAuthenticator.java in the form authentication feature in Apache Tomcat 6.0.21 through 6.0.36 and 7.x before 7.0.33 does not properly handle the relationships between authentication requirements and sessions, which allows remote attackers to inject a request into a session by sending this request during completion of the login form, a variant of a session fixation attack.

### CVE-2011-1184 --> Score: 5.0

The HTTP Digest Access Authentication implementation in Apache Tomcat 5.5.x before 5.5.34, 6.x before 6.0.33, and 7.x before 7.0.12 does not have the expected countermeasures against replay attacks, which makes it easier for remote attackers to bypass intended access restrictions by sniffing the network for valid requests, related to lack of checking of nonce (aka server nonce) and nc (aka nonce-count or client nonce count) values.

### CVE-2011-2204 --> Score: 1.9

Apache Tomcat 5.5.x before 5.5.34, 6.x before 6.0.33, and 7.x before 7.0.17, when the MemoryUserDatabase is used, creates log entries containing passwords upon encountering errors in JMX user creation, which allows local users to obtain sensitive information by reading a log file.

### CVE-2011-2526 --> Score: 4.4

Apache Tomcat 5.5.x before 5.5.34, 6.x before 6.0.33, and 7.x before 7.0.19, when sendfile is enabled for the HTTP APR or HTTP NIO connector, does not validate certain request attributes, which allows local users to bypass intended file access restrictions or cause a denial of service (infinite loop or JVM crash) by leveraging an untrusted web application.

### CVE-2012-4534 --> Score: 2.6

org/apache/tomcat/util/net/NioEndpoint.java in Apache Tomcat 6.x before 6.0.36 and 7.x before 7.0.28, when the NIO connector is used in conjunction with sendfile and HTTPS, allows remote attackers to cause a denial of service (infinite loop) by terminating the connection during the reading of a response.

### CVE-2011-4858 --> Score: 5.0

Apache Tomcat before 5.5.35, 6.x before 6.0.35, and 7.x before 7.0.23 computes hash values for form parameters without restricting the ability to trigger hash collisions predictably, which allows remote attackers to cause a denial of service (CPU consumption) by sending many crafted parameters.

### CVE-2011-5064 --> Score: 4.3

DigestAuthenticator.java in the HTTP Digest Access Authentication implementation in Apache Tomcat 5.5.x before 5.5.34, 6.x before 6.0.33, and 7.x before 7.0.12 uses Catalina as the hard-coded server secret (aka private key), which makes it easier for remote attackers to bypass cryptographic protection mechanisms by leveraging knowledge of this string, a different vulnerability than CVE-2011-1184.

### CVE-2011-5062 --> Score: 5.0

The HTTP Digest Access Authentication implementation in Apache Tomcat 5.5.x before 5.5.34, 6.x before 6.0.33, and 7.x before 7.0.12 does not check qop values, which might allow remote attackers to bypass intended integrity-protection requirements via a qop=auth value, a different vulnerability than CVE-2011-1184.

### CVE-2011-3190 --> Score: 7.5

Certain AJP protocol connector implementations in Apache Tomcat 7.0.0 through 7.0.20, 6.0.0 through 6.0.33, 5.5.0 through 5.5.33, and possibly other versions allow remote attackers to spoof AJP requests, bypass authentication, and obtain sensitive information by causing the connector to interpret a request body as a new request.

### CVE-2012-3544 --> Score: 5.0

Apache Tomcat 6.x before 6.0.37 and 7.x before 7.0.30 does not properly handle chunk extensions in chunked transfer coding, which allows remote attackers to cause a denial of service by streaming data.

### CVE-2012-4431 --> Score: 4.3

org/apache/catalina/filters/CsrfPreventionFilter.java in Apache Tomcat 6.x before 6.0.36 and 7.x before 7.0.32 allows remote attackers to bypass the cross-site request forgery (CSRF) protection mechanism via a request that lacks a session identifier.

### CVE-2011-5063 --> Score: 4.3

The HTTP Digest Access Authentication implementation in Apache Tomcat 5.5.x before 5.5.34, 6.x before 6.0.33, and 7.x before 7.0.12 does not check realm values, which might allow remote attackers to bypass intended access restrictions by leveraging the availability of a protection space with weaker authentication or authorization requirements, a different vulnerability than CVE-2011-1184.

### CVE-2012-2733 --> Score: 5.0

java/org/apache/coyote/http11/InternalNioInputBuffer.java in the HTTP NIO connector in Apache Tomcat 6.x before 6.0.36 and 7.x before 7.0.28 does not properly restrict the request-header size, which allows remote attackers to cause a denial of service (memory consumption) via a large amount of header data.

### CVE-2012-3546 --> Score: 4.3

org/apache/catalina/realm/RealmBase.java in Apache Tomcat 6.x before 6.0.36 and 7.x before 7.0.30, when FORM authentication is used, allows remote attackers to bypass security-constraint checks by leveraging a previous setUserPrincipal call and then placing /j\_security\_check at the end of a URI.

### CVE-2012-5887 --> Score: 5.0

The HTTP Digest Access Authentication implementation in Apache Tomcat 5.5.x before 5.5.36, 6.x before 6.0.36, and 7.x before 7.0.30 does not properly check for stale nonce values in conjunction with enforcement of proper credentials, which makes it easier for remote attackers to bypass intended access restrictions by sniffing the network for valid requests.

### CVE-2012-0022 --> Score: 5.0

Apache Tomcat 5.5.x before 5.5.35, 6.x before 6.0.34, and 7.x before 7.0.23 uses an inefficient approach for handling parameters, which allows remote attackers to cause a denial of service (CPU consumption) via a request that contains many parameters and parameter values, a different vulnerability than CVE-2011-4858.

### CVE-2016-0706 --> Score: 4.0

Apache Tomcat 6.x before 6.0.45, 7.x before 7.0.68, 8.x before 8.0.31, and 9.x before 9.0.0.M2 does not place org.apache.catalina.manager.StatusManagerServlet on the org/apache/catalina/core/RestrictedServlets.properties list, which allows remote authenticated users to bypass intended SecurityManager restrictions and read arbitrary HTTP requests, and consequently discover session ID values, via a crafted web application.

### CVE-2012-5886 --> Score: 5.0

The HTTP Digest Access Authentication implementation in Apache Tomcat 5.5.x before 5.5.36, 6.x before 6.0.36, and 7.x before 7.0.30 caches information about the authenticated user within the session state, which makes it easier for remote attackers to bypass authentication via vectors related to the session ID.

### CVE-2015-5174 --> Score: 4.0

Directory traversal vulnerability in RequestUtil.java in Apache Tomcat 6.x before 6.0.45, 7.x before 7.0.65, and 8.x before 8.0.27 allows remote authenticated users to bypass intended SecurityManager restrictions and list a parent directory via a /.. (slash dot dot) in a pathname used by a web application in a getResource, getResourceAsStream, or getResourcePaths call, as demonstrated by the $CATALINA\_BASE/webapps directory.

### CVE-2012-5885 --> Score: 5.0

The replay-countermeasure functionality in the HTTP Digest Access Authentication implementation in Apache Tomcat 5.5.x before 5.5.36, 6.x before 6.0.36, and 7.x before 7.0.30 tracks cnonce (aka client nonce) values instead of nonce (aka server nonce) and nc (aka nonce-count) values, which makes it easier for remote attackers to bypass intended access restrictions by sniffing the network for valid requests, a different vulnerability than CVE-2011-1184.

### CVE-2016-0714 --> Score: 6.5

The session-persistence implementation in Apache Tomcat 6.x before 6.0.45, 7.x before 7.0.68, 8.x before 8.0.31, and 9.x before 9.0.0.M2 mishandles session attributes, which allows remote authenticated users to bypass intended SecurityManager restrictions and execute arbitrary code in a privileged context via a web application that places a crafted object in a session.

### CVE-2015-5345 --> Score: 5.0

The Mapper component in Apache Tomcat 6.x before 6.0.45, 7.x before 7.0.68, 8.x before 8.0.30, and 9.x before 9.0.0.M2 processes redirects before considering security constraints and Filters, which allows remote attackers to determine the existence of a directory via a URL that lacks a trailing / (slash) character.

### CVE-2014-0227 --> Score: 6.4

java/org/apache/coyote/http11/filters/ChunkedInputFilter.java in Apache Tomcat 6.x before 6.0.42, 7.x before 7.0.55, and 8.x before 8.0.9 does not properly handle attempts to continue reading data after an error has occurred, which allows remote attackers to conduct HTTP request smuggling attacks or cause a denial of service (resource consumption) by streaming data with malformed chunked transfer coding.

### CVE-2014-0075 --> Score: 5.0

Integer overflow in the parseChunkHeader function in java/org/apache/coyote/http11/filters/ChunkedInputFilter.java in Apache Tomcat before 6.0.40, 7.x before 7.0.53, and 8.x before 8.0.4 allows remote attackers to cause a denial of service (resource consumption) via a malformed chunk size in chunked transfer coding of a request during the streaming of data.

### CVE-2014-0119 --> Score: 4.3

Apache Tomcat before 6.0.40, 7.x before 7.0.54, and 8.x before 8.0.6 does not properly constrain the class loader that accesses the XML parser used with an XSLT stylesheet, which allows remote attackers to (1) read arbitrary files via a crafted web application that provides an XML external entity declaration in conjunction with an entity reference, related to an XML External Entity (XXE) issue, or (2) read files associated with different web applications on a single Tomcat instance via a crafted web application.

### CVE-2014-0230 --> Score: 7.8

Apache Tomcat 6.x before 6.0.44, 7.x before 7.0.55, and 8.x before 8.0.9 does not properly handle cases where an HTTP response occurs before finishing the reading of an entire request body, which allows remote attackers to cause a denial of service (thread consumption) via a series of aborted upload attempts.

### CVE-2014-7810 --> Score: 5.0

The Expression Language (EL) implementation in Apache Tomcat 6.x before 6.0.44, 7.x before 7.0.58, and 8.x before 8.0.16 does not properly consider the possibility of an accessible interface implemented by an inaccessible class, which allows attackers to bypass a SecurityManager protection mechanism via a web application that leverages use of incorrect privileges during EL evaluation.

### CVE-2014-0099 --> Score: 4.3

Integer overflow in java/org/apache/tomcat/util/buf/Ascii.java in Apache Tomcat before 6.0.40, 7.x before 7.0.53, and 8.x before 8.0.4, when operated behind a reverse proxy, allows remote attackers to conduct HTTP request smuggling attacks via a crafted Content-Length HTTP header.

### CVE-2014-0096 --> Score: 4.3

java/org/apache/catalina/servlets/DefaultServlet.java in the default servlet in Apache Tomcat before 6.0.40, 7.x before 7.0.53, and 8.x before 8.0.4 does not properly restrict XSLT stylesheets, which allows remote attackers to bypass security-manager restrictions and read arbitrary files via a crafted web application that provides an XML external entity declaration in conjunction with an entity reference, related to an XML External Entity (XXE) issue.

### CVE-2016-6816 --> Score: 6.8

The code in Apache Tomcat 9.0.0.M1 to 9.0.0.M11, 8.5.0 to 8.5.6, 8.0.0.RC1 to 8.0.38, 7.0.0 to 7.0.72, and 6.0.0 to 6.0.47 that parsed the HTTP request line permitted invalid characters. This could be exploited, in conjunction with a proxy that also permitted the invalid characters but with a different interpretation, to inject data into the HTTP response. By manipulating the HTTP response the attacker could poison a web-cache, perform an XSS attack and/or obtain sensitive information from requests other then their own.

### CVE-2016-0762 --> Score: 4.3

The Realm implementations in Apache Tomcat versions 9.0.0.M1 to 9.0.0.M9, 8.5.0 to 8.5.4, 8.0.0.RC1 to 8.0.36, 7.0.0 to 7.0.70 and 6.0.0 to 6.0.45 did not process the supplied password if the supplied user name did not exist. This made a timing attack possible to determine valid user names. Note that the default configuration includes the LockOutRealm which makes exploitation of this vulnerability harder.

### CVE-2013-4590 --> Score: 4.3

Apache Tomcat before 6.0.39, 7.x before 7.0.50, and 8.x before 8.0.0-RC10 allows attackers to obtain "Tomcat internals" information by leveraging the presence of an untrusted web application with a context.xml, web.xml, \*.jspx, \*.tagx, or \*.tld XML document containing an external entity declaration in conjunction with an entity reference, related to an XML External Entity (XXE) issue.

### CVE-2016-5388 --> Score: 5.1

Apache Tomcat 7.x through 7.0.70 and 8.x through 8.5.4, when the CGI Servlet is enabled, follows RFC 3875 section 4.1.18 and therefore does not protect applications from the presence of untrusted client data in the HTTP\_PROXY environment variable, which might allow remote attackers to redirect an application's outbound HTTP traffic to an arbitrary proxy server via a crafted Proxy header in an HTTP request, aka an "httpoxy" issue. NOTE: the vendor states "A mitigation is planned for future releases of Tomcat, tracked as CVE-2016-5388"; in other words, this is not a CVE ID for a vulnerability.

### CVE-2016-6794 --> Score: 5.0

When a SecurityManager is configured, a web application's ability to read system properties should be controlled by the SecurityManager. In Apache Tomcat 9.0.0.M1 to 9.0.0.M9, 8.5.0 to 8.5.4, 8.0.0.RC1 to 8.0.36, 7.0.0 to 7.0.70, 6.0.0 to 6.0.45 the system property replacement feature for configuration files could be used by a malicious web application to bypass the SecurityManager and read system properties that should not be visible.

### CVE-2013-4322 --> Score: 4.3

Apache Tomcat before 6.0.39, 7.x before 7.0.50, and 8.x before 8.0.0-RC10 processes chunked transfer coding without properly handling (1) a large total amount of chunked data or (2) whitespace characters in an HTTP header value within a trailer field, which allows remote attackers to cause a denial of service by streaming data. NOTE: this vulnerability exists because of an incomplete fix for CVE-2012-3544.

### CVE-2016-6796 --> Score: 5.0

A malicious web application running on Apache Tomcat 9.0.0.M1 to 9.0.0.M9, 8.5.0 to 8.5.4, 8.0.0.RC1 to 8.0.36, 7.0.0 to 7.0.70 and 6.0.0 to 6.0.45 was able to bypass a configured SecurityManager via manipulation of the configuration parameters for the JSP Servlet.

### CVE-2017-5647 --> Score: 5.0

A bug in the handling of the pipelined requests in Apache Tomcat 9.0.0.M1 to 9.0.0.M18, 8.5.0 to 8.5.12, 8.0.0.RC1 to 8.0.42, 7.0.0 to 7.0.76, and 6.0.0 to 6.0.52, when send file was used, results in the pipelined request being lost when send file processing of the previous request completed. This could result in responses appearing to be sent for the wrong request. For example, a user agent that sent requests A, B and C could see the correct response for request A, the response for request C for request B and no response for request C.

### CVE-2012-5568 --> Score: 5.0

Apache Tomcat through 7.0.x allows remote attackers to cause a denial of service (daemon outage) via partial HTTP requests, as demonstrated by Slowloris.

### CVE-2016-5018 --> Score: 5.0

In Apache Tomcat 9.0.0.M1 to 9.0.0.M9, 8.5.0 to 8.5.4, 8.0.0.RC1 to 8.0.36, 7.0.0 to 7.0.70 and 6.0.0 to 6.0.45 a malicious web application was able to bypass a configured SecurityManager via a Tomcat utility method that was accessible to web applications.

### CVE-2016-6797 --> Score: 5.0

The ResourceLinkFactory implementation in Apache Tomcat 9.0.0.M1 to 9.0.0.M9, 8.5.0 to 8.5.4, 8.0.0.RC1 to 8.0.36, 7.0.0 to 7.0.70 and 6.0.0 to 6.0.45 did not limit web application access to global JNDI resources to those resources explicitly linked to the web application. Therefore, it was possible for a web application to access any global JNDI resource whether an explicit ResourceLink had been configured or not.

### CVE-2016-8735 --> Score: 7.5

Remote code execution is possible with Apache Tomcat before 6.0.48, 7.x before 7.0.73, 8.x before 8.0.39, 8.5.x before 8.5.7, and 9.x before 9.0.0.M12 if JmxRemoteLifecycleListener is used and an attacker can reach JMX ports. The issue exists because this listener wasn't updated for consistency with the CVE-2016-3427 Oracle patch that affected credential types.

### CVE-2013-4286 --> Score: 5.8

Apache Tomcat before 6.0.39, 7.x before 7.0.47, and 8.x before 8.0.0-RC3, when an HTTP connector or AJP connector is used, does not properly handle certain inconsistent HTTP request headers, which allows remote attackers to trigger incorrect identification of a request's length and conduct request-smuggling attacks via (1) multiple Content-Length headers or (2) a Content-Length header and a "Transfer-Encoding: chunked" header. NOTE: this vulnerability exists because of an incomplete fix for CVE-2005-2090.

# Software: notepad++ 1.0

## CVEs from Vulners

No vulnerability found in CPE.

## CVEs from CPE

No vulnerability found in CPE.

# Software: OpenSSH 1.2

## CVEs from Vulners

No vulnerability found in CPE.

## CVEs from CPE

### CVE-2000-0525 --> Score: 10.0

OpenSSH does not properly drop privileges when the UseLogin option is enabled, which allows local users to execute arbitrary commands by providing the command to the ssh daemon.

### CVE-2000-0992 --> Score: 5.0

Directory traversal vulnerability in scp in sshd 1.2.xx allows a remote malicious scp server to overwrite arbitrary files via a .. (dot dot) attack.

### CVE-2000-0143 --> Score: 4.6

The SSH protocol server sshd allows local users without shell access to redirect a TCP connection through a service that uses the standard system password database for authentication, such as POP or FTP.

### CVE-2000-0217 --> Score: 5.1

The default configuration of SSH allows X forwarding, which could allow a remote attacker to control a client's X sessions via a malicious xauth program.

### CVE-2003-1562 --> Score: 7.6

sshd in OpenSSH 3.6.1p2 and earlier, when PermitRootLogin is disabled and using PAM keyboard-interactive authentication, does not insert a delay after a root login attempt with the correct password, which makes it easier for remote attackers to use timing differences to determine if the password step of a multi-step authentication is successful, a different vulnerability than CVE-2003-0190.

### CVE-2011-4327 --> Score: 2.1

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.

### CVE-2010-4478 --> Score: 7.5

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-2006-5052 --> Score: 5.0

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."

### CVE-2008-3259 --> Score: 1.2

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.

### CVE-2008-4109 --> Score: 5.0

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.

### CVE-2007-2243 --> Score: 5.0

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.

### CVE-2012-0814 --> Score: 3.5

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.

### CVE-2011-5000 --> Score: 3.5

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.

### CVE-2006-5051 --> Score: 9.3

Signal handler race condition in OpenSSH before 4.4 allows remote attackers to cause a denial of service (crash), and possibly execute arbitrary code if GSSAPI authentication is enabled, via unspecified vectors that lead to a double-free.

### CVE-2010-5107 --> Score: 5.0

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.

### CVE-2010-4755 --> Score: 4.0

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-2006-4924 --> Score: 7.8

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.

### CVE-2014-1692 --> Score: 7.5

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

### CVE-2017-15906 --> Score: 5.0

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-2016-10708 --> Score: 5.0

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.