Vulnerability Discovery Results

Wednesday 10th July, 2024

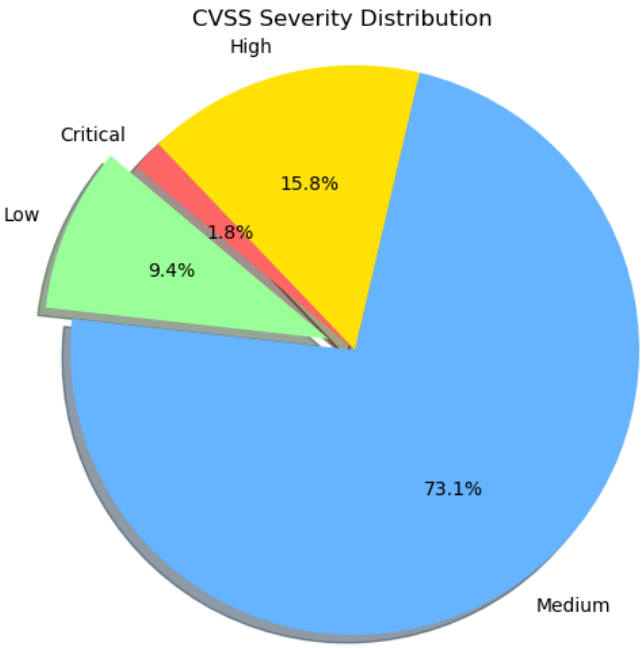
22:47

(UTC+2, PARIS)

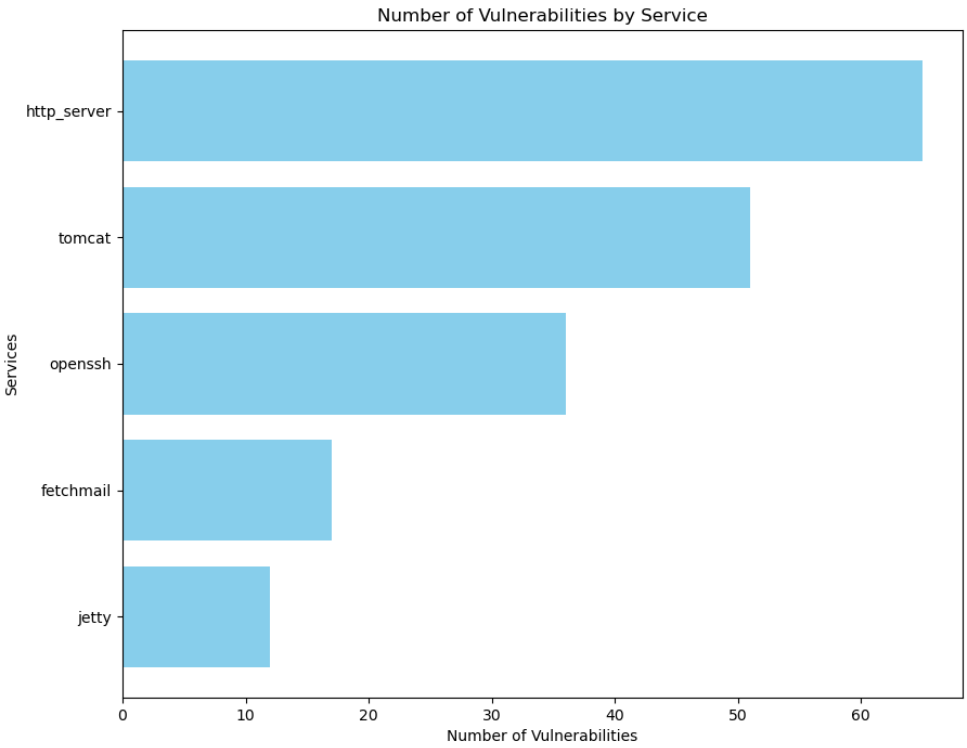
Company Name	First Name	Last Name
Mozilla	**Elise**	**Raff**

Name	OS Name	OS SP
wasp22	**Linux**	**10.04**

CVE	Critical Severity
CVE-2001-0101	10.0
CVE-2001-1009	10.0
CVE-2010-0425	10.0



(a) Figure 1: Pie Chart



(b) Figure 2: Bar Chart

Details

1.1 CVE-2014-0230

!–> CVE for cpe:2.3:a:apache:tomcat:6.0.24:::::*

Summary: 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.

CVSS: 7.8

1.2 CVE-2011-3190

!–> CVE for cpe:2.3:a:apache:tomcat:6.0.24:::::*

Summary: 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.

CVSS: 7.5

1.3 CVE-2013-2185

!–> CVE for cpe:2.3:a:apache:tomcat:6.0.24:::::*

Summary: The readObject method in the DiskFileItem class in Apache Tomcat and JBoss Web, as used in Red Hat JBoss Enterprise Application Platform 6.1.0 and Red Hat JBoss Portal 6.0.0, allows remote attackers to write to arbitrary files via a NULL byte in a file name in a serialized instance, a similar issue to CVE-2013-2186. NOTE: this issue is reportedly disputed by the Apache Tomcat team, although Red Hat considers it a vulnerability. The dispute appears to regard whether it is the responsibility of applications to avoid providing untrusted data to be deserialized, or whether this class should inherently protect against this issue

CVSS: 7.5

1.4 CVE-2016-8735

!–> CVE for cpe:2.3:a:apache:tomcat:6.0.24:::::*

Summary: 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.

CVSS: 7.5

1.5 CVE-2020-8022

!–> CVE for cpe:2.3:a:apache:tomcat:6.0.24:::::*

Summary: A Incorrect Default Permissions vulnerability in the packaging of tomcat on SUSE Enterprise Storage 5, SUSE Linux Enterprise Server 12-SP2-BCL, SUSE Linux

Enterprise Server 12-SP2-LTSS, SUSE Linux Enterprise Server 12-SP3-BCL, SUSE Linux Enterprise Server 12-SP3-LTSS, SUSE Linux Enterprise Server 12-SP4, SUSE Linux Enterprise Server 12-SP5, SUSE Linux Enterprise Server 15-LTSS, SUSE Linux Enterprise Server for SAP 12-SP2, SUSE Linux Enterprise Server for SAP 12-SP3, SUSE Linux Enterprise Server for SAP 15, SUSE OpenStack Cloud 7, SUSE OpenStack Cloud 8, SUSE OpenStack Cloud Crowbar 8 allows local attackers to escalate from group tomcat to root. This issue affects: SUSE Enterprise Storage 5 tomcat versions prior to 8.0.53-29.32.1. SUSE Linux Enterprise Server 12-SP2-BCL tomcat versions prior to 8.0.53-29.32.1. SUSE Linux Enterprise Server 12-SP2-LTSS tomcat versions prior to 8.0.53-29.32.1. SUSE Linux Enterprise Server 12-SP3-BCL tomcat versions prior to 8.0.53-29.32.1. SUSE Linux Enterprise Server 12-SP3-LTSS tomcat versions prior to 8.0.53-29.32.1. SUSE Linux Enterprise Server 12-SP4 tomcat versions prior to 9.0.35-3.39.1. SUSE Linux Enterprise Server 12-SP5 tomcat versions prior to 9.0.35-3.39.1. SUSE Linux Enterprise Server 15-LTSS tomcat versions prior to 9.0.35-3.57.3. SUSE Linux Enterprise Server for SAP 12-SP2 tomcat versions prior to 8.0.53-29.32.1. SUSE Linux Enterprise Server for SAP 12-SP3 tomcat versions prior to 8.0.53-29.32.1. SUSE Linux Enterprise Server for SAP 15 tomcat versions prior to 9.0.35-3.57.3. SUSE OpenStack Cloud 7 tomcat versions prior to 8.0.53-29.32.1. SUSE OpenStack Cloud 8 tomcat versions prior to 8.0.53-29.32.1. SUSE OpenStack Cloud Crowbar 8 tomcat versions prior to 8.0.53-29.32.1.

CVSS: 7.2

1.6 CVE-2013-2067

!–> CVE for cpe:2.3:a:apache:tomcat:6.0.24:::::*

Summary: 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.

CVSS: 6.8

1.7 CVE-2013-4444

!–> CVE for cpe:2.3:a:apache:tomcat:6.0.24:::::*

Summary: Unrestricted file upload vulnerability in Apache Tomcat 7.x before 7.0.40, in certain situations involving outdated java.io.File code and a custom JMX configuration, allows remote attackers to execute arbitrary code by uploading and accessing a JSP file.

CVSS: 6.8

1.8 CVE-2016-6816

!–> CVE for cpe:2.3:a:apache:tomcat:6.0.24:::::*

Summary: 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.

CVSS: 6.8

1.9 CVE-2016-0714

!–> CVE for cpe:2.3:a:apache:tomcat:6.0.24:::::*

Summary: 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.

CVSS: 6.5

1.10 CVE-2010-2227

!–> CVE for cpe:2.3:a:apache:tomcat:6.0.24:::::*

Summary: Apache Tomcat 5.5.0 through 5.5.29, 6.0.0 through 6.0.27, and 7.0.0 beta does not properly handle an invalid Transfer-Encoding header, which allows remote attackers to cause a denial of service (application outage) or obtain sensitive information via a crafted header that interferes with "recycling of a buffer."

CVSS: 6.4

1.11 CVE-2010-4312

!–> CVE for cpe:2.3:a:apache:tomcat:6.0.24:::::*

Summary: The default configuration of Apache Tomcat 6.x does not include the HTTPOnly flag in a Set-Cookie header, which makes it easier for remote attackers to hijack a session via script access to a cookie.

CVSS: 6.4

1.12 CVE-2014-0227

!–> CVE for cpe:2.3:a:apache:tomcat:6.0.24:::::*

Summary: 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.

CVSS: 6.4

1.13 CVE-2016-5018

!–> CVE for cpe:2.3:a:apache:tomcat:6.0.24:::::*

Summary: 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.

CVSS: 6.4

1.14 CVE-2013-4286

!–> CVE for cpe:2.3:a:apache:tomcat:6.0.24:::::*

Summary: 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.

CVSS: 5.8

1.15 CVE-2016-5388

!–> CVE for cpe:2.3:a:apache:tomcat:6.0.24:::::*

Summary: 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.

CVSS: 5.1

1.16 CVE-2011-0534

!–> CVE for cpe:2.3:a:apache:tomcat:6.0.24:::::*

Summary: Apache Tomcat 7.0.0 through 7.0.6 and 6.0.0 through 6.0.30 does not enforce the maxHttpHeaderSize limit for requests involving the NIO HTTP connector, which allows remote attackers to cause a denial of service (OutOfMemoryError) via a crafted request.

CVSS: 5.0

1.17 CVE-2011-4858

!–> CVE for cpe:2.3:a:apache:tomcat:6.0.24:::::*

Summary: 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.

CVSS: 5.0

1.18 CVE-2011-1184

!–> CVE for cpe:2.3:a:apache:tomcat:6.0.24:::::*

Summary: 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.

CVSS: 5.0

1.19 CVE-2011-5062

!–> CVE for cpe:2.3:a:apache:tomcat:6.0.24:::::*

Summary: 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.

CVSS: 5.0

1.20 CVE-2012-0022

!–> CVE for cpe:2.3:a:apache:tomcat:6.0.24:::::*

Summary: 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.

CVSS: 5.0

1.21 CVE-2012-2733

!–> CVE for cpe:2.3:a:apache:tomcat:6.0.24:::::*

Summary: 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.

CVSS: 5.0

1.22 CVE-2012-5885

!–> CVE for cpe:2.3:a:apache:tomcat:6.0.24:::::*

Summary: 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.

CVSS: 5.0

1.23 CVE-2012-5886

!–> CVE for cpe:2.3:a:apache:tomcat:6.0.24:::::*

Summary: 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.

CVSS: 5.0

1.24 CVE-2012-5887

!–> CVE for cpe:2.3:a:apache:tomcat:6.0.24:::::*

Summary: 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.

CVSS: 5.0

1.25 CVE-2012-3544

!–> CVE for cpe:2.3:a:apache:tomcat:6.0.24:::::*

Summary: 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.

CVSS: 5.0

1.26 CVE-2014-0075

!–> CVE for cpe:2.3:a:apache:tomcat:6.0.24:::::*

Summary: 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.

CVSS: 5.0

1.27 CVE-2014-7810

!–> CVE for cpe:2.3:a:apache:tomcat:6.0.24:::::*

Summary: 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.

CVSS: 5.0

1.28 CVE-2015-5345

!–> CVE for cpe:2.3:a:apache:tomcat:6.0.24:::::*

Summary: 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.

CVSS: 5.0

1.29 CVE-2017-5647

!–> CVE for cpe:2.3:a:apache:tomcat:6.0.24:::::*

Summary: 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.

CVSS: 5.0

1.30 CVE-2016-6794

!–> CVE for cpe:2.3:a:apache:tomcat:6.0.24:::::*

Summary: 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.

CVSS: 5.0

1.31 CVE-2016-6797

!–> CVE for cpe:2.3:a:apache:tomcat:6.0.24:::::*

Summary: 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.

CVSS: 5.0

1.32 CVE-2016-6796

!–> CVE for cpe:2.3:a:apache:tomcat:6.0.24:::::*

Summary: 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.

CVSS: 5.0

1.33 CVE-2011-2526

!–> CVE for cpe:2.3:a:apache:tomcat:6.0.24:::::*

Summary: 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.

CVSS: 4.4

1.34 CVE-2010-4172

!–> CVE for cpe:2.3:a:apache:tomcat:6.0.24:::::*

Summary: Multiple cross-site scripting (XSS) vulnerabilities in the Manager application in Apache Tomcat 6.0.12 through 6.0.29 and 7.0.0 through 7.0.4 allow remote attackers to inject arbitrary web script or HTML via the (1) orderBy or (2) sort parameter to sessionsList.jsp, or unspecified input to (3) sessionDetail.jsp or (4) java/org/apache/catalina/manager/JspHelper.java, related to use of untrusted web applications.

CVSS: 4.3

1.35 CVE-2011-0013

!–> CVE for cpe:2.3:a:apache:tomcat:6.0.24:::::*

Summary: Multiple cross-site scripting (XSS) vulnerabilities in the HTML Manager Interface in Apache Tomcat 5.5 before 5.5.32, 6.0 before 6.0.30, and 7.0 before 7.0.6 allow remote attackers to inject arbitrary web script or HTML, as demonstrated via the display-name tag.

CVSS: 4.3

1.36 CVE-2011-5063

!–> CVE for cpe:2.3:a:apache:tomcat:6.0.24:::::*

Summary: 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.

CVSS: 4.3

1.37 CVE-2011-5064

!–> CVE for cpe:2.3:a:apache:tomcat:6.0.24:::::*

Summary: 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.

CVSS: 4.3

1.38 CVE-2012-3546

!–> CVE for cpe:2.3:a:apache:tomcat:6.0.24:::::*

Summary: 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.

CVSS: 4.3

1.39 CVE-2012-4431

!–> CVE for cpe:2.3:a:apache:tomcat:6.0.24:::::*

Summary: 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.

CVSS: 4.3

1.40 CVE-2013-4322

!–> CVE for cpe:2.3:a:apache:tomcat:6.0.24:::::*

Summary: 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.

CVSS: 4.3

1.41 CVE-2013-4590

!–> CVE for cpe:2.3:a:apache:tomcat:6.0.24:::::*

Summary: 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.

CVSS: 4.3

1.42 CVE-2014-0096

!–> CVE for cpe:2.3:a:apache:tomcat:6.0.24:::::*

Summary: 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.

CVSS: 4.3

1.43 CVE-2014-0099

!–> CVE for cpe:2.3:a:apache:tomcat:6.0.24:::::*

Summary: 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.

CVSS: 4.3

1.44 CVE-2014-0119

!–> CVE for cpe:2.3:a:apache:tomcat:6.0.24:::::*

Summary: 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.

CVSS: 4.3

1.45 CVE-2016-0762

!–> CVE for cpe:2.3:a:apache:tomcat:6.0.24:::::*

Summary: 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.

CVSS: 4.3

1.46 CVE-2015-5174

!–> CVE for cpe:2.3:a:apache:tomcat:6.0.24:::::*

Summary: 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.

CVSS: 4.0

1.47 CVE-2016-0706

!–> CVE for cpe:2.3:a:apache:tomcat:6.0.24:::::*

Summary: 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.

CVSS: 4.0

1.48 CVE-2010-1157

!–> CVE for cpe:2.3:a:apache:tomcat:6.0.24:::::*

Summary: Apache Tomcat 5.5.0 through 5.5.29 and 6.0.0 through 6.0.26 might allow remote attackers to discover the server's hostname or IP address by sending a request for a resource that requires (1) BASIC or (2) DIGEST authentication, and then reading the realm field in the WWW-Authenticate header in the reply.

CVSS: 2.6

1.49 CVE-2012-4534

!–> CVE for cpe:2.3:a:apache:tomcat:6.0.24:::::*

Summary: 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.

CVSS: 2.6

1.50 CVE-2011-2204

!–> CVE for cpe:2.3:a:apache:tomcat:6.0.24:::::*

Summary: 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.

CVSS: 1.9

1.51 CVE-2010-3718

!–> CVE for cpe:2.3:a:apache:tomcat:6.0.24:::::*

Summary: Apache Tomcat 7.0.0 through 7.0.3, 6.0.x, and 5.5.x, when running within a SecurityManager, does not make the ServletContext attribute read-only, which allows local web applications to read or write files outside of the intended working directory, as demonstrated using a directory traversal attack.

CVSS: 1.2

1.52 CVE-2017-7657

!–> CVE for cpe:2.3:a:eclipse:jetty:6.1.25:::::*

Summary: In Eclipse Jetty, versions 9.2.x and older, 9.3.x (all configurations), and 9.4.x (non-default configuration with RFC2616 compliance enabled), transfer-encoding chunks are handled poorly. The chunk length parsing was vulnerable to an integer overflow. Thus a large chunk size could be interpreted as a smaller chunk size and content sent as chunk body could be interpreted as a pipelined request. If Jetty was deployed

behind an intermediary that imposed some authorization and that intermediary allowed arbitrarily large chunks to be passed on unchanged, then this flaw could be used to bypass the authorization imposed by the intermediary as the fake pipelined request would not be interpreted by the intermediary as a request.

CVSS: 7.5

1.53 CVE-2017-7658

!–> CVE for cpe:2.3:a:eclipse:jetty:6.1.25:::::*

Summary: In Eclipse Jetty Server, versions 9.2.x and older, 9.3.x (all non HTTP/1.x configurations), and 9.4.x (all HTTP/1.x configurations), when presented with two content-lengths headers, Jetty ignored the second. When presented with a content-length and a chunked encoding header, the content-length was ignored (as per RFC 2616). If an intermediary decided on the shorter length, but still passed on the longer body, then body content could be interpreted by Jetty as a pipelined request. If the intermediary was imposing authorization, the fake pipelined request would bypass that authorization.

CVSS: 7.5

1.54 CVE-2017-9735

!–> CVE for cpe:2.3:a:eclipse:jetty:6.1.25:::::*

Summary: Jetty through 9.4.x is prone to a timing channel in util/security/Password.java, which makes it easier for remote attackers to obtain access by observing elapsed times before rejection of incorrect passwords.

CVSS: 5.0

1.55 CVE-2017-7656

!–> CVE for cpe:2.3:a:eclipse:jetty:6.1.25:::::*

Summary: In Eclipse Jetty, versions 9.2.x and older, 9.3.x (all configurations), and 9.4.x (non-default configuration with RFC2616 compliance enabled), HTTP/0.9 is handled poorly. An HTTP/1 style request line (i.e. method space URI space version) that declares a version of HTTP/0.9 was accepted and treated as a 0.9 request. If deployed behind an intermediary that also accepted and passed through the 0.9 version (but did not act on it), then the response sent could be interpreted by the intermediary as HTTP/1 headers. This could be used to poison the cache if the server allowed the origin client to generate arbitrary content in the response.

CVSS: 5.0

1.56 CVE-2021-28169

!–> CVE for cpe:2.3:a:eclipse:jetty:6.1.25:::::*

Summary: For Eclipse Jetty versions <= 9.4.40, <= 10.0.2, <= 11.0.2, it is possible for requests to the ConcatServlet with a doubly encoded path to access protected resources within the WEB-INF directory. For example a request to `/concat?/%2557EB-INF/web.xml` can retrieve the web.xml file. This can reveal sensitive information regarding the implementation of a web application.

CVSS: 5.0

1.57 CVE-2022-2048

!–> CVE for cpe:2.3:a:eclipse:jetty:6.1.25:::::*

Summary: In Eclipse Jetty HTTP/2 server implementation, when encountering an invalid HTTP/2 request, the error handling has a bug that can wind up not properly cleaning up the active connections and associated resources. This can lead to a Denial of Service scenario where there are no enough resources left to process good requests.

CVSS: 5.0

1.58 CVE-2020-27216

!–> CVE for cpe:2.3:a:eclipse:jetty:6.1.25:::::*

Summary: In Eclipse Jetty versions 1.0 thru 9.4.32.v20200930, 10.0.0.alpha1 thru 10.0.0.beta2, and 11.0.0.alpha1 thru 11.0.0.beta2O, on Unix like systems, the system's temporary directory is shared between all users on that system. A collocated user can observe the process of creating a temporary sub directory in the shared temporary directory and race to complete the creation of the temporary subdirectory. If the attacker wins the race then they will have read and write permission to the subdirectory used to unpack web applications, including their WEB-INF/lib jar files and JSP files. If any code is ever executed out of this temporary directory, this can lead to a local privilege escalation vulnerability.

CVSS: 4.4

1.59 CVE-2022-2047

!–> CVE for cpe:2.3:a:eclipse:jetty:6.1.25:::::*

Summary: In Eclipse Jetty versions 9.4.0 thru 9.4.46, and 10.0.0 thru 10.0.9, and 11.0.0 thru 11.0.9 versions, the parsing of the authority segment of an http scheme URI, the Jetty HttpURI class improperly detects an invalid input as a hostname. This can lead to failures in a Proxy scenario.

CVSS: 4.0

1.60 CVE-2021-34428

!–> CVE for cpe:2.3:a:eclipse:jetty:6.1.25:::::*

Summary: For Eclipse Jetty versions <= 9.4.40, <= 10.0.2, <= 11.0.2, if an exception is thrown from the SessionListener#sessionDestroyed() method, then the session ID is not invalidated in the session ID manager. On deployments with clustered sessions and multiple contexts this can result in a session not being invalidated. This can result in an application used on a shared computer being left logged in.

CVSS: 3.6

1.61 CVE-2023-26048

!–> CVE for cpe:2.3:a:eclipse:jetty:6.1.25:::::*

Summary: Jetty is a java based web server and servlet engine. In affected versions servlets with multipart support (e.g. annotated with `@MultipartConfig`) that call `HttpServletRequest.getParameter()` or `HttpServletRequest.getParts()` may cause `OutOfMemoryError` when the client sends a multipart request with a part that

has a name but no filename and very large content. This happens even with the default settings of `fileSizeThreshold=0` which should stream the whole part content to disk. An attacker client may send a large multipart request and cause the server to throw `OutOfMemoryError`. However, the server may be able to recover after the `OutOfMemoryError` and continue its service – although it may take some time. This issue has been patched in versions 9.4.51, 10.0.14, and 11.0.14. Users are advised to upgrade. Users unable to upgrade may set the multipart parameter `maxRequestSize` which must be set to a non-negative value, so the whole multipart content is limited (although still read into memory).

CVSS: N/A

1.62 CVE-2023-26049

!–> CVE for cpe:2.3:a:eclipse:jetty:6.1.25:::::::*

Summary: Jetty is a java based web server and servlet engine. Nonstandard cookie parsing in Jetty may allow an attacker to smuggle cookies within other cookies, or otherwise perform unintended behavior by tampering with the cookie parsing mechanism. If Jetty sees a cookie VALUE that starts with `"` (double quote), it will continue to read the cookie string until it sees a closing quote – even if a semicolon is encountered. So, a cookie header such as: `DISPLAY_LANGUAGE="b; JSESSIONID=1337; c=d"` will be parsed as one cookie, with the name DISPLAY_LANGUAGE and a value of b; JSESSIONID=1337; c=d instead of 3 separate cookies. This has security implications because if, say, JSESSIONID is an HttpOnly cookie, and the DISPLAY_LANGUAGE cookie value is rendered on the page, an attacker can smuggle the JSESSIONID cookie into the DISPLAY_LANGUAGE cookie and thereby exfiltrate it. This is significant when an intermediary is enacting some policy based on cookies, so a smuggled cookie can bypass that policy yet still be seen by the Jetty server or its logging system. This issue has been addressed in versions 9.4.51, 10.0.14, 11.0.14, and 12.0.0.beta0 and users are advised to upgrade. There are no known workarounds for this issue.

CVSS: N/A

1.63 CVE-2023-44487

!–> CVE for cpe:2.3:a:eclipse:jetty:6.1.25:::::::*

Summary: The HTTP/2 protocol allows a denial of service (server resource consumption) because request cancellation can reset many streams quickly, as exploited in the wild in August through October 2023.

CVSS: N/A

1.64 CVE-2001-0101

!–> CVE for cpe:2.3:a:fetchmail:fetchmail:4.6.0:::::::*

Summary: Vulnerability in fetchmail 5.5.0-2 and earlier in the AUTHENTICATE GSSAPI command.

CVSS: 10.0

1.65 CVE-2001-1009

!–> CVE for cpe:2.3:a:fetchmail:fetchmail:4.6.0:::::::*

Summary: Fetchmail (aka fetchmail-ssl) before 5.8.17 allows a remote malicious (1) IMAP server or (2) POP/POP3 server to overwrite arbitrary memory and possibly gain privileges via a negative index number as part of a response to a LIST request.

CVSS: 10.0

1.66 CVE-2006-5867

!–> CVE for cpe:2.3:a:fetchmail:fetchmail:4.6.0:::::*

Summary: fetchmail before 6.3.6-rc4 does not properly enforce TLS and may transmit cleartext passwords over unsecured links if certain circumstances occur, which allows remote attackers to obtain sensitive information via man-in-the-middle (MITM) attacks.

CVSS: 7.8

1.67 CVE-2001-0819

!–> CVE for cpe:2.3:a:fetchmail:fetchmail:4.6.0:::::*

Summary: A buffer overflow in Linux fetchmail before 5.8.6 allows remote attackers to execute arbitrary code via a large 'To:' field in an email header.

CVSS: 7.5

1.68 CVE-2002-1174

!–> CVE for cpe:2.3:a:fetchmail:fetchmail:4.6.0:::::*

Summary: Buffer overflows in Fetchmail 6.0.0 and earlier allow remote attackers to cause a denial of service (crash) or execute arbitrary code via (1) long headers that are not properly processed by the readheaders function, or (2) via long Received: headers, which are not properly parsed by the parse_received function.

CVSS: 7.5

1.69 CVE-2002-1365

!–> CVE for cpe:2.3:a:fetchmail:fetchmail:4.6.0:::::*

Summary: Heap-based buffer overflow in Fetchmail 6.1.3 and earlier does not account for the "@" character when determining buffer lengths for local addresses, which allows remote attackers to execute arbitrary code via a header with a large number of local addresses.

CVSS: 7.5

1.70 CVE-2009-2666

!–> CVE for cpe:2.3:a:fetchmail:fetchmail:4.6.0:::::*

Summary: socket.c in fetchmail before 6.3.11 does not properly handle a '\0' character in a domain name in the subject's Common Name (CN) field of an X.509 certificate, which allows man-in-the-middle attackers to spoof arbitrary SSL servers via a crafted certificate issued by a legitimate Certification Authority, a related issue to CVE-2009-2408.

CVSS: 6.4

1.71 CVE-2002-0146

!–> CVE for cpe:2.3:a:fetchmail:fetchmail:4.6.0:::::*

Summary: fetchmail email client before 5.9.10 does not properly limit the maximum number of messages available, which allows a remote IMAP server to overwrite memory via a message count that exceeds the boundaries of an array.

CVSS: 5.0

1.72 CVE-2002-1175

!–> CVE for cpe:2.3:a:fetchmail:fetchmail:4.6.0:::::*

Summary: The getmxrecord function in Fetchmail 6.0.0 and earlier does not properly check the boundary of a particular malformed DNS packet from a malicious DNS server, which allows remote attackers to cause a denial of service (crash) when Fetchmail attempts to read data beyond the expected boundary.

CVSS: 5.0

1.73 CVE-2003-0792

!–> CVE for cpe:2.3:a:fetchmail:fetchmail:4.6.0:::::*

Summary: Fetchmail 6.2.4 and earlier does not properly allocate memory for long lines, which allows remote attackers to cause a denial of service (crash) via a certain email.

CVSS: 5.0

1.74 CVE-2005-2335

!–> CVE for cpe:2.3:a:fetchmail:fetchmail:4.6.0:::::*

Summary: Buffer overflow in the POP3 client in Fetchmail before 6.2.5.2 allows remote POP3 servers to cause a denial of service and possibly execute arbitrary code via long UIDL responses. NOTE: a typo in an advisory accidentally used the wrong CVE identifier for the Fetchmail issue. This is the correct identifier.

CVSS: 5.0

1.75 CVE-2007-4565

!–> CVE for cpe:2.3:a:fetchmail:fetchmail:4.6.0:::::*

Summary: sink.c in fetchmail before 6.3.9 allows context-dependent attackers to cause a denial of service (NULL dereference and application crash) by refusing certain warning messages that are sent over SMTP.

CVSS: 5.0

1.76 CVE-2021-36386

!–> CVE for cpe:2.3:a:fetchmail:fetchmail:4.6.0:::::*

Summary: report_vbuild in report.c in Fetchmail before 6.4.20 sometimes omits initialization of the vsnprintf va_list argument, which might allow mail servers to cause a denial of service or possibly have unspecified other impact via long error messages.

NOTE: it is unclear whether use of Fetchmail on any realistic platform results in an impact beyond an inconvenience to the client user.

CVSS: 5.0

1.77 CVE-2008-2711

!–> CVE for cpe:2.3:a:fetchmail:fetchmail:4.6.0:::::*

Summary: fetchmail 6.3.8 and earlier, when running in -v -v (aka verbose) mode, allows remote attackers to cause a denial of service (crash and persistent mail failure) via a malformed mail message with long headers, which triggers an erroneous dereference when using vsnprintf to format log messages.

CVSS: 4.3

1.78 CVE-2010-1167

!–> CVE for cpe:2.3:a:fetchmail:fetchmail:4.6.0:::::*

Summary: fetchmail 4.6.3 through 6.3.16, when debug mode is enabled, does not properly handle invalid characters in a multi-character locale, which allows remote attackers to cause a denial of service (memory consumption and application crash) via a crafted (1) message header or (2) POP3 UIDL list.

CVSS: 4.3

1.79 CVE-2021-39272

!–> CVE for cpe:2.3:a:fetchmail:fetchmail:4.6.0:::::*

Summary: Fetchmail before 6.4.22 fails to enforce STARTTLS session encryption in some circumstances, such as a certain situation with IMAP and PREAUTH.

CVSS: 4.3

1.80 CVE-2001-1378

!–> CVE for cpe:2.3:a:fetchmail:fetchmail:4.6.0:::::*

Summary: fetchmailconf in fetchmail before 5.7.4 allows local users to overwrite files of other users via a symlink attack on temporary files.

CVSS: 2.1

1.81 CVE-2010-0425

!–> CVE for cpe:2.3:a:apache:http_server:2.2.14:::::*

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.”

CVSS: 10.0

1.82 CVE-2011-3192

!–> CVE for cpe:2.3:a:apache:http_server:2.2.14:::::*

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: 7.8

1.83 CVE-2017-3167

!–> CVE for cpe:2.3:a:apache:http_server:2.2.14:::::*

Summary: In Apache httpd 2.2.x before 2.2.33 and 2.4.x before 2.4.26, use of the ap_get_basic_auth_pw() by third-party modules outside of the authentication phase may lead to authentication requirements being bypassed.

CVSS: 7.5

1.84 CVE-2017-3169

!–> CVE for cpe:2.3:a:apache:http_server:2.2.14:::::*

Summary: In Apache httpd 2.2.x before 2.2.33 and 2.4.x before 2.4.26, mod_ssl may dereference a NULL pointer when third-party modules call ap_hook_process_connection() during an HTTP request to an HTTPS port.

CVSS: 7.5

1.85 CVE-2017-7679

!–> CVE for cpe:2.3:a:apache:http_server:2.2.14:::::*

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.

CVSS: 7.5

1.86 CVE-2021-39275

!–> CVE for cpe:2.3:a:apache:http_server:2.2.14:::::*

Summary: ap_escape_quotes() may write beyond the end of a buffer when given malicious input. No included modules pass untrusted data to these functions, but third-party / external modules may. This issue affects Apache HTTP Server 2.4.48 and earlier.

CVSS: 7.5

1.87 CVE-2021-44790

!–> CVE for cpe:2.3:a:apache:http_server:2.2.14:::::*

Summary: A carefully crafted request body can cause a buffer overflow in the mod_lua multipart parser (r:parsebody() called from Lua scripts). The Apache httpd team is not aware of an exploit for the vulnerabilty though it might be possible to craft one. This issue affects Apache HTTP Server 2.4.51 and earlier.

CVSS: 7.5

1.88 CVE-2022-22720

!–> CVE for cpe:2.3:a:apache:http_server:2.2.14:::::*

Summary: Apache HTTP Server 2.4.52 and earlier fails to close inbound connection when errors are encountered discarding the request body, exposing the server to HTTP Request Smuggling

CVSS: 7.5

1.89 CVE-2022-31813

!–> CVE for cpe:2.3:a:apache:http_server:2.2.14:::::*

Summary: Apache HTTP Server 2.4.53 and earlier may not send the X-Forwarded-* headers to the origin server based on client side Connection header hop-by-hop mechanism. This may be used to bypass IP based authentication on the origin server/application.

CVSS: 7.5

1.90 CVE-2012-0883

!–> CVE for cpe:2.3:a:apache:http_server:2.2.14:::::*

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.

CVSS: 6.9

1.91 CVE-2014-0226

!–> CVE for cpe:2.3:a:apache:http_server:2.2.14:::::*

Summary: Race condition in the mod_status module in the Apache HTTP Server before 2.4.10 allows remote attackers to cause a denial of service (heap-based buffer overflow), or possibly obtain sensitive credential information or execute arbitrary code, via a crafted request that triggers improper scoreboard handling within the status_handler function in modules/generators/mod_status.c and the lua_ap_scoreboard_worker function in modules/lua/lua_request.c.

CVSS: 6.8

1.92 CVE-2016-5387

!–> CVE for cpe:2.3:a:apache:http_server:2.2.14:::::*

Summary: The Apache HTTP Server through 2.4.23 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 "This

mitigation has been assigned the identifier CVE-2016-5387"; in other words, this is not a CVE ID for a vulnerability.

CVSS: 6.8

1.93 CVE-2021-40438

!–> CVE for cpe:2.3:a:apache:http_server:2.2.14:::::*

Summary: A crafted request uri-path can cause mod_proxy to forward the request to an origin server choosen by the remote user. This issue affects Apache HTTP Server 2.4.48 and earlier.

CVSS: 6.8

1.94 CVE-2017-9788

!–> CVE for cpe:2.3:a:apache:http_server:2.2.14:::::*

Summary: In Apache httpd before 2.2.34 and 2.4.x before 2.4.27, the value placeholder in [Proxy-]Authorization headers of type 'Digest' was not initialized or reset before or between successive key=value assignments by mod_auth_digest. Providing an initial key with no '=' assignment could reflect the stale value of uninitialized pool memory used by the prior request, leading to leakage of potentially confidential information, and a segfault in other cases resulting in denial of service.

CVSS: 6.4

1.95 CVE-2022-28615

!–> CVE for cpe:2.3:a:apache:http_server:2.2.14:::::*

Summary: Apache HTTP Server 2.4.53 and earlier may crash or disclose information due to a read beyond bounds in ap_strcmp_match() when provided with an extremely large input buffer. While no code distributed with the server can be coerced into such a call, third-party modules or lua scripts that use ap_strcmp_match() may hypothetically be affected.

CVSS: 6.4

1.96 CVE-2009-3555

!–> CVE for cpe:2.3:a:apache:http_server:2.2.14:::::*

Summary: The TLS protocol, and the SSL protocol 3.0 and possibly earlier, as used in Microsoft Internet Information Services (IIS) 7.0, mod_ssl in the Apache HTTP Server 2.2.14 and earlier, OpenSSL before 0.9.8l, GnuTLS 2.8.5 and earlier, Mozilla Network Security Services (NSS) 3.12.4 and earlier, multiple Cisco products, and other products, does not properly associate renegotiation handshakes with an existing connection, which allows man-in-the-middle attackers to insert data into HTTPS sessions, and possibly other types of sessions protected by TLS or SSL, by sending an unauthenticated request that is processed retroactively by a server in a post-renegotiation context, related to a "plaintext injection" attack, aka the "Project Mogul" issue.

CVSS: 5.8

1.97 CVE-2022-22721

!–> CVE for cpe:2.3:a:apache:http_server:2.2.14:::::::*

Summary: If LimitXMLRequestBody is set to allow request bodies larger than 350MB (defaults to 1M) on 32 bit systems an integer overflow happens which later causes out of bounds writes. This issue affects Apache HTTP Server 2.4.52 and earlier.

CVSS: 5.8

1.98 CVE-2013-1862

!–> CVE for cpe:2.3:a:apache:http_server:2.2.14:::::::*

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: 5.1

1.99 CVE-2009-3720

!–> CVE for cpe:2.3:a:apache:http_server:2.2.14:::::::*

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: 5.0

1.100 CVE-2009-3560

!–> CVE for cpe:2.3:a:apache:http_server:2.2.14:::::::*

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: 5.0

1.101 CVE-2010-0408

!–> CVE for cpe:2.3:a:apache:http_server:2.2.14:::::::*

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.

CVSS: 5.0

1.102 CVE-2010-2068

!–> CVE for cpe:2.3:a:apache:http_server:2.2.14:::::*

Summary: mod_proxy_http.c in mod_proxy_http in the Apache HTTP Server 2.2.9 through 2.2.15, 2.3.4-alpha, and 2.3.5-alpha on Windows, NetWare, and OS/2, in certain configurations involving proxy worker pools, does not properly detect timeouts, which allows remote attackers to obtain a potentially sensitive response intended for a different client in opportunistic circumstances via a normal HTTP request.

CVSS: 5.0

1.103 CVE-2010-1452

!–> CVE for cpe:2.3:a:apache:http_server:2.2.14:::::*

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: 5.0

1.104 CVE-2010-1623

!–> CVE for cpe:2.3:a:apache:http_server:2.2.14:::::*

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: 5.0

1.105 CVE-2011-3368

!–> CVE for cpe:2.3:a:apache:http_server:2.2.14:::::*

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: 5.0

1.106 CVE-2007-6750

!–> CVE for cpe:2.3:a:apache:http_server:2.2.14:::::*

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: 5.0

1.107 CVE-2012-4557

!–> CVE for cpe:2.3:a:apache:http_server:2.2.14:::::*

Summary: The mod_proxy_ajp module in the Apache HTTP Server 2.2.12 through 2.2.21 places a worker node into an error state upon detection of a long request-processing time, which allows remote attackers to cause a denial of service (worker consumption) via an expensive request.

CVSS: 5.0

1.108 CVE-2013-6438

!–> CVE for cpe:2.3:a:apache:http_server:2.2.14:::::*

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.

CVSS: 5.0

1.109 CVE-2014-0098

!–> CVE for cpe:2.3:a:apache:http_server:2.2.14:::::*

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.

CVSS: 5.0

1.110 CVE-2013-5704

!–> CVE for cpe:2.3:a:apache:http_server:2.2.14:::::*

Summary: The mod_headers module in the Apache HTTP Server 2.2.22 allows remote attackers to bypass "RequestHeader unset" directives by placing a header in the trailer portion of data sent with chunked transfer coding. NOTE: the vendor states "this is not a security issue in httpd as such."

CVSS: 5.0

1.111 CVE-2014-0231

!–> CVE for cpe:2.3:a:apache:http_server:2.2.14:::::*

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.

CVSS: 5.0

1.112 CVE-2015-0228

!–> CVE for cpe:2.3:a:apache:http_server:2.2.14:::::*

Summary: The lua_websocket_read function in lua_request.c in the mod_lua module in the Apache HTTP Server through 2.4.12 allows remote attackers to cause a denial of service (child-process crash) by sending a crafted WebSocket Ping frame after a Lua script has called the wsupgrade function.

CVSS: 5.0

1.113 CVE-2015-3183

!–> CVE for cpe:2.3:a:apache:http_server:2.2.14:::::*

Summary: The chunked transfer coding implementation in the Apache HTTP Server before 2.4.14 does not properly parse chunk headers, which allows remote attackers to conduct HTTP request smuggling attacks via a crafted request, related to mishandling of large chunk-size values and invalid chunk-extension characters in modules/http/http_filters.c.

CVSS: 5.0

1.114 CVE-2016-8743

!–> CVE for cpe:2.3:a:apache:http_server:2.2.14:::::*

Summary: Apache HTTP Server, in all releases prior to 2.2.32 and 2.4.25, was liberal in the whitespace accepted from requests and sent in response lines and headers. Accepting these different behaviors represented a security concern when httpd participates in any chain of proxies or interacts with back-end application servers, either through mod_proxy or using conventional CGI mechanisms, and may result in request smuggling, response splitting and cache pollution.

CVSS: 5.0

1.115 CVE-2017-9798

!–> CVE for cpe:2.3:a:apache:http_server:2.2.14:::::*

Summary: Apache httpd allows remote attackers to read secret data from process memory if the Limit directive can be set in a user's .htaccess file, or if httpd.conf has certain misconfigurations, aka Optionsbleed. This affects the Apache HTTP Server through 2.2.34 and 2.4.x through 2.4.27. The attacker sends an unauthenticated OPTIONS HTTP request when attempting to read secret data. This is a use-after-free issue and thus secret data is not always sent, and the specific data depends on many factors including configuration. Exploitation with .htaccess can be blocked with a patch to the ap_limit_section function in server/core.c.

CVSS: 5.0

1.116 CVE-2018-1303

!–> CVE for cpe:2.3:a:apache:http_server:2.2.14:::::*

Summary: A specially crafted HTTP request header could have crashed the Apache HTTP Server prior to version 2.4.30 due to an out of bound read while preparing data to be cached in shared memory. It could be used as a Denial of Service attack against users of mod_cache_socache. The vulnerability is considered as low risk since mod_cache_socache is not widely used, mod_cache_disk is not concerned by this vulnerability.

CVSS: 5.0

1.117 CVE-2021-34798

!–> CVE for cpe:2.3:a:apache:http_server:2.2.14:::::*

Summary: Malformed requests may cause the server to dereference a NULL pointer. This issue affects Apache HTTP Server 2.4.48 and earlier.

CVSS: 5.0

1.118 CVE-2022-22719

!–> CVE for cpe:2.3:a:apache:http_server:2.2.14:::::*

Summary: A carefully crafted request body can cause a read to a random memory area which could cause the process to crash. This issue affects Apache HTTP Server 2.4.52 and earlier.

CVSS: 5.0

1.119 CVE-2022-28330

!–> CVE for cpe:2.3:a:apache:http_server:2.2.14:::::*

Summary: Apache HTTP Server 2.4.53 and earlier on Windows may read beyond bounds when configured to process requests with the mod_isapi module.

CVSS: 5.0

1.120 CVE-2022-28614

!–> CVE for cpe:2.3:a:apache:http_server:2.2.14:::::*

Summary: The ap_rwrite() function in Apache HTTP Server 2.4.53 and earlier may read unintended memory if an attacker can cause the server to reflect very large input using ap_rwrite() or ap_rputs(), such as with mod_luas r:puts() function. Modules compiled and distributed separately from Apache HTTP Server that use the 'ap_rputs' function and may pass it a very large (INT_MAX or larger) string must be compiled against current headers to resolve the issue.

CVSS: 5.0

1.121 CVE-2022-29404

!–> CVE for cpe:2.3:a:apache:http_server:2.2.14:::::*

Summary: In Apache HTTP Server 2.4.53 and earlier, a malicious request to a lua script that calls r:parsebody(0) may cause a denial of service due to no default limit on possible input size.

CVSS: 5.0

1.122 CVE-2022-30556

!–> CVE for cpe:2.3:a:apache:http_server:2.2.14:::::*

Summary: Apache HTTP Server 2.4.53 and earlier may return lengths to applications calling r:wsread() that point past the end of the storage allocated for the buffer.

CVSS: 5.0

1.123 CVE-2012-0031

!–> CVE for cpe:2.3:a:apache:http_server:2.2.14:::::::*

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: 4.6

1.124 CVE-2011-3607

!–> CVE for cpe:2.3:a:apache:http_server:2.2.14:::::::*

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: 4.4

1.125 CVE-2008-0455

!–> CVE for cpe:2.3:a:apache:http_server:2.2.14:::::::*

Summary: Cross-site scripting (XSS) vulnerability in the mod_negotiation module in the Apache HTTP Server 2.2.6 and earlier in the 2.2.x series, 2.0.61 and earlier in the 2.0.x series, and 1.3.39 and earlier in the 1.3.x series allows remote authenticated users to inject arbitrary web script or HTML by uploading a file with a name containing XSS sequences and a file extension, which leads to injection within a (1) “406 Not Acceptable” or (2) “300 Multiple Choices” HTTP response when the extension is omitted in a request for the file.

CVSS: 4.3

1.126 CVE-2010-0434

!–> CVE for cpe:2.3:a:apache:http_server:2.2.14:::::::*

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: 4.3

1.127 CVE-2011-0419

!–> CVE for cpe:2.3:a:apache:http_server:2.2.14:::::::*

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.

CVSS: 4.3

1.128 CVE-2011-3348

!–> CVE for cpe:2.3:a:apache:http_server:2.2.14:::::*

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.

CVSS: 4.3

1.129 CVE-2011-3639

!–> CVE for cpe:2.3:a:apache:http_server:2.2.14:::::*

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: 4.3

1.130 CVE-2011-4317

!–> CVE for cpe:2.3:a:apache:http_server:2.2.14:::::*

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: 4.3

1.131 CVE-2012-0053

!–> CVE for cpe:2.3:a:apache:http_server:2.2.14:::::*

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: 4.3

1.132 CVE-2012-3499

!–> CVE for cpe:2.3:a:apache:http_server:2.2.14:::::*

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.

CVSS: 4.3

1.133 CVE-2012-4558

!–> CVE for cpe:2.3:a:apache:http_server:2.2.14:::::*

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.

CVSS: 4.3

1.134 CVE-2013-1896

!–> CVE for cpe:2.3:a:apache:http_server:2.2.14:::::*

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.

CVSS: 4.3

1.135 CVE-2014-0118

!–> CVE for cpe:2.3:a:apache:http_server:2.2.14:::::*

Summary: The deflate_in_filter function in mod_deflate.c in the mod_deflate module in the Apache HTTP Server before 2.4.10, when request body decompression is enabled, allows remote attackers to cause a denial of service (resource consumption) via crafted request data that decompresses to a much larger size.

CVSS: 4.3

1.136 CVE-2018-1301

!–> CVE for cpe:2.3:a:apache:http_server:2.2.14:::::*

Summary: A specially crafted request could have crashed the Apache HTTP Server prior to version 2.4.30, due to an out of bound access after a size limit is reached by reading the HTTP header. This vulnerability is considered very hard if not impossible to trigger in non-debug mode (both log and build level), so it is classified as low risk for common server usage.

CVSS: 4.3

1.137 CVE-2018-1302

!–> CVE for cpe:2.3:a:apache:http_server:2.2.14:::::*

Summary: When an HTTP/2 stream was destroyed after being handled, the Apache HTTP Server prior to version 2.4.30 could have written a NULL pointer potentially to an already freed memory. The memory pools maintained by the server make this vulnerability hard to trigger in usual configurations, the reporter and the team could not reproduce it outside debug builds, so it is classified as low risk.

CVSS: 4.3

1.138 CVE-2016-4975

!–> CVE for cpe:2.3:a:apache:http_server:2.2.14:::::*

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).

CVSS: 4.3

1.139 CVE-2016-8612

!–> CVE for cpe:2.3:a:apache:http_server:2.2.14:::::*

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: 3.3

1.140 CVE-2012-2687

!–> CVE for cpe:2.3:a:apache:http_server:2.2.14:::::*

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.

CVSS: 2.6

1.141 CVE-2011-4415

!–> CVE for cpe:2.3:a:apache:http_server:2.2.14:::::*

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: 1.2

1.142 CVE-2006-20001

!–> CVE for cpe:2.3:a:apache:http_server:2.2.14:::::*

Summary: A carefully crafted If: request header can cause a memory read, or write of a single zero byte, in a pool (heap) memory location beyond the header value sent. This could cause the process to crash.

This issue affects Apache HTTP Server 2.4.54 and earlier.

CVSS: N/A

1.143 CVE-2022-37436

!–> CVE for cpe:2.3:a:apache:http_server:2.2.14:::::*

Summary: Prior to Apache HTTP Server 2.4.55, a malicious backend can cause the response headers to be truncated early, resulting in some headers being incorporated into the response body. If the later headers have any security purpose, they will not be interpreted by the client.

CVSS: N/A

1.144 CVE-2023-31122

!–> CVE for cpe:2.3:a:apache:http_server:2.2.14:::::*

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

CVSS: N/A

1.145 CVE-2023-45802

!–> CVE for cpe:2.3:a:apache:http_server:2.2.14:::::*

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: N/A

1.146 CVE-2015-5600

!–> CVE for cpe:2.3:a:openbsd:openssh:5.3:p1:::::

Summary: The kbdint_next_device function in auth2-chall.c in sshd in OpenSSH through 6.9 does not properly restrict the processing of keyboard-interactive devices within a single connection, which makes it easier for remote attackers to conduct brute-force attacks or cause a denial of service (CPU consumption) via a long and duplicative

list in the ssh -oKbdInteractiveDevices option, as demonstrated by a modified client that provides a different password for each pam element on this list.

CVSS: 8.5

1.147 CVE-2016-6515

!–> CVE for cpe:2.3:a:openbsd:openssh:5.3:p1:::::

Summary: The auth_password function in auth-passwd.c in sshd in OpenSSH before 7.3 does not limit password lengths for password authentication, which allows remote attackers to cause a denial of service (crypt CPU consumption) via a long string.

CVSS: 7.8

1.148 CVE-2010-4478

!–> CVE for cpe:2.3:a:openbsd:openssh:5.3:p1:::::

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: 7.5

1.149 CVE-2014-1692

!–> CVE for cpe:2.3:a:openbsd:openssh:5.3:p1:::::

Summary: 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.

CVSS: 7.5

1.150 CVE-2016-10009

!–> CVE for cpe:2.3:a:openbsd:openssh:5.3:p1:::::

Summary: Untrusted search path vulnerability in ssh-agent.c in ssh-agent in OpenSSH before 7.4 allows remote attackers to execute arbitrary local PKCS#11 modules by leveraging control over a forwarded agent-socket.

CVSS: 7.5

1.151 CVE-2016-1908

!–> CVE for cpe:2.3:a:openbsd:openssh:5.3:p1:::::

Summary: The client in OpenSSH before 7.2 mishandles failed cookie generation for untrusted X11 forwarding and relies on the local X11 server for access-control decisions, which allows remote X11 clients to trigger a fallback and obtain trusted X11 forwarding privileges by leveraging configuration issues on this X11 server, as demonstrated by lack of the SECURITY extension on this X11 server.

CVSS: 7.5

1.152 CVE-2015-8325

!–> CVE for cpe:2.3:a:openbsd:openssh:5.3:p1:::::

Summary: The do_setup_env function in session.c in sshd in OpenSSH through 7.2p2, when the UseLogin feature is enabled and PAM is configured to read .pam_environment files in user home directories, allows local users to gain privileges by triggering a crafted environment for the /bin/login program, as demonstrated by an LD_PRELOAD environment variable.

CVSS: 7.2

1.153 CVE-2016-10012

!–> CVE for cpe:2.3:a:openbsd:openssh:5.3:p1:::::

Summary: The shared memory manager (associated with pre-authentication compression) in sshd in OpenSSH before 7.4 does not ensure that a bounds check is enforced by all compilers, which might allows local users to gain privileges by leveraging access to a sandboxed privilege-separation process, related to the m_zback and m_zlib data structures.

CVSS: 7.2

1.154 CVE-2015-6564

!–> CVE for cpe:2.3:a:openbsd:openssh:5.3:p1:::::

Summary: Use-after-free vulnerability in the mm_answer_pam_free_ctx function in monitor.c in sshd in OpenSSH before 7.0 on non-OpenBSD platforms might allow local users to gain privileges by leveraging control of the sshd uid to send an unexpectedly early MONITOR_REQ_PAM_FREE_CTX request.

CVSS: 6.9

1.155 CVE-2016-10010

!–> CVE for cpe:2.3:a:openbsd:openssh:5.3:p1:::::

Summary: sshd in OpenSSH before 7.4, when privilege separation is not used, creates forwarded Unix-domain sockets as root, which might allow local users to gain privileges via unspecified vectors, related to serverloop.c.

CVSS: 6.9

1.156 CVE-2020-15778

!–> CVE for cpe:2.3:a:openbsd:openssh:5.3:p1:::::

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: 6.8

1.157 CVE-2014-2532

!–> CVE for cpe:2.3:a:openbsd:openssh:5.3:p1:::::

Summary: sshd in OpenSSH before 6.6 does not properly support wildcards on AcceptEnv lines in sshd_config, which allows remote attackers to bypass intended environment restrictions by using a substring located before a wildcard character.

CVSS: 5.8

1.158 CVE-2014-2653

!–> CVE for cpe:2.3:a:openbsd:openssh:5.3:p1:::::

Summary: The verify_host_key function in sshconnect.c in the client in OpenSSH 6.6 and earlier allows remote servers to trigger the skipping of SSHFP DNS RR checking by presenting an unacceptable HostCertificate.

CVSS: 5.8

1.159 CVE-2019-6111

!–> CVE for cpe:2.3:a:openbsd:openssh:5.3:p1:::::

Summary: An issue was discovered in OpenSSH 7.9. Due to the scp implementation being derived from 1983 rcp, the server chooses which files/directories are sent to the client. However, the scp client only performs cursory validation of the object name returned (only directory traversal attacks are prevented). A malicious scp server (or Man-in-The-Middle attacker) can overwrite arbitrary files in the scp client target directory. If recursive operation (-r) is performed, the server can manipulate subdirectories as well (for example, to overwrite the .ssh/authorized_keys file).

CVSS: 5.8

1.160 CVE-2016-3115

!–> CVE for cpe:2.3:a:openbsd:openssh:5.3:p1:::::

Summary: Multiple CRLF injection vulnerabilities in session.c in sshd in OpenSSH before 7.2p2 allow remote authenticated users to bypass intended shell-command restrictions via crafted X11 forwarding data, related to the (1) do_authenticated1 and (2) session_x11_req functions.

CVSS: 5.5

1.161 CVE-2010-5107

!–> CVE for cpe:2.3:a:openbsd:openssh:5.3:p1:::::

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: 5.0

1.162 CVE-2017-15906

!–> CVE for cpe:2.3:a:openbsd:openssh:5.3:p1:::::

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.

CVSS: 5.0

1.163 CVE-2016-10708

!–> CVE for cpe:2.3:a:openbsd:openssh:5.3:p1:::::

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.

CVSS: 5.0

1.164 CVE-2018-15473

!–> CVE for cpe:2.3:a:openbsd:openssh:5.3:p1:::::

Summary: OpenSSH through 7.7 is prone to a user enumeration vulnerability due to not delaying bailout for an invalid authenticating user until after the packet containing the request has been fully parsed, related to auth2-gss.c, auth2-hostbased.c, and auth2-pubkey.c.

CVSS: 5.0

1.165 CVE-2015-5352

!–> CVE for cpe:2.3:a:openbsd:openssh:5.3:p1:::::

Summary: The x11_open_helper function in channels.c in ssh in OpenSSH before 6.9, when ForwardX11Trusted mode is not used, lacks a check of the refusal deadline for X connections, which makes it easier for remote attackers to bypass intended access restrictions via a connection outside of the permitted time window.

CVSS: 4.3

1.166 CVE-2016-6210

!–> CVE for cpe:2.3:a:openbsd:openssh:5.3:p1:::::

Summary: sshd in OpenSSH before 7.3, when SHA256 or SHA512 are used for user password hashing, uses BLOWFISH hashing on a static password when the username does not exist, which allows remote attackers to enumerate users by leveraging the timing difference between responses when a large password is provided.

CVSS: 4.3

1.167 CVE-2016-20012

!–> CVE for cpe:2.3:a:openbsd:openssh:5.3:p1:::::

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: 4.3

1.168 CVE-2010-4755

!–> CVE for cpe:2.3:a:openbsd:openssh:5.3:p1:::::

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: 4.0

1.169 CVE-2016-0777

!–> CVE for cpe:2.3:a:openbsd:openssh:5.3:p1:::::

Summary: The resend_bytes function in roaming_common.c in the client in OpenSSH 5.x, 6.x, and 7.x before 7.1p2 allows remote servers to obtain sensitive information from process memory by requesting transmission of an entire buffer, as demonstrated by reading a private key.

CVSS: 4.0

1.170 CVE-2019-6109

!–> CVE for cpe:2.3:a:openbsd:openssh:5.3:p1:::::

Summary: An issue was discovered in OpenSSH 7.9. Due to missing character encoding in the progress display, a malicious server (or Man-in-The-Middle attacker) can employ crafted object names to manipulate the client output, e.g., by using ANSI control codes to hide additional files being transferred. This affects refresh_progress_meter() in progressmeter.c.

CVSS: 4.0

1.171 CVE-2019-6110

!–> CVE for cpe:2.3:a:openbsd:openssh:5.3:p1:::::

Summary: In OpenSSH 7.9, due to accepting and displaying arbitrary stderr output from the server, a malicious server (or Man-in-The-Middle attacker) can manipulate the client output, for example to use ANSI control codes to hide additional files being transferred.

CVSS: 4.0

1.172 CVE-2012-0814

!–> CVE for cpe:2.3:a:openbsd:openssh:5.3:p1:::::

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: 3.5

1.173 CVE-2011-5000

!–> CVE for cpe:2.3:a:openbsd:openssh:5.3:p1:::::

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: 3.5

1.174 CVE-2018-20685

!–> CVE for cpe:2.3:a:openbsd:openssh:5.3:p1:::::

Summary: In OpenSSH 7.9, scp.c in the scp client allows remote SSH servers to bypass intended access restrictions via the filename of . or an empty filename. The impact is modifying the permissions of the target directory on the client side.

CVSS: 2.6

1.175 CVE-2021-36368

!–> CVE for cpe:2.3:a:openbsd:openssh:5.3:p1:::::

Summary: An issue was discovered in OpenSSH before 8.9. If a client is using public-key authentication with agent forwarding but without -oLogLevel=verbose, and an attacker has silently modified the server to support the None authentication option, then the user cannot determine whether FIDO authentication is going to confirm that the user wishes to connect to that server, or that the user wishes to allow that server to connect to a different server on the user's behalf. NOTE: the vendor's position is "this is not an authentication bypass, since nothing is being bypassed.

CVSS: 2.6

1.176 CVE-2011-4327

!–> CVE for cpe:2.3:a:openbsd:openssh:5.3:p1:::::

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: 2.1

1.177 CVE-2016-10011

!–> CVE for cpe:2.3:a:openbsd:openssh:5.3:p1:::::

Summary: authfile.c in sshd in OpenSSH before 7.4 does not properly consider the effects of realloc on buffer contents, which might allow local users to obtain sensitive private-key information by leveraging access to a privilege-separated child process.

CVSS: 2.1

1.178 CVE-2015-6563

!–> CVE for cpe:2.3:a:openbsd:openssh:5.3:p1:::::

Summary: The monitor component in sshd in OpenSSH before 7.0 on non-OpenBSD platforms accepts extraneous username data in MONITOR_REQ_PAM_INIT_CTX requests, which allows local users to conduct impersonation attacks by leveraging any SSH login access in conjunction with control of the sshd uid to send a crafted MONITOR_REQ_PWNAM request, related to monitor.c and monitor_wrap.c.

CVSS: 1.9

1.179 CVE-2023-38408

!–> CVE for cpe:2.3:a:openbsd:openssh:5.3:p1:::::

Summary: The PKCS#11 feature in ssh-agent in OpenSSH before 9.3p2 has an insufficiently trustworthy search path, leading to remote code execution if an agent is forwarded to an attacker-controlled system. (Code in /usr/lib is not necessarily safe for loading into ssh-agent.) NOTE: this issue exists because of an incomplete fix for CVE-2016-10009.

CVSS: N/A

1.180 CVE-2023-48795

!–> CVE for cpe:2.3:a:openbsd:openssh:5.3:p1:::::

Summary: The SSH transport protocol with certain OpenSSH extensions, found in OpenSSH before 9.6 and other products, allows remote attackers to bypass integrity checks such that some packets are omitted (from the extension negotiation message), and a client and server may consequently end up with a connection for which some security features have been downgraded or disabled, aka a Terrapin attack. This occurs because the SSH Binary Packet Protocol (BPP), implemented by these extensions, mishandles the handshake phase and mishandles use of sequence numbers. For example, there is an effective attack against SSH's use of ChaCha20-Poly1305 (and CBC with Encrypt-then-MAC). The bypass occurs in chacha20-poly1305@openssh.com and (if CBC is used) the -etm@openssh.com MAC algorithms. This also affects Maverick Synergy Java SSH API before 3.1.0-SNAPSHOT, Dropbear through 2022.83, Ssh before 5.1.1 in Erlang/OTP, PuTTY before 0.80, AsyncSSH before 2.14.2, golang.org/x/crypto before 0.17.0, libssh before 0.10.6, libssh2 through 1.11.0, Thorn Tech SFTP Gateway before 3.4.6, Tera Term before 5.1, Paramiko before 3.4.0, jsch before 0.2.15, SFTPGo before 2.5.6, Netgate pfSense Plus through 23.09.1, Netgate pfSense CE through 2.7.2, HPN-SSH through 18.2.0, ProFTPD before 1.3.8b (and before 1.3.9rc2), ORYX CycloneSSH before 2.3.4, NetSarang XShell 7 before Build 0144, CrushFTP before 10.6.0, ConnectBot SSH library before 2.2.22, Apache MINA sshd through 2.11.0, sshj through 0.37.0, TinySSH through 20230101, trilead-ssh2 6401, LANCOM LCOS and LANconfig, FileZilla before 3.66.4, Nova before 11.8, PKIX-SSH before 14.4, SecureCRT before 9.4.3, Transmit5 before 5.10.4, Win32-OpenSSH before 9.5.0.0p1-Beta, WinSCP before 6.2.2, Bitvise SSH

Server before 9.32, Bitvise SSH Client before 9.33, KiTTY through 0.76.1.13, the net-ssh gem 7.2.0 for Ruby, the mscdex ssh2 module before 1.15.0 for Node.js, the thrussh library before 0.35.1 for Rust, and the Russh crate before 0.40.2 for Rust.

CVSS: N/A

1.181 CVE-2023-51385

!–> CVE for cpe:2.3:a:openbsd:openssh:5.3:p1:::::

Summary: In ssh in OpenSSH before 9.6, OS command injection might occur if a user name or host name has shell metacharacters, and this name is referenced by an expansion token in certain situations. For example, an untrusted Git repository can have a submodule with shell metacharacters in a user name or host name.

CVSS: N/A