netsparker

30-07-23 11.49.37 AM (UTC+05:30)

Detailed Scan Report

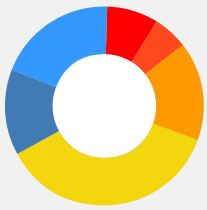
http://zero.webappsecurity.com/

Scan Time	: 30-07-23 11.38.35 AM (UTC+05:30)
Scan Duration	: 00:00:10:53
Total Requests	: 18,732
Average Speed	: 28.7 r/s

Risk Level:
CRITICAL

36 IDENTIFIED	**8** CONFIRMED	**3** CRITICAL
2 HIGH	6 MEDIUM	13 LOW
	5 BEST PRACTICE	7 INFORMATION

Identified Vulnerabilities



Critical	3
High	2
Medium	6
Low	13
Best Practice	5
Information	7
TOTAL	**36**

Confirmed Vulnerabilities

Critical	0
High	2
Medium	3
Low	1
Best Practice	0
Information	2
TOTAL	**8**

Vulnerability Summary

CONFIRM	VULNERABILITY	METHOD	URL	PARAMETER
	Out-of-date Version (Apache)	GET	https://zero.webappsecurity.com/	
	Out-of-date Version (OpenSSL)	GET	https://zero.webappsecurity.com/	
	Out-of-date Version (Tomcat)	GET	http://zero.webappsecurity.com/resources/	
	Insecure Transportation Security Protocol Supported (SSLv2)	GET	https://zero.webappsecurity.com/	
	Password Transmitted over HTTP	GET	http://zero.webappsecurity.com/login.html	
	Apache Server-Status Detected	GET	http://zero.webappsecurity.com/server-status	
	HTTP Strict Transport Security (HSTS) Policy Not Enabled	GET	https://zero.webappsecurity.com/	
	Out-of-date Version (jQuery)	GET	http://zero.webappsecurity.com/	
	Insecure Transportation Security Protocol Supported (SSLv3)	GET	https://zero.webappsecurity.com/	
	Invalid SSL Certificate	GET	https://zero.webappsecurity.com/	
	Weak Ciphers Enabled	GET	https://zero.webappsecurity.com/	
	[Possible] Cross-site Request Forgery	GET	http://zero.webappsecurity.com/feedback.html	
	[Possible] Cross-site Request Forgery in Login Form	GET	http://zero.webappsecurity.com/login.html	
	[Possible] Phishing by Navigating Browser Tabs	GET	http://zero.webappsecurity.com/	

CONFIRM	VULNERABILITY	METHOD	URL	PARAMETER
	Misconfigured Access-Control-Allow-Origin Header	GET	http://zero.webappsecurity.com/	
	Missing X-Frame-Options Header	GET	http://zero.webappsecurity.com/	
	Social Security Number Disclosure	GET	http://zero.webappsecurity.com/admin/users.html	
	Version Disclosure (Apache Coyote)	GET	http://zero.webappsecurity.com/	
	Version Disclosure (Apache Module)	GET	https://zero.webappsecurity.com/	
	Version Disclosure (Apache)	GET	https://zero.webappsecurity.com/	
	Version Disclosure (mod_ssl)	GET	https://zero.webappsecurity.com/	
	Version Disclosure (OpenSSL)	GET	https://zero.webappsecurity.com/	
	Version Disclosure (Tomcat)	GET	http://zero.webappsecurity.com/resources/	
	Insecure Transportation Security Protocol Supported (TLS 1.0)	GET	https://zero.webappsecurity.com/	
	Content Security Policy (CSP) Not Implemented	GET	http://zero.webappsecurity.com/	
	Expect-CT Not Enabled	GET	https://zero.webappsecurity.com/	
	Missing X-XSS-Protection Header	GET	http://zero.webappsecurity.com/	
	Referrer-Policy Not Implemented	GET	http://zero.webappsecurity.com/	
	SameSite Cookie Not Implemented	GET	http://zero.webappsecurity.com/bank/	

CONFIRM	VULNERABILITY	METHOD	URL	PARAMETER
	[Possible] Login Page Identified	GET	http://zero.webappsecurity.com/login.html	
	Apache Web Server Identified	GET	http://zero.webappsecurity.com/	
	Default Page Detected (Apache)	GET	https://zero.webappsecurity.com/	
	Default Page Detected (Tomcat)	GET	http://zero.webappsecurity.com/docs/index.html	
	Email Address Disclosure	GET	http://zero.webappsecurity.com/resources/css/font-awesome.css	
	Forbidden Resource	GET	http://zero.webappsecurity.com/cgi-bin/	
	OPTIONS Method Enabled	OPTIONS	http://zero.webappsecurity.com/	

1. Out-of-date Version (Apache)

CRITICAL 1

Netsparker identified you are using an out-of-date version of Apache.

Impact

Since this is an old version of the software, it may be vulnerable to attacks.

Apache HTTP Server CVE-2016-8743 Vulnerability

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.

Affected Versions

2.2.0 to 2.2.31

External References

- CVE-2016-8743

Apache HTTP Server CVE-2016-5387 Vulnerability

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.

Affected Versions

2.2.0 to 2.2.31

External References

- CVE-2016-5387

Apache HTTP Server Integer Overflow or Wraparound Vulnerability

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.

Affected Versions

2.0 to 2.4.53

External References

- CVE-2022-28615

Apache HTTP Server Insufficient Verification of Data Authenticity Vulnerability

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.

Affected Versions
2.0 to 2.4.53

External References
- CVE-2022-31813

Apache HTTP Server CVE-2012-0053 Vulnerability

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.

Affected Versions
2.2.0 to 2.2.21

External References
- CVE-2012-0053

Apache HTTP Server CVE-2012-0883 Vulnerability

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.

Affected Versions
2.2.0 to 2.2.22

External References
- CVE-2012-0883

Apache HTTP Server CVE-2013-1862 Vulnerability

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.

Affected Versions
2.2.0 to 2.2.24

External References
- CVE-2013-1862

Apache HTTP Server CVE-2013-1896 Vulnerability

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.

Affected Versions
2.2.0 to 2.2.24

External References
- CVE-2013-1896

Apache HTTP Server CVE-2013-6438 Vulnerability

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.

Affected Versions
2.2.0 to 2.2.26

External References
- CVE-2013-6438

Apache HTTP Server Uncontrolled Resource Consumption Vulnerability

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.

Affected Versions
2.2.0 to 2.2.28

External References
- CVE-2014-0118

Apache HTTP Server Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition') Vulnerability

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.

Affected Versions
2.2.0 to 2.2.28

External References
- CVE-2014-0226

Apache HTTP Server CVE-2012-0031 Vulnerability

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.

Affected Versions
2.2.0 to 2.2.21

External References
- CVE-2012-0031

Apache HTTP Server Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') Vulnerability

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

Affected Versions

2.2.0 to 2.2.7

External References

- CVE-2008-0005

Apache HTTP Server Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') Vulnerability

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.

Affected Versions

2.2.0 to 2.2.22

External References

- CVE-2008-0455

Apache HTTP Server Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection') Vulnerability

CRLF injection 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 HTTP headers and conduct HTTP response splitting attacks by uploading a file with a multi-line name containing HTTP header 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.

Affected Versions

2.2.0 to 2.2.11

External References

- CVE-2008-0456

Apache HTTP Server Allocation of Resources Without Limits or Throttling Vulnerability

The ap_proxy_http_process_response function in mod_proxy_http.c in the mod_proxy module in the Apache HTTP Server 2.0.63 and 2.2.8 does not limit the number of forwarded interim responses, which allows remote HTTP servers to cause a denial of service (memory consumption) via a large number of interim responses.

Affected Versions

2.2.0 to 2.2.8

External References

- CVE-2008-2364

Apache HTTP Server Uncontrolled Resource Consumption Vulnerability

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

Affected Versions

2.2.0 to 2.2.11

External References

- CVE-2009-1891

Apache HTTP Server Other Vulnerability

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

Affected Versions

2.2.0 to 2.2.13

External References

- CVE-2009-3095

Apache HTTP Server NULL Pointer Dereference Vulnerability

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

Affected Versions

2.2.0 to 2.2.13

External References

- CVE-2009-3094

Apache HTTP Server Uncontrolled Resource Consumption Vulnerability

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.

Affected Versions

2.2.0 to 2.2.19

External References

- CVE-2011-3192

Apache HTTP Server Allocation of Resources Without Limits or Throttling Vulnerability

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.

Affected Versions

2.2.0 to 2.2.18

External References

- CVE-2011-0419

Apache HTTP Server Exposure of Sensitive Information to an Unauthorized Actor Vulnerability

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.

Affected Versions
2.2.0 to 2.2.14

External References
- CVE-2010-0434

Apache HTTP Server CVE-2014-0098 Vulnerability

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.

Affected Versions
2.2.0 to 2.2.26

External References
- CVE-2014-0098

Apache HTTP Server CVE-2009-2699 Vulnerability

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

Affected Versions
2.2.0 to 2.2.13

External References
- CVE-2009-2699

Apache HTTP Improper Initialization Server Vulnerability

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.

Affected Versions
0.8.11 to 2.4.52

External References
- CVE-2022-22719

Apache HTTP Inconsistent Interpretation of HTTP Requests ('HTTP Request Smuggling') Server Vulnerability

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

Affected Versions
0.8.11 to 2.4.52

External References

- CVE-2022-22720

Apache Denial of service in mod_lua r:parsebody Vulnerability

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.

Affected Versions
0.8.11 to 2.4.53

External References
- CVE-2022-29404

Apache read beyond bounds via ap_rwrite() Vulnerability

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.

Affected Versions
0.8.11 to 2.4.53

External References
- CVE-2022-28614

Apache read beyond bounds in mod_isapi Vulnerability

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

Affected Versions
0.8.11 to 2.4.53

External References
- CVE-2022-28330

Apache HTTP Server Exposure of Sensitive Information to an Unauthorized Actor Vulnerability

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.

Affected Versions
2.0 to 2.4.53

External References
- CVE-2022-30556

Apache HTTP Server Integer Overflow or Wraparound Vulnerability

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.

Affected Versions
2.0 to 2.4.52

External References

- CVE-2022-22721

Apache HTTP Server Out-of-bounds Write Vulnerability

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.

Affected Versions
2.0 to 2.4.48

External References
- CVE-2021-39275

Apache HTTP Server CVE-2013-5704 Vulnerability

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."

Affected Versions
2.2.2 to 2.2.6

External References
- CVE-2013-5704

Apache HTTP Server Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') Vulnerability

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

Affected Versions
2.2.0 to 2.2.6

External References
- CVE-2007-5000

Apache HTTP Server Numeric Errors Vulnerability

Off-by-one error in the apr_brigade_vprintf function in Apache APR-util before 1.3.5 on big-endian platforms allows remote attackers to obtain sensitive information or cause a denial of service (application crash) via crafted input.

Affected Versions
2.2.0 to 2.2.11

External References
- CVE-2009-1956

Apache HTTP Server NULL Pointer Dereference Vulnerability

mod_auth_openidc is an authentication and authorization module for the Apache 2.x HTTP server that implements the OpenID Connect Relying Party functionality. In versions 2.0.0 through 2.4.13.1, when `OIDCStripCookies` is set and a crafted cookie supplied, a NULL pointer dereference would occur, resulting in a segmentation fault. This could be used in a Denial-of-Service attack and thus presents an availability risk. Version 2.4.13.2 contains a patch for this issue. As a workaround, avoid using `OIDCStripCookies`.

Affected Versions
2.0.0 to 2.4.13

External References
- CVE-2023-28625

Apache HTTP Server Interpretation Conflict Vulnerability

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.

Affected Versions
2.0 to 2.4.54

External References
- CVE-2022-37436

Apache HTTP Server Uncontrolled Resource Consumption Vulnerability

CVE-2009-1890 httpd: mod_proxy reverse proxy DoS (infinite loop)

Affected Versions
2.2.0 to 2.2.11

External References
- CVE-2009-1890

Apache HTTP Server Out-of-bounds Write Vulnerability

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.

Affected Versions
2.0 to 2.4.54

External References
- CVE-2006-20001

Apache HTTP Server Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') Vulnerability

CVE-2008-2939 httpd: mod_proxy_ftp globbing XSS

Affected Versions
2.2.6

External References
- CVE-2008-2939

Apache HTTP Server Server-Side Request Forgery (SSRF) Vulnerability

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.

Affected Versions
0.8.11 to 2.4.48

External References
- CVE-2021-40438

Apache HTTP Server NULL Pointer Dereference Vulnerability

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

Affected Versions
0.8.11 to 2.4.48

External References
- CVE-2021-34798

Apache HTTP Server Out-of-bounds Write Vulnerability

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.

Affected Versions
0.8.11 to 2.4.51

External References
- CVE-2021-44790

Apache HTTP Server Resource Management Errors Vulnerability

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.

Affected Versions
2.2.6

External References
- CVE-2014-0231

Apache HTTP Server Improper Input Validation Vulnerability

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.

Affected Versions
2.2 to 2.2.6

External References
- CVE-2015-0228

Apache HTTP Server Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') Vulnerability

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.

Affected Versions
2.2.6

External References
- CVE-2012-3499

Apache HTTP Server Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') Vulnerability

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.

Affected Versions
2.2.6

External References
- CVE-2012-4558

Apache HTTP Server Resource Management Errors Vulnerability

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.

Affected Versions
2.2 to 2.2.6

External References
- CVE-2014-0231

Apache HTTP Server DEPRECATED: Code Vulnerability

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.

Affected Versions
2.2 to 2.2.6

External References
- CVE-2015-3183

Apache HTTP Server Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') Vulnerability

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.

Affected Versions
2.2.6

External References
- CVE-2012-2687

Apache HTTP Server Other Vulnerability

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.

Affected Versions

2.2.6 to 2.2.15

External References

- CVE-2010-1452

Apache HTTP Server Improper Input Validation Vulnerability

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.

Affected Versions

2.2.6

External References

- CVE-2011-3368

Apache HTTP Server Numeric Errors Vulnerability

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.

Affected Versions

2.2.6

External References

- CVE-2011-3607

Apache HTTP Server CVE-2010-0425 Vulnerability

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."

Affected Versions

2.2.6 to 2.2.14

External References

- CVE-2010-0425

Apache HTTP Server Other Vulnerability

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.

Affected Versions
2.2.6

External References
- CVE-2010-0408

Apache HTTP Server Resource Management Errors Vulnerability

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.

Affected Versions
2.2 to 2.2.6

External References
- CVE-2007-6750

Apache HTTP Server Resource Management Errors Vulnerability

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.

Affected Versions
2.2.6

External References
- CVE-2007-6750

Apache HTTP Server Improper Input Validation Vulnerability

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.

Affected Versions
2.2.6

External References
- CVE-2011-4415

Apache HTTP Server Improper Input Validation Vulnerability

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.

Affected Versions
2.2.6

External References
- CVE-2011-3639

Apache HTTP Server Improper Input Validation Vulnerability

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.

Affected Versions

2.2.6

External References

- CVE-2011-4317

Apache HTTP Server Configuration Vulnerability

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

Affected Versions

2.2 to 2.2.6

External References

- CVE-2009-1195

Apache HTTP Server Configuration Vulnerability

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

Affected Versions

2.2.6 to 2.2.10

External References

- CVE-2009-1195

Apache HTTP Server Cryptographic Issues Vulnerability

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.

Affected Versions

2.2 to 2.2.6

External References

- CVE-2009-3555

Apache HTTP Server Exposure of Sensitive Information to an Unauthorized Actor Vulnerability

Apache HTTP Server, when running on Linux with a document root on a Windows share mounted using smbfs, allows remote attackers to obtain unprocessed content such as source files for .php programs via a trailing "\" (backslash), which is not handled by the intended AddType directive.

Affected Versions
2.2.6

External References
- CVE-2007-6514

Apache HTTP Server Resource Management Errors Vulnerability

The balancer_handler function in mod_proxy_balancer in the Apache HTTP Server 2.2.0 through 2.2.6, when a threaded Multi-Processing Module is used, allows remote authenticated users to cause a denial of service (child process crash) via an invalid bb variable.

Affected Versions
2.2.6

External References
- CVE-2007-6422

Apache HTTP Server Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') Vulnerability

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

Affected Versions
2.2.6

External References
- CVE-2007-6388

Apache HTTP Server Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') Vulnerability

Cross-site scripting (XSS) vulnerability in balancer-manager in mod_proxy_balancer in the Apache HTTP Server 2.2.0 through 2.2.6 allows remote attackers to inject arbitrary web script or HTML via the (1) ss, (2) wr, or (3) rr parameters, or (4) the URL.

Affected Versions
2.2.6

External References
- CVE-2007-6421

Apache HTTP Server Resource Management Errors Vulnerability

** DISPUTED ** Unspecified vulnerability in mod_proxy_balancer for Apache HTTP Server 2.2.x before 2.2.7-dev, when running on Windows, allows remote attackers to trigger memory corruption via a long URL. NOTE: the vendor could not reproduce this issue.

Affected Versions
2.2.6

External References

- CVE-2007-6423

Apache HTTP Server Cross-Site Request Forgery (CSRF) Vulnerability

Cross-site request forgery (CSRF) vulnerability in the balancer-manager in mod_proxy_balancer for Apache HTTP Server 2.2.x allows remote attackers to gain privileges via unspecified vectors.

Affected Versions

2.2.6

External References

- CVE-2007-6420

Apache HTTP Server Out-of-bounds Read Vulnerability

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.

Affected Versions

2.2 to 2.2.6

External References

- CVE-2018-1303

Apache HTTP Server NULL Pointer Dereference Vulnerability

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.

Affected Versions

2.2 to 2.2.6

External References

- CVE-2018-1302

Apache HTTP Server Improper Restriction of Operations within the Bounds of a Memory Buffer Vulnerability

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.

Affected Versions

2.2 to 2.2.6

External References

- CVE-2018-1301

Apache HTTP Server Improper Neutralization of CRLF Sequences ('CRLF Injection') Vulnerability

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).

Affected Versions
2.2.6

External References
- CVE-2016-4975

Apache HTTP Server Improper Restriction of Operations within the Bounds of a Memory Buffer Vulnerability

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.

Affected Versions
2.2.0 to 2.2.6

External References
- CVE-2017-7679

Apache HTTP Server Improper Input Validation Vulnerability

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.

Affected Versions
2.2 to 2.2.6

External References
- CVE-2017-9788

Apache HTTP Server Use After Free Vulnerability

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.

Affected Versions
2.2 to 2.2.6

External References
- CVE-2017-9798

Apache HTTP Server Improper Input Validation Vulnerability

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.

Affected Versions
2.2 to 2.2.6

External References

- CVE-2016-8612

Vulnerabilities

1.1. https://zero.webappsecurity.com/

Identified Version

- 2.2.6

Latest Version

- 2.2.34 (in this branch)

Vulnerability Database

- Result is based on 07/27/2023 20:30:00 vulnerability database content.

Certainty

Request

```
GET / HTTP/1.1
Host: zero.webappsecurity.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: JSESSIONID=5CF19C3A
Referer: https://zero.webappsecurity.com/
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.
77 Safari/537.36
X-Scanner: Netsparker
```

Response

Response Time (ms) : 191.9997 **Total Bytes Received** : 345 **Body Length** : 44 **Is Compressed** : No

```
HTTP/1.1 200 OK
Content-Type: text/html
Server: Apache/2.2.6 (Win32) mod_ssl/2.2.6 OpenSSL/0.9.8e mod_jk/1.2.40

Content-Length: 44
Last-Modified: Sat, 20 Nov 2004 14:16:24 GMT
Accept-Ranges: bytes
Access-Control-Allow-Origin: *
Date: Sun, 30 Jul 2023 06:09:00 GMT
ETag: "24c22-2c-44adde00"

<html><body><h1>It works!</h1></body></html>
```

Remedy

Please upgrade your installation of Apache to the latest stable version.

Remedy References

- Downloading the Apache HTTP Server

CLASSIFICATION

PCI DSS v3.2	6.2
OWASP 2013	A9
OWASP 2017	A9
CWE	829
CAPEC	310
HIPAA	164.308(A)(1)(I)
OWASP Proactive Controls	C1
ISO27001	A.14.1.2

2. Out-of-date Version (OpenSSL)

CRITICAL 1

Netsparker identified you are using an out-of-date version of OpenSSL.

Impact

Since this is an old version of the software, it may be vulnerable to attacks.

OpenSSL Improper Authentication Vulnerability

CVE-2010-4252 openssl: session key retrieval flaw in J-PAKE implementation

Affected Versions

0.9.2b to 0.9.8zh

External References

- CVE-2010-4252

OpenSSL Improper Authentication Vulnerability

CVE-2010-4252 openssl: session key retrieval flaw in J-PAKE implementation

Affected Versions

0.9.8e

External References

- CVE-2010-4252

OpenSSL Cryptographic Issues Vulnerability

A flaw was found in the way SSL 3.0 handled padding bytes when decrypting messages encrypted using block ciphers in cipher block chaining (CBC) mode. This flaw allows a man-in-the-middle (MITM) attacker to decrypt a selected byte of a cipher text in as few as 256 tries if they are able to force a victim application to repeatedly send the same data over newly created SSL 3.0 connections.

Affected Versions

0.9.8e

External References

- CVE-2014-3566

OpenSSL Resource Management Errors Vulnerability

The do_free_upto function in crypto/cms/cms_smime.c in OpenSSL before 0.9.8zg, 1.0.0 before 1.0.0s, 1.0.1 before 1.0.1n, and 1.0.2 before 1.0.2b allows remote attackers to cause a denial of service (infinite loop) via vectors that trigger a NULL value of a BIO data structure, as demonstrated by an unrecognized X.660 OID for a hash function.

Affected Versions

0.9.2b to 0.9.8zf

External References

- CVE-2015-1792

OpenSSL Cryptographic Issues Vulnerability

The TLS protocol 1.2 and earlier, when a DHE_EXPORT ciphersuite is enabled on a server but not on a client, does not properly convey a DHE_EXPORT choice, which allows man-in-the-middle attackers to conduct cipher-downgrade attacks by rewriting a ClientHello with DHE replaced by DHE_EXPORT and then rewriting a ServerHello with DHE_EXPORT replaced by DHE, aka the "Logjam" issue.

Affected Versions

0.9.2b to 0.9.8zh

External References

- CVE-2015-4000

OpenSSL Cryptographic Issues Vulnerability

OpenSSL 0.9.8c-1 up to versions before 0.9.8g-9 on Debian-based operating systems uses a random number generator that generates predictable numbers, which makes it easier for remote attackers to conduct brute force guessing attacks against cryptographic keys.

Affected Versions

0.9.8d to 0.9.8g

External References

- CVE-2008-0166

OpenSSL Loop with Unreachable Exit Condition ('Infinite Loop') Vulnerability

Internally libssl in OpenSSL calls X509_verify_cert() on the client side to verify a certificate supplied by a server. That function may return a negative return value to indicate an internal error (for example out of memory). Such a negative return value is mishandled by OpenSSL and will cause an IO function (such as SSL_connect() or SSL_do_handshake()) to not indicate success and a subsequent call to SSL_get_error() to return the value SSL_ERROR_WANT_RETRY_VERIFY. This return value is only supposed to be returned by OpenSSL if the application has previously called SSL_CTX_set_cert_verify_callback(). Since most applications do not do this the SSL_ERROR_WANT_RETRY_VERIFY return value from SSL_get_error() will be totally unexpected and applications may not behave correctly as a result. The exact behaviour will depend on the application but it could result in crashes, infinite loops or other similar incorrect responses. This issue is made more serious in combination with a separate bug in OpenSSL 3.0 that will cause X509_verify_cert() to indicate an internal error when processing a certificate chain. This will occur where a certificate does not include the Subject Alternative Name extension but where a Certificate Authority has enforced name constraints. This issue can occur even with valid chains. By combining the two issues an attacker could induce incorrect, application dependent behaviour. Fixed in OpenSSL 3.0.1 (Affected 3.0.0).

Affected Versions

0.9.2b to 0.9.8zh

External References

- CVE-2021-4044

OpenSSL Resource Management Errors Vulnerability

The ephemeral ECDH ciphersuite functionality in OpenSSL 0.9.8 through 0.9.8r and 1.0.x before 1.0.0e does not ensure thread safety during processing of handshake messages from clients, which allows remote attackers to cause a denial of service (daemon crash) via out-of-order messages that violate the TLS protocol.

Affected Versions

0.9.8 to 0.9.8s

External References

- CVE-2011-3210

OpenSSL Cryptographic Issues Vulnerability

The DTLS implementation in OpenSSL before 0.9.8s and 1.x before 1.0.0f performs a MAC check only if certain padding is valid, which makes it easier for remote attackers to recover plaintext via a padding oracle attack.

Affected Versions

0.9.2b to 0.9.8zh

External References

- CVE-2011-4108

OpenSSL Cryptographic Issues Vulnerability

The DTLS implementation in OpenSSL before 0.9.8s and 1.x before 1.0.0f performs a MAC check only if certain padding is valid, which makes it easier for remote attackers to recover plaintext via a padding oracle attack.

Affected Versions

0.9.2b to 0.9.8r

External References

- CVE-2011-4108

OpenSSL Cryptographic Issues Vulnerability

The DTLS implementation in OpenSSL before 0.9.8s and 1.x before 1.0.0f performs a MAC check only if certain padding is valid, which makes it easier for remote attackers to recover plaintext via a padding oracle attack.

Affected Versions

0.9.4 to 0.9.8q

External References

- CVE-2011-4108

OpenSSL Resource Management Errors Vulnerability

Double free vulnerability in OpenSSL 0.9.8 before 0.9.8s, when X509_V_FLAG_POLICY_CHECK is enabled, allows remote attackers to have an unspecified impact by triggering failure of a policy check.

Affected Versions

0.9.8 to 0.9.8r

External References

- CVE-2011-4109

OpenSSL Cryptographic Issues Vulnerability

The SSL 3.0 implementation in OpenSSL before 0.9.8s and 1.x before 1.0.0f does not properly initialize data structures for block cipher padding, which might allow remote attackers to obtain sensitive information by decrypting the padding data sent by an SSL peer.

Affected Versions

0.9.2b to 0.9.8zh

External References

- CVE-2011-4576

OpenSSL Cryptographic Issues Vulnerability

The SSL 3.0 implementation in OpenSSL before 0.9.8s and 1.x before 1.0.0f does not properly initialize data structures for block cipher padding, which might allow remote attackers to obtain sensitive information by decrypting the padding data sent by an SSL peer.

Affected Versions

0.9.2b to 0.9.8r

External References

- CVE-2011-4576

OpenSSL Cryptographic Issues Vulnerability

The SSL 3.0 implementation in OpenSSL before 0.9.8s and 1.x before 1.0.0f does not properly initialize data structures for block cipher padding, which might allow remote attackers to obtain sensitive information by decrypting the padding data sent by an SSL peer.

Affected Versions

0.9.4 to 0.9.8q

External References

- CVE-2011-4576

OpenSSL Resource Management Errors Vulnerability

OpenSSL before 0.9.8s and 1.x before 1.0.0f, when RFC 3779 support is enabled, allows remote attackers to cause a denial of service (assertion failure) via an X.509 certificate containing certificate-extension data associated with (1) IP address blocks or (2) Autonomous System (AS) identifiers.

Affected Versions

0.9.2b to 0.9.8zh

External References

- CVE-2011-4577

OpenSSL Cryptographic Issues Vulnerability

The elliptic curve cryptography (ECC) subsystem in OpenSSL 1.0.0d and earlier, when the Elliptic Curve Digital Signature Algorithm (ECDSA) is used for the ECDHE_ECDSA cipher suite, does not properly implement curves over binary fields, which makes it easier for context-dependent attackers to determine private keys via a timing attack and a lattice calculation.

Affected Versions

0.9.2b to 0.9.8p

External References

- CVE-2011-1945

OpenSSL Cryptographic Issues Vulnerability

The Cryptographic Message Syntax (CMS) implementation in crypto/cms/cms_asn1.c in OpenSSL before 0.9.8o and 1.x before 1.0.0a does not properly handle structures that contain OriginatorInfo, which allows context-dependent attackers to modify invalid memory locations or conduct double-free attacks, and possibly execute arbitrary code, via unspecified vectors.

Affected Versions
0.9.2b to 0.9.8n

External References
- CVE-2010-0742

OpenSSL Cryptographic Issues Vulnerability

The Cryptographic Message Syntax (CMS) implementation in crypto/cms/cms_asn1.c in OpenSSL before 0.9.8o and 1.x before 1.0.0a does not properly handle structures that contain OriginatorInfo, which allows context-dependent attackers to modify invalid memory locations or conduct double-free attacks, and possibly execute arbitrary code, via unspecified vectors.

Affected Versions
0.9.2b to 0.9.8m

External References
- CVE-2010-0742

OpenSSL Other Vulnerability

OpenSSL before 0.9.8q, and 1.0.x before 1.0.0c, when SSL_OP_NETSCAPE_REUSE_CIPHER_CHANGE_BUG is enabled, does not properly prevent modification of the ciphersuite in the session cache, which allows remote attackers to force the downgrade to an unintended cipher via vectors involving sniffing network traffic to discover a session identifier.

Affected Versions
0.9.2b to 0.9.8p

External References
- CVE-2010-4180

OpenSSL Other Vulnerability

OpenSSL before 0.9.8q, and 1.0.x before 1.0.0c, when SSL_OP_NETSCAPE_REUSE_CIPHER_CHANGE_BUG is enabled, does not properly prevent modification of the ciphersuite in the session cache, which allows remote attackers to force the downgrade to an unintended cipher via vectors involving sniffing network traffic to discover a session identifier.

Affected Versions
0.9.2b to 0.9.8o

External References
- CVE-2010-4180

OpenSSL Cryptographic Issues Vulnerability

OpenSSL before 0.9.8j, when SSL_OP_NETSCAPE_REUSE_CIPHER_CHANGE_BUG is enabled, does not prevent modification of the ciphersuite in the session cache, which allows remote attackers to force the use of a disabled cipher via vectors involving sniffing network traffic to discover a session identifier, a different vulnerability than CVE-2010-4180.

Affected Versions
0.9.2b to 0.9.8i

External References
- CVE-2008-7270

OpenSSL Cryptographic Issues Vulnerability

OpenSSL before 0.9.8j, when SSL_OP_NETSCAPE_REUSE_CIPHER_CHANGE_BUG is enabled, does not prevent modification of the ciphersuite in the session cache, which allows remote attackers to force the use of a disabled cipher via vectors involving sniffing network traffic to discover a session identifier, a different vulnerability than CVE-2010-4180.

Affected Versions
0.9.2b to 0.9.8h

External References
- CVE-2008-7270

OpenSSL Cryptographic Issues Vulnerability

The elliptic curve cryptography (ECC) subsystem in OpenSSL 1.0.0d and earlier, when the Elliptic Curve Digital Signature Algorithm (ECDSA) is used for the ECDHE_ECDSA cipher suite, does not properly implement curves over binary fields, which makes it easier for context-dependent attackers to determine private keys via a timing attack and a lattice calculation.

Affected Versions
0.9.2b to 0.9.8zh

External References
- CVE-2011-1945

OpenSSL Resource Management Errors Vulnerability

OpenSSL before 0.9.8s and 1.x before 1.0.0f, when RFC 3779 support is enabled, allows remote attackers to cause a denial of service (assertion failure) via an X.509 certificate containing certificate-extension data associated with (1) IP address blocks or (2) Autonomous System (AS) identifiers.

Affected Versions
0.9.2b to 0.9.8r

External References
- CVE-2011-4577

OpenSSL Resource Management Errors Vulnerability

OpenSSL before 0.9.8s and 1.x before 1.0.0f, when RFC 3779 support is enabled, allows remote attackers to cause a denial of service (assertion failure) via an X.509 certificate containing certificate-extension data associated with (1) IP address blocks or (2) Autonomous System (AS) identifiers.

Affected Versions
0.9.4 to 0.9.8q

External References
- CVE-2011-4577

OpenSSL Resource Management Errors Vulnerability

The mime_param_cmp function in crypto/asn1/asn_mime.c in OpenSSL before 0.9.8u and 1.x before 1.0.0h allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via a crafted S/MIME message, a different vulnerability than CVE-2006-7250.

Affected Versions

0.9.2b to 0.9.8t

External References

- CVE-2012-1165

OpenSSL Resource Management Errors Vulnerability

The mime_param_cmp function in crypto/asn1/asn_mime.c in OpenSSL before 0.9.8u and 1.x before 1.0.0h allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via a crafted S/MIME message, a different vulnerability than CVE-2006-7250.

Affected Versions

0.9.2b to 0.9.8s

External References

- CVE-2012-1165

OpenSSL Improper Restriction of Operations within the Bounds of a Memory Buffer Vulnerability

The asn1_d2i_read_bio function in crypto/asn1/a_d2i_fp.c in OpenSSL before 0.9.8v, 1.0.0 before 1.0.0i, and 1.0.1 before 1.0.1a does not properly interpret integer data, which allows remote attackers to conduct buffer overflow attacks, and cause a denial of service (memory corruption) or possibly have unspecified other impact, via crafted DER data, as demonstrated by an X.509 certificate or an RSA public key.

Affected Versions

0.9.2b to 0.9.8u

External References

- CVE-2012-2110

OpenSSL Improper Restriction of Operations within the Bounds of a Memory Buffer Vulnerability

The asn1_d2i_read_bio function in crypto/asn1/a_d2i_fp.c in OpenSSL before 0.9.8v, 1.0.0 before 1.0.0i, and 1.0.1 before 1.0.1a does not properly interpret integer data, which allows remote attackers to conduct buffer overflow attacks, and cause a denial of service (memory corruption) or possibly have unspecified other impact, via crafted DER data, as demonstrated by an X.509 certificate or an RSA public key.

Affected Versions

0.9.2b to 0.9.8t

External References

- CVE-2012-2110

OpenSSL Numeric Errors Vulnerability

Integer underflow in OpenSSL before 0.9.8x, 1.0.0 before 1.0.0j, and 1.0.1 before 1.0.1c, when TLS 1.1, TLS 1.2, or DTLS is used with CBC encryption, allows remote attackers to cause a denial of service (buffer over-read) or possibly have unspecified other impact via a crafted TLS packet that is not properly handled during a certain explicit IV calculation.

Affected Versions

0.9.2b to 0.9.8w

External References

- CVE-2012-2333

OpenSSL Numeric Errors Vulnerability

Integer underflow in OpenSSL before 0.9.8x, 1.0.0 before 1.0.0j, and 1.0.1 before 1.0.1c, when TLS 1.1, TLS 1.2, or DTLS is used with CBC encryption, allows remote attackers to cause a denial of service (buffer over-read) or possibly have unspecified other impact via a crafted TLS packet that is not properly handled during a certain explicit IV calculation.

Affected Versions

0.9.2b to 0.9.8v

External References

- CVE-2012-2333

OpenSSL Permissions, Privileges, and Access Controls Vulnerability

** DISPUTED ** OpenSSL before 0.9.8l, and 0.9.8m through 1.x, does not properly restrict client-initiated renegotiation within the SSL and TLS protocols, which might make it easier for remote attackers to cause a denial of service (CPU consumption) by performing many renegotiations within a single connection, a different vulnerability than CVE-2011-5094. NOTE: it can also be argued that it is the responsibility of server deployments, not a security library, to prevent or limit renegotiation when it is inappropriate within a specific environment.

Affected Versions

0.9.2b to 0.9.8k

External References

- CVE-2011-1473

OpenSSL Cryptographic Issues Vulnerability

The implementation of Cryptographic Message Syntax (CMS) and PKCS #7 in OpenSSL before 0.9.8u and 1.x before 1.0.0h does not properly restrict certain oracle behavior, which makes it easier for context-dependent attackers to decrypt data via a Million Message Attack (MMA) adaptive chosen ciphertext attack.

Affected Versions

0.9.2b to 0.9.8s

External References

- CVE-2012-0884

OpenSSL Resource Management Errors Vulnerability

The Server Gated Cryptography (SGC) implementation in OpenSSL before 0.9.8s and 1.x before 1.0.0f does not properly handle handshake restarts, which allows remote attackers to cause a denial of service (CPU consumption) via unspecified vectors.

Affected Versions

0.9.2b to 0.9.8zh

External References

- CVE-2011-4619

OpenSSL Resource Management Errors Vulnerability

The Server Gated Cryptography (SGC) implementation in OpenSSL before 0.9.8s and 1.x before 1.0.0f does not properly handle handshake restarts, which allows remote attackers to cause a denial of service (CPU consumption) via unspecified vectors.

Affected Versions
0.9.2b to 0.9.8r

External References
- CVE-2011-4619

OpenSSL Resource Management Errors Vulnerability

The Server Gated Cryptography (SGC) implementation in OpenSSL before 0.9.8s and 1.x before 1.0.0f does not properly handle handshake restarts, which allows remote attackers to cause a denial of service (CPU consumption) via unspecified vectors.

Affected Versions
0.9.4 to 0.9.8q

External References
- CVE-2011-4619

OpenSSL Resource Management Errors Vulnerability

The GOST ENGINE in OpenSSL before 1.0.0f does not properly handle invalid parameters for the GOST block cipher, which allows remote attackers to cause a denial of service (daemon crash) via crafted data from a TLS client.

Affected Versions
0.9.2b to 0.9.8zh

External References
- CVE-2012-0027

OpenSSL Resource Management Errors Vulnerability

The GOST ENGINE in OpenSSL before 1.0.0f does not properly handle invalid parameters for the GOST block cipher, which allows remote attackers to cause a denial of service (daemon crash) via crafted data from a TLS client.

Affected Versions
0.9.2b to 0.9.8s

External References
- CVE-2012-0027

OpenSSL Cryptographic Issues Vulnerability

crypto/bn/bn_nist.c in OpenSSL before 0.9.8h on 32-bit platforms, as used in stunnel and other products, in certain circumstances involving ECDH or ECDHE cipher suites, uses an incorrect modular reduction algorithm in its implementation of the P-256 and P-384 NIST elliptic curves, which allows remote attackers to obtain the private key of a TLS server via multiple handshake attempts.

Affected Versions
0.9.2b to 0.9.8f

External References
- CVE-2011-4354

OpenSSL Other Vulnerability

The mime_hdr_cmp function in crypto/asn1/asn_mime.c in OpenSSL 0.9.8t and earlier allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via a crafted S/MIME message.

Affected Versions
0.9.2b to 0.9.8t

External References
- CVE-2006-7250

OpenSSL Other Vulnerability

The mime_hdr_cmp function in crypto/asn1/asn_mime.c in OpenSSL 0.9.8t and earlier allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via a crafted S/MIME message.

Affected Versions
0.9.2b to 0.9.8s

External References
- CVE-2006-7250

OpenSSL Cryptographic Issues Vulnerability

The implementation of Cryptographic Message Syntax (CMS) and PKCS #7 in OpenSSL before 0.9.8u and 1.x before 1.0.0h does not properly restrict certain oracle behavior, which makes it easier for context-dependent attackers to decrypt data via a Million Message Attack (MMA) adaptive chosen ciphertext attack.

Affected Versions
0.9.2b to 0.9.8t

External References
- CVE-2012-0884

OpenSSL Improper Input Validation Vulnerability

The kssl_keytab_is_available function in ssl/kssl.c in OpenSSL before 0.9.8n, when Kerberos is enabled but Kerberos configuration files cannot be opened, does not check a certain return value, which allows remote attackers to cause a denial of service (NULL pointer dereference and daemon crash) via SSL cipher negotiation, as demonstrated by a chroot installation of Dovecot or stunnel without Kerberos configuration files inside the chroot.

Affected Versions
0.9.8 to 0.9.8l

External References
- CVE-2010-0433

OpenSSL Improper Input Validation Vulnerability

The kssl_keytab_is_available function in ssl/kssl.c in OpenSSL before 0.9.8n, when Kerberos is enabled but Kerberos configuration files cannot be opened, does not check a certain return value, which allows remote attackers to cause a denial of service (NULL pointer dereference and daemon crash) via SSL cipher negotiation, as demonstrated by a chroot installation of Dovecot or stunnel without Kerberos configuration files inside the chroot.

Affected Versions
0.9.2b to 0.9.8m

External References

- CVE-2010-0433

OpenSSL Resource Management Errors Vulnerability

Multiple memory leaks in the dtls1_process_out_of_seq_message function in ssl/d1_both.c in OpenSSL 0.9.8k and earlier 0.9.8 versions allow remote attackers to cause a denial of service (memory consumption) via DTLS records that (1) are duplicates or (2) have sequence numbers much greater than current sequence numbers, aka "DTLS fragment handling memory leak."

Affected Versions
0.9.8a to 0.9.8j

External References
- CVE-2009-1378

OpenSSL Other Vulnerability

ssl/s3_pkt.c in OpenSSL before 0.9.8i allows remote attackers to cause a denial of service (NULL pointer dereference and daemon crash) via a DTLS ChangeCipherSpec packet that occurs before ClientHello.

Affected Versions
0.9.7a to 0.9.8h

External References
- CVE-2009-1386

OpenSSL Resource Management Errors Vulnerability

The dtls1_retrieve_buffered_fragment function in ssl/d1_both.c in OpenSSL before 1.0.0 Beta 2 allows remote attackers to cause a denial of service (NULL pointer dereference and daemon crash) via an out-of-sequence DTLS handshake message, related to a "fragment bug."

Affected Versions
0.9.7a to 0.9.8k

External References
- CVE-2009-1387

OpenSSL Improper Authentication Vulnerability

Mutt 1.5.19, when linked against (1) OpenSSL (mutt_ssl.c) or (2) GnuTLS (mutt_ssl_gnutls.c), allows connections when only one TLS certificate in the chain is accepted instead of verifying the entire chain, which allows remote attackers to spoof trusted servers via a man-in-the-middle attack.

Affected Versions
0.9.2b to 0.9.8zh

External References
- CVE-2009-1390

OpenSSL Cryptographic Issues Vulnerability

The Network Security Services (NSS) library before 3.12.3, as used in Firefox; GnuTLS before 2.6.4 and 2.7.4; OpenSSL 0.9.8 through 0.9.8k; and other products support MD2 with X.509 certificates, which might allow remote attackers to spoof certificates by using MD2 design flaws to generate a hash collision in less than brute-force time. NOTE: the scope of this issue is currently limited because the amount of computation required is still large.

Affected Versions
0.9.8 to 0.9.8k

External References
- CVE-2009-2409

OpenSSL Cryptographic Issues Vulnerability

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.

Affected Versions
0.9.2b to 0.9.8k

External References
- CVE-2009-3555

OpenSSL Resource Management Errors Vulnerability

Memory leak in the zlib_stateful_finish function in crypto/comp/c_zlib.c in OpenSSL 0.9.8l and earlier and 1.0.0 Beta through Beta 4 allows remote attackers to cause a denial of service (memory consumption) via vectors that trigger incorrect calls to the CRYPTO_cleanup_all_ex_data function, as demonstrated by use of SSLv3 and PHP with the Apache HTTP Server, a related issue to CVE-2008-1678.

Affected Versions
0.9.2b to 0.9.8l

External References
- CVE-2009-4355

OpenSSL Resource Management Errors Vulnerability

Memory leak in the zlib_stateful_finish function in crypto/comp/c_zlib.c in OpenSSL 0.9.8l and earlier and 1.0.0 Beta through Beta 4 allows remote attackers to cause a denial of service (memory consumption) via vectors that trigger incorrect calls to the CRYPTO_cleanup_all_ex_data function, as demonstrated by use of SSLv3 and PHP with the Apache HTTP Server, a related issue to CVE-2008-1678.

Affected Versions
0.9.2b to 0.9.8k

External References
- CVE-2009-4355

OpenSSL Improper Input Validation Vulnerability

OpenSSL before 0.9.8m does not check for a NULL return value from bn_wexpand function calls in (1) crypto/bn/bn_div.c, (2) crypto/bn/bn_gf2m.c, (3) crypto/ec/ec2_smpl.c, and (4) engines/e_ubsec.c, which has unspecified impact and context-dependent attack vectors.

Affected Versions
0.9.2b to 0.9.8l

External References
- CVE-2009-3245

OpenSSL Improper Input Validation Vulnerability

OpenSSL before 0.9.8m does not check for a NULL return value from bn_wexpand function calls in (1) crypto/bn/bn_div.c, (2) crypto/bn/bn_gf2m.c, (3) crypto/ec/ec2_smpl.c, and (4) engines/e_ubsec.c, which has unspecified impact and context-dependent attack vectors.

Affected Versions
0.9.8 to 0.9.8k

External References
- CVE-2009-3245

OpenSSL Resource Management Errors Vulnerability

Multiple memory leaks in the dtls1_process_out_of_seq_message function in ssl/d1_both.c in OpenSSL 0.9.8k and earlier 0.9.8 versions allow remote attackers to cause a denial of service (memory consumption) via DTLS records that (1) are duplicates or (2) have sequence numbers much greater than current sequence numbers, aka "DTLS fragment handling memory leak."

Affected Versions
0.9.2b to 0.9.8k

External References
- CVE-2009-1378

OpenSSL Improper Restriction of Operations within the Bounds of a Memory Buffer Vulnerability

The dtls1_buffer_record function in ssl/d1_pkt.c in OpenSSL 0.9.8k and earlier 0.9.8 versions allows remote attackers to cause a denial of service (memory consumption) via a large series of "future epoch" DTLS records that are buffered in a queue, aka "DTLS record buffer limitation bug."

Affected Versions
0.9.8a to 0.9.8j

External References
- CVE-2009-1377

OpenSSL Other Vulnerability

The BN_from_montgomery function in crypto/bn/bn_mont.c in OpenSSL 0.9.8e and earlier does not properly perform Montgomery multiplication, which might allow local users to conduct a side-channel attack and retrieve RSA private keys.

Affected Versions
0.9.2b to 0.9.8e

External References
- CVE-2007-3108

OpenSSL Numeric Errors Vulnerability

Off-by-one error in the SSL_get_shared_ciphers function in OpenSSL 0.9.7 up to 0.9.7l, and 0.9.8 up to 0.9.8f, might allow remote attackers to execute arbitrary code via a crafted packet that triggers a one-byte buffer underflow. NOTE: this issue was introduced as a result of a fix for CVE-2006-3738. As of 20071012, it is unknown whether code execution is possible.

Affected Versions
0.9.8 to 0.9.8f

External References
- CVE-2007-5135

OpenSSL Numeric Errors Vulnerability

Off-by-one error in the DTLS implementation in OpenSSL 0.9.8 before 0.9.8f allows remote attackers to execute arbitrary code via unspecified vectors.

Affected Versions
0.9.8 to 0.9.8e

External References
- CVE-2007-4995

OpenSSL Improper Input Validation Vulnerability

OpenSSL 0.9.8i and earlier does not properly check the return value from the EVP_VerifyFinal function, which allows remote attackers to bypass validation of the certificate chain via a malformed SSL/TLS signature for DSA and ECDSA keys.

Affected Versions
0.9.2b to 0.9.8h

External References
- CVE-2008-5077

OpenSSL Improper Input Validation Vulnerability

OpenSSL 0.9.8i and earlier does not properly check the return value from the EVP_VerifyFinal function, which allows remote attackers to bypass validation of the certificate chain via a malformed SSL/TLS signature for DSA and ECDSA keys.

Affected Versions
0.9.8 to 0.9.8g

External References
- CVE-2008-5077

OpenSSL Improper Restriction of Operations within the Bounds of a Memory Buffer Vulnerability

The ASN1_STRING_print_ex function in OpenSSL before 0.9.8k allows remote attackers to cause a denial of service (invalid memory access and application crash) via vectors that trigger printing of a (1) BMPString or (2) UniversalString with an invalid encoded length.

Affected Versions
0.9.2b to 0.9.8j

External References
- CVE-2009-0590

OpenSSL Numeric Errors Vulnerability

OpenSSL before 0.9.8k on WIN64 and certain other platforms does not properly handle a malformed ASN.1 structure, which allows remote attackers to cause a denial of service (invalid memory access and application crash) by placing this structure in the public key of a certificate, as demonstrated by an RSA public key.

Affected Versions
0.9.2b to 0.9.8j

External References
- CVE-2009-0789

OpenSSL Numeric Errors Vulnerability

OpenSSL before 0.9.8k on WIN64 and certain other platforms does not properly handle a malformed ASN.1 structure, which allows remote attackers to cause a denial of service (invalid memory access and application crash) by placing this structure in the public key of a certificate, as demonstrated by an RSA public key.

Affected Versions
0.9.2b to 0.9.8i

External References
- CVE-2009-0789

OpenSSL Improper Restriction of Operations within the Bounds of a Memory Buffer Vulnerability

The dtls1_buffer_record function in ssl/d1_pkt.c in OpenSSL 0.9.8k and earlier 0.9.8 versions allows remote attackers to cause a denial of service (memory consumption) via a large series of "future epoch" DTLS records that are buffered in a queue, aka "DTLS record buffer limitation bug."

Affected Versions
0.9.2b to 0.9.8k

External References
- CVE-2009-1377

OpenSSL Cryptographic Issues Vulnerability

OpenSSL before 0.9.8y, 1.0.0 before 1.0.0k, and 1.0.1 before 1.0.1d does not properly perform signature verification for OCSP responses, which allows remote OCSP servers to cause a denial of service (NULL pointer dereference and application crash) via an invalid key.

Affected Versions
0.9.2b to 0.9.8x

External References
- CVE-2013-0166

OpenSSL DEPRECATED: Code Vulnerability

The ASN1_TYPE_cmp function in crypto/asn1/a_type.c in OpenSSL before 0.9.8zf, 1.0.0 before 1.0.0r, 1.0.1 before 1.0.1m, and 1.0.2 before 1.0.2a does not properly perform boolean-type comparisons, which allows remote attackers to cause a denial of service (invalid read operation and application crash) via a crafted X.509 certificate to an endpoint that uses the certificate-verification feature.

Affected Versions

0.9.2b to 0.9.8ze

External References

- CVE-2015-0286

OpenSSL DEPRECATED: Code Vulnerability

The ASN1_item_ex_d2i function in crypto/asn1/tasn_dec.c in OpenSSL before 0.9.8zf, 1.0.0 before 1.0.0r, 1.0.1 before 1.0.1m, and 1.0.2 before 1.0.2a does not reinitialize CHOICE and ADB data structures, which might allow attackers to cause a denial of service (invalid write operation and memory corruption) by leveraging an application that relies on ASN.1 structure reuse.

Affected Versions

0.9.2b to 0.9.8ze

External References

- CVE-2015-0287

OpenSSL Other Vulnerability

The X509_to_X509_REQ function in crypto/x509/x509_req.c in OpenSSL before 0.9.8zf, 1.0.0 before 1.0.0r, 1.0.1 before 1.0.1m, and 1.0.2 before 1.0.2a might allow attackers to cause a denial of service (NULL pointer dereference and application crash) via an invalid certificate key.

Affected Versions

0.9.2b to 0.9.8ze

External References

- CVE-2015-0288

OpenSSL Other Vulnerability

The PKCS#7 implementation in OpenSSL before 0.9.8zf, 1.0.0 before 1.0.0r, 1.0.1 before 1.0.1m, and 1.0.2 before 1.0.2a does not properly handle a lack of outer ContentInfo, which allows attackers to cause a denial of service (NULL pointer dereference and application crash) by leveraging an application that processes arbitrary PKCS#7 data and providing malformed data with ASN.1 encoding, related to crypto/pkcs7/pk7_doit.c and crypto/pkcs7/pk7_lib.c.

Affected Versions

0.9.2b to 0.9.8ze

External References

- CVE-2015-0289

OpenSSL Improper Restriction of Operations within the Bounds of a Memory Buffer Vulnerability

Integer underflow in the EVP_DecodeUpdate function in crypto/evp/encode.c in the base64-decoding implementation in OpenSSL before 0.9.8za, 1.0.0 before 1.0.0m, and 1.0.1 before 1.0.1h allows remote attackers to cause a denial of service (memory corruption) or possibly have unspecified other impact via crafted base64 data that triggers a buffer overflow.

Affected Versions

0.9.2b to 0.9.8z

External References

- CVE-2015-0292

OpenSSL Cryptographic Issues Vulnerability

OpenSSL before 0.9.8zd, 1.0.0 before 1.0.0p, and 1.0.1 before 1.0.1k does not enforce certain constraints on certificate data, which allows remote attackers to defeat a fingerprint-based certificate-blacklist protection mechanism by including crafted data within a certificate's unsigned portion, related to crypto/asn1/a_verify.c, crypto/dsa/dsa_asn1.c, crypto/ecdsa/ecs_vrf.c, and crypto/x509/x_all.c.

Affected Versions
0.9.2b to 0.9.8zc

External References
- CVE-2014-8275

OpenSSL Cryptographic Issues Vulnerability

The ssl3_get_key_exchange function in s3_clnt.c in OpenSSL before 0.9.8zd, 1.0.0 before 1.0.0p, and 1.0.1 before 1.0.1k allows remote SSL servers to conduct RSA-to-EXPORT_RSA downgrade attacks and facilitate brute-force decryption by offering a weak ephemeral RSA key in a noncompliant role, related to the "FREAK" issue. NOTE: the scope of this CVE is only client code based on OpenSSL, not EXPORT_RSA issues associated with servers or other TLS implementations.

Affected Versions
0.9.2b to 0.9.8zc

External References
- CVE-2015-0204

OpenSSL Other Vulnerability

Use-after-free vulnerability in the d2i_ECPrivateKey function in crypto/ec/ec_asn1.c in OpenSSL before 0.9.8zf, 1.0.0 before 1.0.0r, 1.0.1 before 1.0.1m, and 1.0.2 before 1.0.2a might allow remote attackers to cause a denial of service (memory corruption and application crash) or possibly have unspecified other impact via a malformed Elliptic Curve (EC) private-key file that is improperly handled during import.

Affected Versions
0.9.2b to 0.9.8ze

External References
- CVE-2015-0209

OpenSSL Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition') Vulnerability

Race condition in the ssl3_get_new_session_ticket function in ssl/s3_clnt.c in OpenSSL before 0.9.8zg, 1.0.0 before 1.0.0s, 1.0.1 before 1.0.1n, and 1.0.2 before 1.0.2b, when used for a multi-threaded client, allows remote attackers to cause a denial of service (double free and application crash) or possibly have unspecified other impact by providing a NewSessionTicket during an attempt to reuse a ticket that had been obtained earlier.

Affected Versions
0.9.2b to 0.9.8zf

External References
- CVE-2015-1791

OpenSSL Exposure of Sensitive Information to an Unauthorized Actor Vulnerability

The ASN1_TFLG_COMBINE implementation in crypto/asn1/tasn_dec.c in OpenSSL before 0.9.8zh, 1.0.0 before 1.0.0t, 1.0.1 before

1.0.1q, and 1.0.2 before 1.0.2e mishandles errors caused by malformed X509_ATTRIBUTE data, which allows remote attackers to obtain sensitive information from process memory by triggering a decoding failure in a PKCS#7 or CMS application.

Affected Versions
0.9.2b to 0.9.8zg

External References
- CVE-2015-3195

OpenSSL Improper Input Validation Vulnerability

The SSLv2 implementation in OpenSSL before 0.9.8zf, 1.0.0 before 1.0.0r, 1.0.1 before 1.0.1m, and 1.0.2 before 1.0.2a allows remote attackers to cause a denial of service (s2_lib.c assertion failure and daemon exit) via a crafted CLIENT-MASTER-KEY message.

Affected Versions
0.9.2b to 0.9.8ze

External References
- CVE-2015-0293

OpenSSL Improper Restriction of Operations within the Bounds of a Memory Buffer Vulnerability

The dtls1_clear_queues function in ssl/d1_lib.c in OpenSSL before 0.9.8za, 1.0.0 before 1.0.0m, and 1.0.1 before 1.0.1h frees data structures without considering that application data can arrive between a ChangeCipherSpec message and a Finished message, which allows remote DTLS peers to cause a denial of service (memory corruption and application crash) or possibly have unspecified other impact via unexpected application data.

Affected Versions
0.9.2b to 0.9.8z

External References
- CVE-2014-8176

OpenSSL Resource Management Errors Vulnerability

The BN_GF2m_mod_inv function in crypto/bn/bn_gf2m.c in OpenSSL before 0.9.8s, 1.0.0 before 1.0.0e, 1.0.1 before 1.0.1n, and 1.0.2 before 1.0.2b does not properly handle ECParameters structures in which the curve is over a malformed binary polynomial field, which allows remote attackers to cause a denial of service (infinite loop) via a session that uses an Elliptic Curve algorithm, as demonstrated by an attack against a server that supports client authentication.

Affected Versions
0.9.2b to 0.9.8zf

External References
- CVE-2015-1788

OpenSSL Improper Restriction of Operations within the Bounds of a Memory Buffer Vulnerability

The X509_cmp_time function in crypto/x509/x509_vfy.c in OpenSSL before 0.9.8zg, 1.0.0 before 1.0.0s, 1.0.1 before 1.0.1n, and 1.0.2 before 1.0.2b allows remote attackers to cause a denial of service (out-of-bounds read and application crash) via a crafted length field in ASN1_TIME data, as demonstrated by an attack against a server that supports client authentication with a custom verification callback.

Affected Versions

0.9.2b to 0.9.8zf

External References

- CVE-2015-1789

OpenSSL Other Vulnerability

The PKCS7_dataDecodefunction in crypto/pkcs7/pk7_doit.c in OpenSSL before 0.9.8zg, 1.0.0 before 1.0.0s, 1.0.1 before 1.0.1n, and 1.0.2 before 1.0.2b allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via a PKCS#7 blob that uses ASN.1 encoding and lacks inner EncryptedContent data.

Affected Versions

0.9.2b to 0.9.8zf

External References

- CVE-2015-1790

OpenSSL Cryptographic Issues Vulnerability

The ssl3_get_key_exchange function in s3_clnt.c in OpenSSL before 0.9.8zd, 1.0.0 before 1.0.0p, and 1.0.1 before 1.0.1k allows remote SSL servers to conduct ECDHE-to-ECDH downgrade attacks and trigger a loss of forward secrecy by omitting the ServerKeyExchange message.

Affected Versions

0.9.2b to 0.9.8zc

External References

- CVE-2014-3572

OpenSSL Improper Restriction of Operations within the Bounds of a Memory Buffer Vulnerability

The dtls1_reassemble_fragment function in d1_both.c in OpenSSL before 0.9.8za, 1.0.0 before 1.0.0m, and 1.0.1 before 1.0.1h does not properly validate fragment lengths in DTLS ClientHello messages, which allows remote attackers to execute arbitrary code or cause a denial of service (buffer overflow and application crash) via a long non-initial fragment.

Affected Versions

0.9.2b to 0.9.8y

External References

- CVE-2014-0195

OpenSSL Improper Restriction of Operations within the Bounds of a Memory Buffer Vulnerability

The dtls1_reassemble_fragment function in d1_both.c in OpenSSL before 0.9.8za, 1.0.0 before 1.0.0m, and 1.0.1 before 1.0.1h does not properly validate fragment lengths in DTLS ClientHello messages, which allows remote attackers to execute arbitrary code or cause a denial of service (buffer overflow and application crash) via a long non-initial fragment.

Affected Versions

0.9.8 to 0.9.8x

External References

- CVE-2014-0195

OpenSSL Resource Management Errors Vulnerability

The dtls1_get_message_fragment function in d1_both.c in OpenSSL before 0.9.8za, 1.0.0 before 1.0.0m, and 1.0.1 before 1.0.1h allows remote attackers to cause a denial of service (recursion and client crash) via a DTLS hello message in an invalid DTLS handshake.

Affected Versions
0.9.2b to 0.9.8y

External References
- CVE-2014-0221

OpenSSL Resource Management Errors Vulnerability

The dtls1_get_message_fragment function in d1_both.c in OpenSSL before 0.9.8za, 1.0.0 before 1.0.0m, and 1.0.1 before 1.0.1h allows remote attackers to cause a denial of service (recursion and client crash) via a DTLS hello message in an invalid DTLS handshake.

Affected Versions
0.9.8 to 0.9.8x

External References
- CVE-2014-0221

OpenSSL Inadequate Encryption Strength Vulnerability

OpenSSL before 0.9.8za, 1.0.0 before 1.0.0m, and 1.0.1 before 1.0.1h does not properly restrict processing of ChangeCipherSpec messages, which allows man-in-the-middle attackers to trigger use of a zero-length master key in certain OpenSSL-to-OpenSSL communications, and consequently hijack sessions or obtain sensitive information, via a crafted TLS handshake, aka the "CCS Injection" vulnerability.

Affected Versions
0.9.2b to 0.9.8z

External References
- CVE-2014-0224

OpenSSL Cryptographic Issues Vulnerability

The ssl3_send_client_key_exchange function in s3_clnt.c in OpenSSL before 0.9.8za, 1.0.0 before 1.0.0m, and 1.0.1 before 1.0.1h, when an anonymous ECDH cipher suite is used, allows remote attackers to cause a denial of service (NULL pointer dereference and client crash) by triggering a NULL certificate value.

Affected Versions
0.9.2b to 0.9.8y

External References
- CVE-2014-3470

OpenSSL Cryptographic Issues Vulnerability

The ssl3_send_client_key_exchange function in s3_clnt.c in OpenSSL before 0.9.8za, 1.0.0 before 1.0.0m, and 1.0.1 before 1.0.1h, when an anonymous ECDH cipher suite is used, allows remote attackers to cause a denial of service (NULL pointer dereference and client crash) by triggering a NULL certificate value.

Affected Versions
0.9.8 to 0.9.8x

External References

- CVE-2014-3470

OpenSSL Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition') Vulnerability

Race condition in the ssl3_read_bytes function in s3_pkt.c in OpenSSL through 1.0.1g, when SSL_MODE_RELEASE_BUFFERS is enabled, allows remote attackers to inject data across sessions or cause a denial of service (use-after-free and parsing error) via an SSL connection in a multithreaded environment.

Affected Versions

0.9.2b to 0.9.8y

External References

- CVE-2010-5298

OpenSSL Cryptographic Issues Vulnerability

The TLS protocol 1.1 and 1.2 and the DTLS protocol 1.0 and 1.2, as used in OpenSSL, OpenJDK, PolarSSL, and other products, do not properly consider timing side-channel attacks on a MAC check requirement during the processing of malformed CBC padding, which allows remote attackers to conduct distinguishing attacks and plaintext-recovery attacks via statistical analysis of timing data for crafted packets, aka the "Lucky Thirteen" issue.

Affected Versions

0.9.8 to 0.9.8x

External References

- CVE-2013-0169

OpenSSL Cryptographic Issues Vulnerability

The ssl_get_algorithm2 function in ssl/s3_lib.c in OpenSSL before 1.0.2 obtains a certain version number from an incorrect data structure, which allows remote attackers to cause a denial of service (daemon crash) via crafted traffic from a TLS 1.2 client.

Affected Versions

0.9.2b to 0.9.8zh

External References

- CVE-2013-6449

OpenSSL Cryptographic Issues Vulnerability

The Montgomery ladder implementation in OpenSSL through 1.0.0l does not ensure that certain swap operations have a constant-time behavior, which makes it easier for local users to obtain ECDSA nonces via a FLUSH+RELOAD cache side-channel attack.

Affected Versions

0.9.2b to 0.9.8zh

External References

- CVE-2014-0076

OpenSSL Cryptographic Issues Vulnerability

The Montgomery ladder implementation in OpenSSL through 1.0.0l does not ensure that certain swap operations have a constant-time behavior, which makes it easier for local users to obtain ECDSA nonces via a FLUSH+RELOAD cache side-channel attack.

Affected Versions
0.9.2b to 0.9.8y

External References
- CVE-2014-0076

OpenSSL Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition') Vulnerability

Race condition in the ssl3_read_bytes function in s3_pkt.c in OpenSSL through 1.0.1g, when SSL_MODE_RELEASE_BUFFERS is enabled, allows remote attackers to inject data across sessions or cause a denial of service (use-after-free and parsing error) via an SSL connection in a multithreaded environment.

Affected Versions
0.9.2b to 0.9.8zh

External References
- CVE-2010-5298

OpenSSL Other Vulnerability

Double free vulnerability in d1_both.c in the DTLS implementation in OpenSSL 0.9.8 before 0.9.8zb, 1.0.0 before 1.0.0n, and 1.0.1 before 1.0.1i allows remote attackers to cause a denial of service (application crash) via crafted DTLS packets that trigger an error condition.

Affected Versions
0.9.8 to 0.9.8y

External References
- CVE-2014-3505

OpenSSL Improper Input Validation Vulnerability

Memory leak in the tls_decrypt_ticket function in t1_lib.c in OpenSSL before 0.9.8zc, 1.0.0 before 1.0.0o, and 1.0.1 before 1.0.1j allows remote attackers to cause a denial of service (memory consumption) via a crafted session ticket that triggers an integrity-check failure.

Affected Versions
0.9.2b to 0.9.8zb

External References
- CVE-2014-3567

OpenSSL Cryptographic Issues Vulnerability

OpenSSL before 0.9.8zc, 1.0.0 before 1.0.0o, and 1.0.1 before 1.0.1j does not properly enforce the no-ssl3 build option, which allows remote attackers to bypass intended access restrictions via an SSL 3.0 handshake, related to s23_clnt.c and s23_srvr.c.

Affected Versions
0.9.2b to 0.9.8zb

External References
- CVE-2014-3568

OpenSSL Cryptographic Issues Vulnerability

The BN_sqr implementation in OpenSSL before 0.9.8zd, 1.0.0 before 1.0.0p, and 1.0.1 before 1.0.1k does not properly calculate the

square of a BIGNUM value, which might make it easier for remote attackers to defeat cryptographic protection mechanisms via unspecified vectors, related to crypto/bn/asm/mips.pl, crypto/bn/asm/x86_64-gcc.c, and crypto/bn/bn_asm.c.

Affected Versions
0.9.2b to 0.9.8zc

External References
- CVE-2014-3570

OpenSSL Other Vulnerability

OpenSSL before 0.9.8zd, 1.0.0 before 1.0.0p, and 1.0.1 before 1.0.1k allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via a crafted DTLS message that is processed with a different read operation for the handshake header than for the handshake body, related to the dtls1_get_record function in d1_pkt.c and the ssl3_read_n function in s3_pkt.c.

Affected Versions
0.9.2b to 0.9.8zc

External References
- CVE-2014-3571

OpenSSL Resource Management Errors Vulnerability

d1_both.c in the DTLS implementation in OpenSSL 0.9.8 before 0.9.8zb, 1.0.0 before 1.0.0n, and 1.0.1 before 1.0.1i allows remote attackers to cause a denial of service (memory consumption) via crafted DTLS handshake messages that trigger memory allocations corresponding to large length values.

Affected Versions
0.9.8 to 0.9.8y

External References
- CVE-2014-3506

OpenSSL Resource Management Errors Vulnerability

Memory leak in d1_both.c in the DTLS implementation in OpenSSL 0.9.8 before 0.9.8zb, 1.0.0 before 1.0.0n, and 1.0.1 before 1.0.1i allows remote attackers to cause a denial of service (memory consumption) via zero-length DTLS fragments that trigger improper handling of the return value of a certain insert function.

Affected Versions
0.9.8 to 0.9.8y

External References
- CVE-2014-3507

OpenSSL Exposure of Sensitive Information to an Unauthorized Actor Vulnerability

The OBJ_obj2txt function in crypto/objects/obj_dat.c in OpenSSL 0.9.8 before 0.9.8zb, 1.0.0 before 1.0.0n, and 1.0.1 before 1.0.1i, when pretty printing is used, does not ensure the presence of '\0' characters, which allows context-dependent attackers to obtain sensitive information from process stack memory by reading output from X509_name_oneline, X509_name_print_ex, and unspecified other functions.

Affected Versions
0.9.8 to 0.9.8y

External References

- CVE-2014-3508

OpenSSL Other Vulnerability

The ssl3_send_client_key_exchange function in s3_clnt.c in OpenSSL 0.9.8 before 0.9.8zb, 1.0.0 before 1.0.0n, and 1.0.1 before 1.0.1i allows remote DTLS servers to cause a denial of service (NULL pointer dereference and client application crash) via a crafted handshake message in conjunction with a (1) anonymous DH or (2) anonymous ECDH ciphersuite.

Affected Versions

0.9.8 to 0.9.8y

External References

- CVE-2014-3510

OpenSSL Key Management Errors Vulnerability

A timing attack flaw was found in OpenSSL 1.0.1u and before that could allow a malicious user with local access to recover ECDSA P-256 private keys.

Affected Versions

0.9.2b to 0.9.8zh

External References

- CVE-2016-7056

OpenSSL Improper Restriction of Operations within the Bounds of a Memory Buffer Vulnerability

While parsing an IPAddressFamily extension in an X.509 certificate, it is possible to do a one-byte overread. This would result in an incorrect text display of the certificate. This bug has been present since 2006 and is present in all versions of OpenSSL before 1.0.2m and 1.1.0g.

Affected Versions

0.9.7j to 0.9.8zc

External References

- CVE-2017-3735

OpenSSL Exposure of Sensitive Information to an Unauthorized Actor Vulnerability

The get_client_master_key function in s2_srvr.c in the SSLv2 implementation in OpenSSL before 0.9.8zf, 1.0.0 before 1.0.0r, 1.0.1 before 1.0.1m, and 1.0.2 before 1.0.2a accepts a nonzero CLIENT-MASTER-KEY CLEAR-KEY-LENGTH value for an arbitrary cipher, which allows man-in-the-middle attackers to determine the MASTER-KEY value and decrypt TLS ciphertext data by leveraging a Bleichenbacher RSA padding oracle, a related issue to CVE-2016-0800.

Affected Versions

0.9.2b to 0.9.8ze

External References

- CVE-2016-0703

OpenSSL Exposure of Sensitive Information to an Unauthorized Actor Vulnerability

An oracle protection mechanism in the get_client_master_key function in s2_srvr.c in the SSLv2 implementation in OpenSSL before

0.9.8zf, 1.0.0 before 1.0.0r, 1.0.1 before 1.0.1m, and 1.0.2 before 1.0.2a overwrites incorrect MASTER-KEY bytes during use of export cipher suites, which makes it easier for remote attackers to decrypt TLS ciphertext data by leveraging a Bleichenbacher RSA padding oracle, a related issue to CVE-2016-0800.

Affected Versions
0.9.2b to 0.9.8ze

External References
- CVE-2016-0704

OpenSSL Numeric Errors Vulnerability

Integer overflow in the EVP_EncryptUpdate function in crypto/evp/evp_enc.c in OpenSSL before 1.0.1t and 1.0.2 before 1.0.2h allows remote attackers to cause a denial of service (heap memory corruption) via a large amount of data.

Affected Versions
0.9.2b to 0.9.8zh

External References
- CVE-2016-2106

OpenSSL Exposure of Sensitive Information to an Unauthorized Actor Vulnerability

The AES-NI implementation in OpenSSL before 1.0.1t and 1.0.2 before 1.0.2h does not consider memory allocation during a certain padding check, which allows remote attackers to obtain sensitive cleartext information via a padding-oracle attack against an AES CBC session. NOTE: this vulnerability exists because of an incorrect fix for CVE-2013-0169.

Affected Versions
0.9.2b to 0.9.8zh

External References
- CVE-2016-2107

OpenSSL Improper Restriction of Operations within the Bounds of a Memory Buffer Vulnerability

The ASN.1 implementation in OpenSSL before 1.0.1o and 1.0.2 before 1.0.2c allows remote attackers to execute arbitrary code or cause a denial of service (buffer underflow and memory corruption) via an ANY field in crafted serialized data, aka the "negative zero" issue.

Affected Versions
0.9.2b to 0.9.8zh

External References
- CVE-2016-2108

OpenSSL Resource Management Errors Vulnerability

The asn1_d2i_read_bio function in crypto/asn1/a_d2i_fp.c in the ASN.1 BIO implementation in OpenSSL before 1.0.1t and 1.0.2 before 1.0.2h allows remote attackers to cause a denial of service (memory consumption) via a short invalid encoding.

Affected Versions
0.9.2b to 0.9.8zh

External References

- CVE-2016-2109

OpenSSL Improper Restriction of Operations within the Bounds of a Memory Buffer Vulnerability

The X509_NAME_oneline function in crypto/x509/x509_obj.c in OpenSSL before 1.0.1t and 1.0.2 before 1.0.2h allows remote attackers to obtain sensitive information from process stack memory or cause a denial of service (buffer over-read) via crafted EBCDIC ASN.1 data.

Affected Versions
0.9.2b to 0.9.8zh

External References
- CVE-2016-2176

Vulnerabilities

2.1. https://zero.webappsecurity.com/

Identified Version
- 0.9.8e

Latest Version
- 3.1.1 (in this branch)

Vulnerability Database
- Result is based on 07/27/2023 20:30:00 vulnerability database content.

Certainty

Request

```
GET / HTTP/1.1
Host: zero.webappsecurity.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: JSESSIONID=5CF19C3A
Referer: https://zero.webappsecurity.com/
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.
77 Safari/537.36
X-Scanner: Netsparker
```

Response

Response Time (ms) : 191.9997 Total Bytes Received : 345 Body Length : 44 Is Compressed : No

```
HTTP/1.1 200 OK
Content-Type: text/html
Server: Apache/2.2.6 (Win32) mod_ssl/2.2.6 OpenSSL/0.9.8e mod_jk/1.2.40

Content-Length: 44
Last-Modified: Sat, 20 Nov 2004 14:16:24 GMT
Accept-Ranges: bytes
Access-Control-Allow-Origin: *
Date: Sun, 30 Jul 2023 06:09:00 GMT
ETag: "24c22-2c-44adde00"

<html><body><h1>It works!</h1></body></html>
```

Remedy

Please upgrade your installation of OpenSSL to the latest stable version.

Remedy References

- OpenSSL Project

CLASSIFICATION

PCI DSS v3.2	6.2
OWASP 2013	A9
OWASP 2017	A9
CWE	829
CAPEC	310
HIPAA	164.308(A)(1)(I)
OWASP Proactive Controls	C1
ISO27001	A.14.1.2

3. Out-of-date Version (Tomcat)

CRITICAL 1

Netsparker identified you are using an out-of-date version of Tomcat.

Apache Tomcat Use of Incorrectly-Resolved Name or Reference Vulnerability

When serving resources from a network location using the NTFS file system, Apache Tomcat versions 10.0.0-M1 to 10.0.0-M9, 9.0.0.M1 to 9.0.39, 8.5.0 to 8.5.59 and 7.0.0 to 7.0.106 were susceptible to JSP source code disclosure in some configurations. The root cause was the unexpected behaviour of the JRE API File.getCanonicalPath() which in turn was caused by the inconsistent behaviour of the Windows API (FindFirstFileW) in some circumstances.

Affected Versions
7.0.0 to 7.0.106

External References
- CVE-2021-24122

Apache Tomcat CVE-2019-2684 Vulnerability

Vulnerability in the Java SE, Java SE Embedded component of Oracle Java SE (subcomponent: RMI). Supported versions that are affected are Java SE: 7u211, 8u202, 11.0.2 and 12; Java SE Embedded: 8u201. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Java SE, Java SE Embedded accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.0 Base Score 5.9 (Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:H/A:N).

Affected Versions
7.0.0 to 7.0.97

External References
- CVE-2019-2684

Apache Tomcat Improper Privilege Management Vulnerability

When using the Apache JServ Protocol (AJP), care must be taken when trusting incoming connections to Apache Tomcat. Tomcat treats AJP connections as having higher trust than, for example, a similar HTTP connection. If such connections are available to an attacker, they can be exploited in ways that may be surprising. In Apache Tomcat 9.0.0.M1 to 9.0.0.30, 8.5.0 to 8.5.50 and 7.0.0 to 7.0.99, Tomcat shipped with an AJP Connector enabled by default that listened on all configured IP addresses. It was expected (and recommended in the security guide) that this Connector would be disabled if not required. This vulnerability report identified a mechanism that allowed: - returning arbitrary files from anywhere in the web application - processing any file in the web application as a JSP Further, if the web application allowed file upload and stored those files within the web application (or the attacker was able to control the content of the web application by some other means) then this, along with the ability to process a file as a JSP, made remote code execution possible. It is important to note that mitigation is only required if an AJP port is accessible to untrusted users. Users wishing to take a defence-in-depth approach and block the vector that permits returning arbitrary files and execution as JSP may upgrade to Apache Tomcat 9.0.31, 8.5.51 or 7.0.100 or later. A number of changes were made to the default AJP Connector configuration in 9.0.31 to harden the default configuration. It is likely that users upgrading to 9.0.31, 8.5.51 or 7.0.100 or later will need to make small changes to their configurations.

Affected Versions
7.0.0 to 7.0.99

External References
- CVE-2020-1938

Apache Tomcat CVE-2016-5018 Vulnerability

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.

Affected Versions
7.0.0 to 7.0.70

External References
- CVE-2016-5018

Apache Tomcat CVE-2016-6796 Vulnerability

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.

Affected Versions
7.0.0 to 7.0.70

External References
- CVE-2016-6796

Apache Tomcat Incorrect Authorization Vulnerability

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.

Affected Versions
7.0.0 to 7.0.70

External References
- CVE-2016-6797

Apache Tomcat Improper Encoding or Escaping of Output Vulnerability

A vulnerability in the JNDI Realm of Apache Tomcat allows an attacker to authenticate using variations of a valid user name and/or to bypass some of the protection provided by the LockOut Realm. This issue affects Apache Tomcat 10.0.0-M1 to 10.0.5; 9.0.0.M1 to 9.0.45; 8.5.0 to 8.5.65.

Affected Versions
7.0.0 to 7.0.108

External References
- CVE-2021-30640

Apache Tomcat Deserialization of Untrusted Data Vulnerability

The fix for CVE-2020-9484 was incomplete. When using Apache Tomcat 10.0.0-M1 to 10.0.0, 9.0.0.M1 to 9.0.41, 8.5.0 to 8.5.61 or 7.0.0. to 7.0.107 with a configuration edge case that was highly unlikely to be used, the Tomcat instance was still vulnerable to CVE-2020-9494. Note that both the previously published prerequisites for CVE-2020-9484 and the previously published mitigations for CVE-2020-9484 also apply to this issue.

Affected Versions
7.0.0 to 7.0.107

External References
- CVE-2021-25329

Apache Tomcat Improper Access Control Vulnerability

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.

Affected Versions
7.0 to 7.0.70

External References
- CVE-2016-5388

Apache Tomcat Improper Access Control Vulnerability

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.

Affected Versions
7.0.0 to 7.0.72

External References
- CVE-2016-8735

Apache Tomcat Permissions, Privileges, and Access Controls Vulnerability

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.

Affected Versions
7.0.52 to 7.0.70

External References
- CVE-2016-0762

Apache Tomcat Inconsistent Interpretation of HTTP Requests ('HTTP Request Smuggling') Vulnerability

In Apache Tomcat 9.0.0.M1 to 9.0.30, 8.5.0 to 8.5.50 and 7.0.0 to 7.0.99 the HTTP header parsing code used an approach to end-of-line parsing that allowed some invalid HTTP headers to be parsed as valid. This led to a possibility of HTTP Request Smuggling if Tomcat

was located behind a reverse proxy that incorrectly handled the invalid Transfer-Encoding header in a particular manner. Such a reverse proxy is considered unlikely.

Affected Versions
7.0.0 to 7.0.99

External References
- CVE-2020-1935

Apache Tomcat Deserialization of Untrusted Data Vulnerability

When using Apache Tomcat versions 10.0.0-M1 to 10.0.0-M4, 9.0.0.M1 to 9.0.34, 8.5.0 to 8.5.54 and 7.0.0 to 7.0.103 if a) an attacker is able to control the contents and name of a file on the server; and b) the server is configured to use the PersistenceManager with a FileStore; and c) the PersistenceManager is configured with sessionAttributeValueClassNameFilter="null" (the default unless a SecurityManager is used) or a sufficiently lax filter to allow the attacker provided object to be deserialized; and d) the attacker knows the relative file path from the storage location used by FileStore to the file the attacker has control over; then, using a specifically crafted request, the attacker will be able to trigger remote code execution via deserialization of the file under their control. Note that all of conditions a) to d) must be true for the attack to succeed.

Affected Versions
7.0.0 to 7.0.100

External References
- CVE-2020-9484

Apache Tomcat Loop with Unreachable Exit Condition ('Infinite Loop') Vulnerability

The payload length in a WebSocket frame was not correctly validated in Apache Tomcat 10.0.0-M1 to 10.0.0-M6, 9.0.0.M1 to 9.0.36, 8.5.0 to 8.5.56 and 7.0.27 to 7.0.104. Invalid payload lengths could trigger an infinite loop. Multiple requests with invalid payload lengths could lead to a denial of service.

Affected Versions
7.0.27 to 7.0.100

External References
- CVE-2020-13935

Apache Tomcat Insufficiently Protected Credentials Vulnerability

When Apache Tomcat 9.0.0.M1 to 9.0.28, 8.5.0 to 8.5.47, 7.0.0 and 7.0.97 is configured with the JMX Remote Lifecycle Listener, a local attacker without access to the Tomcat process or configuration files is able to manipulate the RMI registry to perform a man-in-the-middle attack to capture user names and passwords used to access the JMX interface. The attacker can then use these credentials to access the JMX interface and gain complete control over the Tomcat instance.

Affected Versions
7.0.0 to 7.0.97

External References
- CVE-2019-12418

Apache Tomcat Session Fixation Vulnerability

When using FORM authentication with Apache Tomcat 9.0.0.M1 to 9.0.29, 8.5.0 to 8.5.49 and 7.0.0 to 7.0.98 there was a narrow window where an attacker could perform a session fixation attack. The window was considered too narrow for an exploit to be

practical but, erring on the side of caution, this issue has been treated as a security vulnerability.

Affected Versions
7.0.0 to 7.0.98

External References
- CVE-2019-17563

Apache Tomcat 7PK - Errors Vulnerability

A bug in the error handling of the send file code for the NIO HTTP connector in Apache Tomcat 9.0.0.M1 to 9.0.0.M13, 8.5.0 to 8.5.8, 8.0.0.RC1 to 8.0.39, 7.0.0 to 7.0.73 and 6.0.16 to 6.0.48 resulted in the current Processor object being added to the Processor cache multiple times. This in turn meant that the same Processor could be used for concurrent requests. Sharing a Processor can result in information leakage between requests including, not not limited to, session ID and the response body. The bug was first noticed in 8.5.x onwards where it appears the refactoring of the Connector code for 8.5.x onwards made it more likely that the bug was observed. Initially it was thought that the 8.5.x refactoring introduced the bug but further investigation has shown that the bug is present in all currently supported Tomcat versions.

Affected Versions
7.0.52 to 7.0.73

External References
- CVE-2016-8745

Apache Tomcat Insufficient Verification of Data Authenticity Vulnerability

The CORS Filter in Apache Tomcat 9.0.0.M1 to 9.0.0.M21, 8.5.0 to 8.5.15, 8.0.0.RC1 to 8.0.44 and 7.0.41 to 7.0.78 did not add an HTTP Vary header indicating that the response varies depending on Origin. This permitted client and server side cache poisoning in some circumstances.

Affected Versions
7.0.52 to 7.0.78

External References
- CVE-2017-7674

Apache Tomcat URL Redirection to Untrusted Site ('Open Redirect') Vulnerability

When the default servlet in Apache Tomcat versions 9.0.0.M1 to 9.0.11, 8.5.0 to 8.5.33 and 7.0.23 to 7.0.90 returned a redirect to a directory (e.g. redirecting to '/foo/' when the user requested '/foo') a specially crafted URL could be used to cause the redirect to be generated to any URI of the attackers choice.

Affected Versions
7.0.23 to 7.0.90

External References
- CVE-2018-11784

Apache Tomcat Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') Vulnerability

The SSI printenv command in Apache Tomcat 9.0.0.M1 to 9.0.0.17, 8.5.0 to 8.5.39 and 7.0.0 to 7.0.93 echoes user provided data without escaping and is, therefore, vulnerable to XSS. SSI is disabled by default. The printenv command is intended for debugging and is unlikely to be present in a production website.

Affected Versions
7.0.0 to 7.0.93

External References
- CVE-2019-0221

Apache Tomcat Loop with Unreachable Exit Condition ('Infinite Loop') Vulnerability

An improper handing of overflow in the UTF-8 decoder with supplementary characters can lead to an infinite loop in the decoder causing a Denial of Service. Versions Affected: Apache Tomcat 9.0.0.M9 to 9.0.7, 8.5.0 to 8.5.30, 8.0.0.RC1 to 8.0.51, and 7.0.28 to 7.0.86.

Affected Versions
7.0.28 to 7.0.86

External References
- CVE-2018-1336

Apache Tomcat Exposure of Sensitive Information to an Unauthorized Actor Vulnerability

When using a VirtualDirContext with Apache Tomcat 7.0.0 to 7.0.80 it was possible to bypass security constraints and/or view the source code of JSPs for resources served by the VirtualDirContext using a specially crafted request.

Affected Versions
7.0.54 to 7.0.77

External References
- CVE-2017-12616

Apache Tomcat CVE-2018-1305 Vulnerability

Security constraints defined by annotations of Servlets in Apache Tomcat 9.0.0.M1 to 9.0.4, 8.5.0 to 8.5.27, 8.0.0.RC1 to 8.0.49 and 7.0.0 to 7.0.84 were only applied once a Servlet had been loaded. Because security constraints defined in this way apply to the URL pattern and any URLs below that point, it was possible - depending on the order Servlets were loaded - for some security constraints not to be applied. This could have exposed resources to users who were not authorised to access them.

Affected Versions
7.0.0 to 7.0.84

External References
- CVE-2018-1305

Apache Tomcat CVE-2018-1304 Vulnerability

The URL pattern of "" (the empty string) which exactly maps to the context root was not correctly handled in Apache Tomcat 9.0.0.M1 to 9.0.4, 8.5.0 to 8.5.27, 8.0.0.RC1 to 8.0.49 and 7.0.0 to 7.0.84 when used as part of a security constraint definition. This caused the constraint to be ignored. It was, therefore, possible for unauthorised users to gain access to web application resources that should have been protected. Only security constraints with a URL pattern of the empty string were affected.

Affected Versions
7.0.0 to 7.0.84

External References
- CVE-2018-1304

Apache Tomcat Unrestricted Upload of File with Dangerous Type Vulnerability

When running Apache Tomcat versions 9.0.0.M1 to 9.0.0, 8.5.0 to 8.5.22, 8.0.0.RC1 to 8.0.46 and 7.0.0 to 7.0.81 with HTTP PUTs enabled (e.g. via setting the readonly initialisation parameter of the Default servlet to false) it was possible to upload a JSP file to the server via a specially crafted request. This JSP could then be requested and any code it contained would be executed by the server.

Affected Versions
7.0.54 to 7.0.77

External References
- CVE-2017-12617

Apache Tomcat Insecure Default Initialization of Resource Vulnerability

The defaults settings for the CORS filter provided in Apache Tomcat 9.0.0.M1 to 9.0.8, 8.5.0 to 8.5.31, 8.0.0.RC1 to 8.0.52, 7.0.41 to 7.0.88 are insecure and enable 'supportsCredentials' for all origins. It is expected that users of the CORS filter will have configured it appropriately for their environment rather than using it in the default configuration. Therefore, it is expected that most users will not be impacted by this issue.

Affected Versions
7.0.41 to 7.0.88

External References
- CVE-2018-8014

Apache Tomcat Improper Certificate Validation Vulnerability

The host name verification when using TLS with the WebSocket client was missing. It is now enabled by default. Versions Affected: Apache Tomcat 9.0.0.M1 to 9.0.9, 8.5.0 to 8.5.31, 8.0.0.RC1 to 8.0.52, and 7.0.35 to 7.0.88.

Affected Versions
7.0.35 to 7.0.88

External References
- CVE-2018-8034

Apache Tomcat Exposure of Sensitive Information to an Unauthorized Actor Vulnerability

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.

Affected Versions
7.0.0 to 7.0.76

External References
- CVE-2017-5647

Apache Tomcat Exposure of Resource to Wrong Sphere Vulnerability

While investigating bug 60718, it was noticed that some calls to application listeners in Apache Tomcat 9.0.0.M1 to 9.0.0.M17, 8.5.0 to 8.5.11, 8.0.0.RC1 to 8.0.41, and 7.0.0 to 7.0.75 did not use the appropriate facade object. When running an untrusted application under a SecurityManager, it was therefore possible for that untrusted application to retain a reference to the request or response object and

thereby access and/or modify information associated with another web application.

Affected Versions
7.0.0 to 7.0.75

External References
- CVE-2017-5648

Apache Tomcat Exposure of Sensitive Information to an Unauthorized Actor Vulnerability

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.

Affected Versions
7.0.52 to 7.0.70

External References
- CVE-2016-6794

Apache Tomcat Improper Handling of Exceptional Conditions Vulnerability

The error page mechanism of the Java Servlet Specification requires that, when an error occurs and an error page is configured for the error that occurred, the original request and response are forwarded to the error page. This means that the request is presented to the error page with the original HTTP method. If the error page is a static file, expected behaviour is to serve content of the file as if processing a GET request, regardless of the actual HTTP method. The Default Servlet in Apache Tomcat 9.0.0.M1 to 9.0.0.M20, 8.5.0 to 8.5.14, 8.0.0.RC1 to 8.0.43 and 7.0.0 to 7.0.77 did not do this. Depending on the original request this could lead to unexpected and undesirable results for static error pages including, if the DefaultServlet is configured to permit writes, the replacement or removal of the custom error page. Notes for other user provided error pages: (1) Unless explicitly coded otherwise, JSPs ignore the HTTP method. JSPs used as error pages must must ensure that they handle any error dispatch as a GET request, regardless of the actual method. (2) By default, the response generated by a Servlet does depend on the HTTP method. Custom Servlets used as error pages must ensure that they handle any error dispatch as a GET request, regardless of the actual method.

Affected Versions
7.0.54 to 7.0.77

External References
- CVE-2017-5664

Apache Tomcat Improper Input Validation Vulnerability

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.

Affected Versions
7.0.0 to 7.0.72

External References
- CVE-2016-6816

Apache Tomcat Incorrect Default Permissions Vulnerability

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.

Affected Versions

1.1.3 to 7.0.100

External References

- CVE-2020-8022

Apache Tomcat Incorrect Default Permissions Vulnerability

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.

Affected Versions

1.1.3 to 7.0.100

External References

- CVE-2020-8022

Apache Tomcat Incorrect Default Permissions Vulnerability

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.

Affected Versions
1.1.3 to 7.0.100

External References
- CVE-2020-8022

Apache Tomcat Incorrect Default Permissions Vulnerability

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.

Affected Versions
1.1.3 to 7.0.100

External References
- CVE-2020-8022

Apache Tomcat Incorrect Default Permissions Vulnerability

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.

Affected Versions
1.1.3 to 7.0.100

External References
- CVE-2020-8022

Apache Tomcat Incorrect Default Permissions Vulnerability

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.

Affected Versions
1.1.3 to 7.0.100

External References
- CVE-2020-8022

Apache Tomcat Incorrect Default Permissions Vulnerability

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.

Affected Versions
1.1.3 to 7.0.100

External References
- CVE-2020-8022

Apache Tomcat Incorrect Default Permissions Vulnerability

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.

Affected Versions
1.1.3 to 7.0.100

External References
- CVE-2020-8022

Apache Tomcat Incorrect Default Permissions Vulnerability

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.

Affected Versions
1.1.3 to 7.0.100

External References
- CVE-2020-8022

Apache Tomcat 7PK - Security Features Vulnerability

Jenkins before 1.586 does not set the secure flag on session cookies when run on Tomcat 7.0.41 or later, which makes it easier for remote attackers to capture cookies by intercepting their transmission within an HTTP session.

Affected Versions
7.0.54 to 7.0.81

External References

- CVE-2014-9634

Apache Tomcat 7PK - Security Features Vulnerability

Jenkins before 1.586 does not set the HttpOnly flag in a Set-Cookie header for session cookies when run on Tomcat 7.0.41 or later, which makes it easier for remote attackers to obtain potentially sensitive information via script access to cookies.

Affected Versions
7.0.54 to 7.0.81

External References
- CVE-2014-9635

Apache Tomcat Unrestricted Upload of File with Dangerous Type Vulnerability

When running Apache Tomcat 7.0.0 to 7.0.79 on Windows with HTTP PUTs enabled (e.g. via setting the readonly initialisation parameter of the Default to false) it was possible to upload a JSP file to the server via a specially crafted request. This JSP could then be requested and any code it contained would be executed by the server.

Affected Versions
7.0.54 to 7.0.77

External References
- CVE-2017-12615

Apache Tomcat Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') Vulnerability

When running on Windows with enableCmdLineArguments enabled, the CGI Servlet in Apache Tomcat 9.0.0.M1 to 9.0.17, 8.5.0 to 8.5.39 and 7.0.0 to 7.0.93 is vulnerable to Remote Code Execution due to a bug in the way the JRE passes command line arguments to Windows. The CGI Servlet is disabled by default. The CGI option enableCmdLineArguments is disable by default in Tomcat 9.0.x (and will be disabled by default in all versions in response to this vulnerability). For a detailed explanation of the JRE behaviour, see Markus Wulftange's blog (https://codewhitesec.blogspot.com/2016/02/java-and-command-line-injections-in-windows.html) and this archived MSDN blog (https://web.archive.org/web/20161228144344/https://blogs.msdn.microsoft.com/twistylittlepassagesallalike/2011/04/23/everyone-quotes-command-line-arguments-the-wrong-way/).

Affected Versions
7.0.0 to 7.0.93

External References
- CVE-2019-0232

Apache Tomcat Incorrect Default Permissions Vulnerability

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.

Affected Versions
1.1.3 to 7.0.100

External References
- CVE-2020-8022

Apache Tomcat Incorrect Default Permissions Vulnerability

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.

Affected Versions
1.1.3 to 7.0.100

External References
- CVE-2020-8022

Apache Tomcat Incorrect Default Permissions Vulnerability

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.

Affected Versions
1.1.3 to 7.0.100

External References

- CVE-2020-8022

Apache Tomcat Incorrect Default Permissions Vulnerability

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.

Affected Versions

1.1.3 to 7.0.100

External References

- CVE-2020-8022

Apache Tomcat CVE-2012-5568 Vulnerability

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.

Affected Versions

7.0.0 to 7.0.100

External References

- CVE-2012-5568

Vulnerabilities

3.1. http://zero.webappsecurity.com/resources/

Identified Version

- 7.0.70

Latest Version

- 10.1.11 (in this branch)

Vulnerability Database

- Result is based on 07/27/2023 20:30:00 vulnerability database content.

Certainty

Request

```
GET /resources/ HTTP/1.1
Host: zero.webappsecurity.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.
77 Safari/537.36
X-Scanner: Netsparker
```

Response

Response Time (ms) : 395.3092 **Total Bytes Received** : 1216 **Body Length** : 949 **Is Compressed** : No

```
HTTP/1.1 404 Not Found
Content-Type: text/html;charset=utf-8
Server: Apache-Coyote/1.1
Content-Length: 949
Content-Language: en
Access-Control-Allow-Origin: *
Date: Sun, 30 Jul 2023 06:08:57 GMT
Cache-Control: no-cache, max-age=0, must-revalidate, no-store

<html><head><title>Apache Tomcat/7.0.70 - Error report</title><style><!--H1 {font-family:Tahoma,Arial,s
ans-serif;color:white;background-color:#525D76;font-size:22px;} H2 {font-family:Tahoma,Arial,sans-seri
f;color:white;background-color:#525D76;font-size:16px;} H3 {font-family:Tahoma,Arial,sans-serif;color:w
hite;background-color:#525D76;font-size:14px;} BODY {font-family:Tahoma,Arial,sans-serif;color:black;ba
ckground-color:white;} B {font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;} P
 {font-family:Tahoma,Arial,sans-serif;background:white;color:black;font-size:12px;}A {color : black;}A.
name {color : black;}HR {color : #525D76;}--></style> </head><body><h1>HTTP Status 404 - </h1><HR size
="1" noshade="noshade"><p><b>type</b> Status report</p><p><b>message</b> <u></u></p><p><b>description</
b> <u>The requested resource is not available.</u></p><HR size="1" noshade="noshade"><h3>Apache Tomcat/
7.0.70</h3></body></html>
```

Remedy

Please upgrade your installation of Tomcat to the latest stable version.

Remedy References

- Apache Tomcat Versions and Download

CLASSIFICATION

PCI DSS v3.2	6.2
OWASP 2013	A9
OWASP 2017	A9
CWE	829
CAPEC	310
HIPAA	164.308(A)(1)(I)
OWASP Proactive Controls	C1
ISO27001	A.14.1.2

4. Insecure Transportation Security Protocol Supported (SSLv2)

HIGH 1 CONFIRMED 1

Netsparker detected that insecure transportation security protocol (SSLv2) is supported by your web server.

SSLv2 has several flaws. For example, your secure traffic can be observed when you have established it over SSLv2.

Impact

Attackers can perform man-in-the-middle attacks and observe the encryption traffic between your website and its visitors. Also an attacker can exploit vulnerabilities like DROWN.

Vulnerabilities

4.1. https://zero.webappsecurity.com/

CONFIRMED

Request

```
[NETSPARKER] SSL Connection
```

Response

Response Time (ms) : 1 **Total Bytes Received :** 27 **Body Length :** 0 **Is Compressed :** No

```
[NETSPARKER] SSL Connection
```

Actions to Take

We recommended to disable SSLv2 and replace it with TLS 1.2 or higher. See Remedy section for more details.

Remedy

Configure your web server to disallow using weak ciphers.

- For Apache, you should modify the SSLProtocol directive in the `httpd.conf`.

```
SSLProtocol +TLSv1.2
```

- For Nginx, locate any use of the directive ssl_protocols in the `nginx.conf` file and remove `SSLv3`.

```
ssl_protocols TLSv1.2;
```

-
- For Microsoft IIS, you should make some changes on the system registry. **Incorrectly editing the registry may severely damage your system. Before making changes to the registry, you should back up any valued data on your computer.**
    1. Click Start, click Run, type regedt32 or type regedit, and then click OK.
    2. In Registry Editor, locate the following registry key:
       HKey_Local_Machine\System\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\SSL2\
    3. Locate a key named "Server." If it doesn't exist, create it.
    4. Under the "Server" key, locate a DWORD value named "Enabled." If it doesn't exist, create it and set it to "0".
- For lighttpd, put the following lines in your configuration file:

```
ssl.use-sslv2 = "disable"
ssl.use-sslv3 = "disable"
ssl.openssl.ssl-conf-cmd = ("Protocol" => "-TLSv1.1, -TLSv1, -SSLv3") # v1.4.48 or up
ssl.ec-curve = "secp384r1"
```

External References

- OWASP - Insecure Configuration Management
- How to disable PCT 1.0, SSL 2.0, SSL 3.0, or TLS 1.0 in Internet Information Services
- OWASP Top 10-2017 A3-Sensitive Data Exposure
- The DROWN Attack

CLASSIFICATION

PCI DSS v3.2	6.5.4
OWASP 2013	A6
OWASP 2017	A3
CWE	326
CAPEC	217
WASC	4
HIPAA	164.306
ISO27001	A.14.1.3

CVSS 3.0 SCORE

Base	6.8 (Medium)
Temporal	6.1 (Medium)
Environmental	6.1 (Medium)

CVSS Vector String

CVSS:3.0/AV:A/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:N/E:P/RL:O/RC:C

CVSS 3.1 SCORE

Base	6.8 (Medium)
Temporal	6.1 (Medium)
Environmental	6.1 (Medium)

CVSS Vector String
CVSS:3.1/AV:A/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:N/E:P/RL:O/RC:C

5. Password Transmitted over HTTP

HIGH 1 CONFIRMED 1

Netsparker detected that password data is being transmitted over HTTP.

Impact

If an attacker can intercept network traffic, he/she can steal users' credentials.

Vulnerabilities

5.1. http://zero.webappsecurity.com/login.html

CONFIRMED

Input Name

- user_password

Form target action

- http://zero.webappsecurity.com/signin.html

Request

```
GET /login.html HTTP/1.1
Host: zero.webappsecurity.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Referer: http://zero.webappsecurity.com/feedback.html
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.
77 Safari/537.36
X-Scanner: Netsparker
```

Response

Response Time (ms) : 198.3096 **Total Bytes Received** : 7588 **Body Length** : 7318 **Is Compressed** : No

```
HTTP/1.1 200 OK
Content-Type: text/html;charset=UTF-8
Server: Apache-Coyote/1.1
Content-Language: en-US
Access-Control-Allow-Origin: *
Transfer-Encoding: chunked
Date: Sun, 30 Jul 2023 06:08:58 GMT
Cache-Control: no-cache, max-age=0, must-reval
…
                <div class="control-group">
                    <label class="control-label" for="user_password">Password</label>
                    <div class="controls">
                        <input type="password" id="user_password" name="user_password" tabindex="2" aut
ocomplete="off"/>
                    </div>
                </div>

                <div class="control-group">
                    <label class="control-label" for="user_remember_me">Keep me signed in</label>

…
```

Actions to Take

1. See the remedy for solution.
2. Move all of your critical forms and pages to HTTPS and do not serve them over HTTP.

Remedy

All sensitive data should be transferred over HTTPS rather than HTTP. Forms should be served over HTTPS. All aspects of the application that accept user input, starting from the login process, should only be served over HTTPS.

CLASSIFICATION

PCI DSS v3.2	6.5.4
OWASP 2013	A6
OWASP 2017	A3
CWE	319
CAPEC	65
WASC	4
ISO27001	A.14.1.3

CVSS 3.0 SCORE

Base	5.7 (Medium)
Temporal	5.7 (Medium)
Environmental	5.7 (Medium)

CVSS Vector String

CVSS:3.0/AV:A/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N

CVSS 3.1 SCORE

Base	5.7 (Medium)
Temporal	5.7 (Medium)
Environmental	5.7 (Medium)

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

6. Apache Server-Status Detected

MEDIUM | 1

Netsparker detected that Apache `server-status` is enabled.

Information disclosed from this page can be used to gain additional information about the target system.

Impact

An attacker can gather reconnaissance information about the internals of the target web server, such as:

- Server uptime
- Individual request-response statistics and CPU usage of the working processes
- Current HTTP requests, client IP addresses, requested paths, and processed virtual hosts

This type of information can help the attacker gain a greater understanding of the system in use and the other potential avenues of attack available.

Vulnerabilities

6.1. http://zero.webappsecurity.com/server-status

Certainty

Request

```
GET /server-status HTTP/1.1
Host: zero.webappsecurity.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.
77 Safari/537.36
X-Scanner: Netsparker
```

Response

Response Time (ms) : 197.5176 **Total Bytes Received** : 5699 **Body Length** : 5523 **Is Compressed** : No

```
HTTP/1.1 200 OK
Content-Type: text/html;charset=UTF-8
Server: Apache-Coyote/1.1
Content-Length: 5523
Access-Control-Allow-Origin: *
Date: Sun, 30 Jul 20
…
523
Access-Control-Allow-Origin: *
Date: Sun, 30 Jul 2023 06:08:56 GMT

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 3.2 Final//EN">
<html><head>
    <title>Apache Status</title>
</head><body>
<h1>Apache Server Status for localhost</h1>

<dl><dt>Server Version: Apache/2.2.22 (Win32) mod_ssl/2.2.22 OpenSSL/0.9.8t mod_jk/1.2.37</dt>
    <dt>Server Built: Jan 28 2012 11:16:39
    </dt></dl><hr /><dl>
    <dt>Cur
…
```

Remedy

We recommend disabling this functionality. Comment out the `Location/server-info` section from Apache configuration file `httpd.conf` (for Redhat, Centos, Fedora) or `apache2.conf` (for Debian, Ubuntu).

External References

- Exploiting Misconfigured Apache server-status Instances with server-status_PWN

CLASSIFICATION

OWASP 2013	A5
OWASP 2017	A6
CWE	16
CAPEC	347
WASC	14
ISO27001	A.18.1.3

CVSS 3.0 SCORE

Base	5.3 (Medium)
Temporal	5.1 (Medium)
Environmental	5.1 (Medium)

CVSS Vector String

CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N/E:H/RL:O/RC:C

CVSS 3.1 SCORE

Base	5.3 (Medium)
Temporal	5.1 (Medium)
Environmental	5.1 (Medium)

CVSS Vector String
CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N/E:H/RL:O/RC:C

7. HTTP Strict Transport Security (HSTS) Policy Not Enabled

MEDIUM | 1

Netsparker identified that HTTP Strict Transport Security (HSTS) policy is not enabled.

The target website is being served from not only HTTPS but also HTTP and it lacks of HSTS policy implementation.

HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure (HTTPS) connections. The HSTS Policy is communicated by the server to the user agent via a HTTP response header field named "Strict-Transport-Security". HSTS Policy specifies a period of time during which the user agent shall access the server in only secure fashion.

When a web application issues HSTS Policy to user agents, conformant user agents behave as follows:

- Automatically turn any insecure (HTTP) links referencing the web application into secure (HTTPS) links. (For instance, http://example.com/some/page/ will be modified to https://example.com/some/page/ before accessing the server.)
- If the security of the connection cannot be ensured (e.g. the server's TLS certificate is self-signed), user agents show an error message and do not allow the user to access the web application.

Vulnerabilities

7.1. https://zero.webappsecurity.com/

Certainty

Request

```
GET / HTTP/1.1
Host: zero.webappsecurity.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Connection: Keep-Alive
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.
77 Safari/537.36
X-Scanner: Netsparker
```

Response

Response Time (ms) : 1286.3876 **Total Bytes Received** : 401 **Body Length** : 44 **Is Compressed** : No

```
HTTP/1.1 200 OK
Content-Type: text/html
Server: Apache/2.2.6 (Win32) mod_ssl/2.2.6 OpenSSL/0.9.8e mod_jk/1.2.40
Connection: Keep-Alive
Keep-Alive: timeout=5, max=100
Content-Length: 44
Last-Modified: Sat, 20 Nov 2004 14:16:24 GMT
Accept-Ranges: bytes
Access-Control-Allow-Origin: *
Date: Sun, 30 Jul 2023 06:08:58 GMT
ETag: "24c22-2c-44adde00"

<html><body><h1>It works!</h1></body></html>
```

Remedy

Configure your webserver to redirect HTTP requests to HTTPS.

i.e. for Apache, you should have modification in the httpd.conf. For more configurations, please refer to External References section.

```
# load module
LoadModule headers_module modules/mod_headers.so

# redirect all HTTP to HTTPS (optional)
<VirtualHost *:80>
       ServerAlias *
       RewriteEngine On
       RewriteRule ^(.*)$ https://%{HTTP_HOST}$1 [redirect=301]
</VirtualHost>

# HTTPS-Host-Configuration
<VirtualHost *:443>
      # Use HTTP Strict Transport Security to force client to use secure connections only
      Header always set Strict-Transport-Security "max-age=31536000; includeSubDomains"

      # Further Configuration goes here
      [...]
</VirtualHost>
```

External References

- Wikipedia - HTTP Strict Transport Security
- Configure HSTS (HTTP Strict Transport Security) for Apache/Nginx

- HTTP Strict Transport Security (HSTS) HTTP Header
- Mozilla SSL Configuration Generator

CLASSIFICATION

OWASP 2013	A6
OWASP 2017	A3
CWE	523
CAPEC	217
WASC	4
ISO27001	A.14.1.2

8. Insecure Transportation Security Protocol Supported (SSLv3)

MEDIUM 1 CONFIRMED 1

Netsparker detected that insecure transportation security protocol (SSLv3) is supported by your web server.

SSLv3 has several flaws. An attacker can cause connection failures and they can trigger the use of SSL 3.0 to exploit vulnerabilities like POODLE.

Impact

Attackers can perform man-in-the-middle attacks and observe the encryption traffic between your website and its visitors.

Vulnerabilities

8.1. https://zero.webappsecurity.com/

CONFIRMED

Request

```
[NETSPARKER] SSL Connection
```

Response

Response Time (ms) : 1 **Total Bytes Received :** 27 **Body Length :** 0 **Is Compressed :** No

```
[NETSPARKER] SSL Connection
```

Actions to Take

We recommended to disable SSLv3 and replace it with TLS 1.2 or higher. See Remedy section for more details.

Remedy

Configure your web server to disallow using weak ciphers. You need to restart the web server to enable changes.

- For Apache, adjust the SSLProtocol directive provided by the mod_ssl module. This directive can be set either at the server level or in a virtual host configuration.

```
SSLProtocol +TLSv1.2
```

- For Nginx, locate any use of the directive ssl_protocols in the `nginx.conf` file and remove `SSLv3`.

```
ssl_protocols TLSv1.2;
```

- For Microsoft IIS, you should make some changes on the system registry. **Incorrectly editing the registry may severely damage your system. Before making changes to the registry, you should back up any valued data on your computer.**
    1. Click on Start and then Run, type `regedt32` or `regedit`, and then click OK.
    2. In Registry Editor, locate the following registry key or create if it does not exist:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\SSL 3.0\
```

    3. Locate a key named `Server` or create if it doesn't exist.
    4. Under the `Server` key, locate a DWORD value named `Enabled` or create if it doesn't exist and set its value to "0".
- For lighttpd, put the following lines in your configuration file:

```
ssl.use-sslv2 = "disable"
ssl.use-sslv3 = "disable"
ssl.openssl.ssl-conf-cmd = ("Protocol" => "-TLSv1.1, -TLSv1, -SSLv3") # v1.4.48 or up
ssl.ec-curve = "secp384r1"
```

External References

- How to disable SSlv3
- OWASP - Insecure Configuration Management
- OWASP Top 10-2017 A3-Sensitive Data Exposure
- How to disable PCT 1.0, SSL 2.0, SSL 3.0, or TLS 1.0 in Internet Information Services
- This POODLE Bites: Exploiting The SSL 3.0 Fallback
- IIS Crypto is a free tool that gives administrators the ability to enable or disable protocols, ciphers, hashes and key exchange algorithms on Windows Server 2003, 2008 and 2012
- OWASP - Insufficient Transport Layer Protection

CLASSIFICATION

PCI DSS v3.2	6.5.4
OWASP 2013	A6
OWASP 2017	A3
CWE	326
CAPEC	217
WASC	4
HIPAA	164.306
ISO27001	A.14.1.3

CVSS 3.0 SCORE

Base	6.8 (Medium)
Temporal	6.1 (Medium)
Environmental	6.1 (Medium)

CVSS Vector String

CVSS:3.0/AV:A/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:N/E:P/RL:O/RC:C

CVSS 3.1 SCORE

Base	6.8 (Medium)
Temporal	6.1 (Medium)
Environmental	6.1 (Medium)

CVSS Vector String
CVSS:3.1/AV:A/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:N/E:P/RL:O/RC:C

9. Invalid SSL Certificate

MEDIUM 1 CONFIRMED 1

Netsparker identified an invalid SSL certificate.

An SSL certificate can be created and signed by anyone. You should have a valid SSL certificate to make your visitors sure about the secure communication between your website and them. If you have an invalid certificate, your visitors will have trouble distinguishing between your certificate and those of attackers.

Impact

Attackers can perform man-in-the-middle attacks and observe the encryption traffic between your website and its visitors.

Vulnerabilities

9.1. https://zero.webappsecurity.com/

CONFIRMED

List of Problems

- The certificate is not signed by a trusted authority -

Request

```
[NETSPARKER] SSL Connection
```

Response

Response Time (ms) : 1 **Total Bytes Received :** 27 **Body Length :** 0 **Is Compressed :** No

```
[NETSPARKER] SSL Connection
```

Remedy

Fix the problem with your SSL certificate to provide secure communication between your website and its visitors.

External References

- OWASP - Insecure Configuration Management
- OWASP Top 10-2017 A3-Sensitive Data Exposure

CLASSIFICATION

PCI DSS v3.2	6.5.4
OWASP 2013	A6
OWASP 2017	A3
CWE	295
CAPEC	459
WASC	4
ISO27001	A.14.1.3

CVSS 3.0 SCORE

Base	6.8 (Medium)
Temporal	6.8 (Medium)
Environmental	6.8 (Medium)

CVSS Vector String

CVSS:3.0/AV:A/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:N

CVSS 3.1 SCORE

Base	6.8 (Medium)
Temporal	6.8 (Medium)
Environmental	6.8 (Medium)

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

10. Out-of-date Version (jQuery)

MEDIUM | 1

Netsparker identified the target web site is using jQuery and detected that it is out of date.

Impact

Since this is an old version of the software, it may be vulnerable to attacks.

jQuery Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') Vulnerability

jQuery before 3.0.0 is vulnerable to Cross-site Scripting (XSS) attacks when a cross-domain Ajax request is performed without the dataType option, causing text/javascript responses to be executed.

Affected Versions

1.8.0 to 2.2.4

External References

- CVE-2015-9251

jQuery Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') Vulnerability

jQuery before 1.9.0 is vulnerable to Cross-site Scripting (XSS) attacks. The jQuery(strInput) function does not differentiate selectors from HTML in a reliable fashion. In vulnerable versions, jQuery determined whether the input was HTML by looking for the '<' character anywhere in the string, giving attackers more flexibility when attempting to construct a malicious payload. In fixed versions, jQuery only deems the input to be HTML if it explicitly starts with the '<' character, limiting exploitability only to attackers who can control the beginning of a string, which is far less common.

Affected Versions

1.8.0 to 1.8.3

External References

- CVE-2012-6708

jQuery Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') Vulnerability

In jQuery versions greater than or equal to 1.0.3 and before 3.5.0, passing HTML containing <option> elements from untrusted sources - even after sanitizing it - to one of jQuery's DOM manipulation methods (i.e. .html(), .append(), and others) may execute untrusted code. This problem is patched in jQuery 3.5.0.

Affected Versions

1.8.0 to 1.8.3

External References

- CVE-2020-11023

jQuery Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') Vulnerability

In jQuery versions greater than or equal to 1.2 and before 3.5.0, passing HTML from untrusted sources - even after sanitizing it - to one of jQuery's DOM manipulation methods (i.e. .html(), .append(), and others) may execute untrusted code. This problem is patched in jQuery 3.5.0.

Affected Versions
1.8.0 to 1.8.3

External References
- CVE-2020-11022

jQuery Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') Vulnerability

jquery prior to 1.9.0 allows Cross-site Scripting attacks via the load method. The load method fails to recognize and remove "<script>" HTML tags that contain a whitespace character, i.e: "</script >", which results in the enclosed script logic to be executed.

Affected Versions
1.8.0 to 1.8.3

External References
- CVE-2020-7656

JQuery Prototype Pollution Vulnerability

jQuery before 3.4.0, as used in Drupal, Backdrop CMS, and other products, mishandles jQuery.extend(true, {}, ...) because of Object.prototype pollution. If an unsanitized source object contained an enumerable __proto__ property, it could extend the native Object.prototype.

Affected Versions
1.0 to 3.3.1

External References
- CVE-2019-11358

Vulnerabilities

10.1. http://zero.webappsecurity.com/

Identified Version
- 1.8.2

Latest Version
- 1.12.4 (in this branch)

Vulnerability Database
- Result is based on 07/27/2023 20:30:00 vulnerability database content.

Certainty

Request

```
GET / HTTP/1.1
Host: zero.webappsecurity.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.
77 Safari/537.36
X-Scanner: Netsparker
```

Response

Response Time (ms) : 631.2942 **Total Bytes Received** : 12741 **Body Length** : 12471 **Is Compressed** : No

```
HTTP/1.1 200 OK
Content-Type: text/html;charset=UTF-8
Server: Apache-Coyote/1.1
Content-Language: en-US
Access-Control-Allow-Origin: *
Transfer-Encoding: chunked
Date: Sun, 30 Jul 2023 06:08:38 GMT
Cache-Control: no-cache, max-age=0, must-reval
…
"/>
    <link type="text/css" rel="stylesheet" href="/resources/css/font-awesome.css"/>
    <link type="text/css" rel="stylesheet" href="/resources/css/main.css"/>

    <script src="/resources/js/jquery-1.8.2.min.js"></script>
        <script src="/resources/js/bootstrap.min.js"></script>

    <script src="/resources/js/placeholders.min.js"></script>
    <script type="text/javascript">
        Placeholders.
…
```

Remedy

Please upgrade your installation of jQuery to the latest stable version.

Remedy References

- Downloading jQuery

CLASSIFICATION

PCI DSS v3.2	6.2
OWASP 2013	A9
OWASP 2017	A9
CWE	829
CAPEC	310
HIPAA	164.308(A)(1)(I)
OWASP Proactive Controls	C1
ISO27001	A.14.1.2

11. Weak Ciphers Enabled

MEDIUM 1 CONFIRMED 1

Netsparker detected that weak ciphers are enabled during secure communication (SSL).

You should allow only strong ciphers on your web server to protect secure communication with your visitors.

Impact

Attackers might decrypt SSL traffic between your server and your visitors.

Vulnerabilities

11.1. https://zero.webappsecurity.com/

CONFIRMED

List of Supported Weak Ciphers

- RC4_128_WITH_MD5 (0x10080)
- RC4_128_EXPORT40_WITH_MD5 (0x20080)
- RC2_128_CBC_WITH_MD5 (0x30080)
- RC2_128_CBC_EXPORT40_WITH_MD5 (0x40080)
- DES_64_CBC_WITH_MD5 (0x60040)
- DES_192_EDE3_CBC_WITH_MD5 (0x700C0)
- TLS_RSA_EXPORT_WITH_RC4_40_MD5 (0x0003)
- TLS_RSA_WITH_RC4_128_MD5 (0x0004)
- TLS_RSA_WITH_RC4_128_SHA (0x0005)
- TLS_RSA_EXPORT_WITH_RC2_CBC_40_MD5 (0x0006)
- TLS_RSA_EXPORT_WITH_DES40_CBC_SHA (0x0008)
- TLS_RSA_WITH_DES_CBC_SHA (0x0009)
- TLS_RSA_WITH_3DES_EDE_CBC_SHA (0x000A)
- TLS_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA (0x0014)
- TLS_DHE_RSA_WITH_DES_CBC_SHA (0x0015)
- TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA (0x0016)
- TLS_RSA_WITH_AES_128_CBC_SHA (0x002F)
- TLS_DHE_RSA_WITH_AES_128_CBC_SHA (0x0033)
- TLS_RSA_WITH_AES_256_CBC_SHA (0x0035)
- TLS_DHE_RSA_WITH_AES_256_CBC_SHA (0x0039)

Request

```
[NETSPARKER] SSL Connection
```

Response

Response Time (ms) : 1 Total Bytes Received : 27 Body Length : 0 Is Compressed : No

```
[NETSPARKER] SSL Connection
```

Actions to Take

1. For Apache, you should modify the SSLCipherSuite directive in the `httpd.conf`.

```
SSLCipherSuite HIGH:MEDIUM:!MD5:!RC4
```

2. Lighttpd:

```
ssl.honor-cipher-order = "enable"
ssl.cipher-list = "EECDH+AESGCM:EDH+AESGCM"
```

3. For Microsoft IIS, you should make some changes to the system registry. **Incorrectly editing the registry may severely damage your system. Before making changes to the registry, you should back up any valued data on your computer.**

   a. Click Start, click Run, type `regedt32` or type `regedit`, and then click OK.
   b. In Registry Editor, locate the following registry key: `HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders`
   c. Set "Enabled" DWORD to "0x0" for the following registry keys:

```
SCHANNEL\Ciphers\DES 56/56
SCHANNEL\Ciphers\RC4 64/128
SCHANNEL\Ciphers\RC4 40/128
SCHANNEL\Ciphers\RC2 56/128
SCHANNEL\Ciphers\RC2 40/128
SCHANNEL\Ciphers\NULL
SCHANNEL\Hashes\MD5
```

Remedy

Configure your web server to disallow using weak ciphers.

External References

- OWASP - Insecure Configuration Management
- OWASP Top 10-2017 A3-Sensitive Data Exposure
- Zombie Poodle - Golden Doodle (CBC)
- Mozilla SSL Configuration Generator
- Strong Ciphers for Apache, Nginx and Lighttpd

CLASSIFICATION

PCI DSS v3.2	6.5.4
OWASP 2013	A6
OWASP 2017	A3
CWE	327
CAPEC	217
WASC	4
ISO27001	A.14.1.3

CVSS 3.0 SCORE

Base	6.8 (Medium)
Temporal	6.8 (Medium)
Environmental	6.8 (Medium)

CVSS Vector String

CVSS:3.0/AV:A/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:N

CVSS 3.1 SCORE

Base	6.8 (Medium)
Temporal	6.8 (Medium)
Environmental	6.8 (Medium)

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

12. [Possible] Cross-site Request Forgery

LOW | 1

Netsparker identified a possible Cross-Site Request Forgery.

CSRF is a very common vulnerability. It's an attack which forces a user to execute unwanted actions on a web application in which the user is currently authenticated.

Impact

Depending on the application, an attacker can mount any of the actions that can be done by the user such as adding a user, modifying content, deleting data. All the functionality that's available to the victim can be used by the attacker. Only exception to this rule is a page that requires extra information that only the legitimate user can know (such as user's password).

Vulnerabilities

12.1. http://zero.webappsecurity.com/feedback.html

Form Action(s)

- /sendFeedback.html

Certainty

Request

```
GET /feedback.html HTTP/1.1
Host: zero.webappsecurity.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Referer: http://zero.webappsecurity.com/online-banking.html
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.
77 Safari/537.36
X-Scanner: Netsparker
```

Response

Response Time (ms) : 204.3134 **Total Bytes Received** : 9528 **Body Length** : 9258 **Is Compressed** : No

```
HTTP/1.1 200 OK
Content-Type: text/html;charset=UTF-8
Server: Apache-Coyote/1.1
Content-Language: en-US
Access-Control-Allow-Origin: *
Transfer-Encoding: chunked
Date: Sun, 30 Jul 2023 06:08:58 GMT
Cache-Control: no-cache, max-age=0, must-reval
…
is not secure. Please do not send any
                <br/>
                account information in a message sent from here.
            </p>

            <hr class="wide"/>

            <form action="/sendFeedback.html" method="post" class="">

                <div class="signin-controls form-inputs">
                    <div class="control-group">
                        <div class="controls pictured">

…
```

Remedy

- Send additional information in each HTTP request that can be used to determine whether the request came from an authorized source. This "validation token" should be hard to guess for attacker who does not already have access to the user's account. If a request is missing a validation token or the token does not match the expected value, the server should reject the request.
- If you are posting form in ajax request, custom HTTP headers can be used to prevent CSRF because the browser prevents sites from sending custom HTTP headers to another site but allows sites to send custom HTTP headers to themselves using XMLHttpRequest.
    - For native XMLHttpRequest (XHR) object in JavaScript;

      ```
      xhr = new XMLHttpRequest();
      xhr.setRequestHeader('custom-header', 'valueNULL');
      ```

      For JQuery, if you want to add a custom header (or set of headers) to
      a. **individual request**

```
$.ajax({
    url: 'foo/bar',
    headers: { 'x-my-custom-header': 'some value' }
});
```

b. **every request**

```
$.ajaxSetup({
    headers: { 'x-my-custom-header': 'some value' }
});
OR
$.ajaxSetup({
    beforeSend: function(xhr) {
        xhr.setRequestHeader('x-my-custom-header', 'some value');
    }
});
```

External References

- OWASP Cross-Site Request Forgery (CSRF)

Remedy References

- OWASP Cross-Site Request Forgery (CSRF) Prevention Cheat Sheet

CLASSIFICATION

PCI DSS v3.2	6.5.9
OWASP 2013	A8
OWASP 2017	A5
CWE	352
CAPEC	62
WASC	9
HIPAA	164.306(A)
ISO27001	A.14.2.5

13. [Possible] Cross-site Request Forgery in Login Form

LOW | 1

Netsparker identified a possible Cross-Site Request Forgery in Login Form.

In a login CSRF attack, the attacker forges a login request to an honest site using the attacker's user name and password at that site. If the forgery succeeds, the honest server responds with a Set-Cookie header that instructs the browser to mutate its state by storing a session cookie, logging the user into the honest site as the attacker. This session cookie is used to bind subsequent requests to the user's session and hence to the attacker's authentication credentials. The attacker can later log into the site with his legitimate credentials and view private information like activity history that has been saved in the account.

Impact

In this particular case CSRF affects the login form in which the impact of this vulnerability is decreased significantly. Unlike normal CSRF vulnerabilities this will only allow an attacker to exploit some complex XSS vulnerabilities otherwise it can't be exploited.

For example;

If there is a page that's different for every user (such as "edit my profile") and vulnerable to XSS (Cross-site Scripting) then normally it cannot be exploited. However if the login form is vulnerable, an attacker can prepare a special profile, force victim to login as that user which will trigger the XSS exploit. Again attacker is still quite limited with this XSS as there is no active session. However the attacker can leverage this XSS in many ways such as showing the same login form again but this time capturing and sending the entered username/password to the attacker.

In this kind of attack, attacker will send a link containing html as simple as the following in which attacker's user name and password is attached.

```
<form method="POST" action="http://honest.site/login">
  <input type="text" name="user" value="h4ck3r" />
  <input type="password" name="pass" value="passw0rd" />
</form>
<script>
    document.forms[0].submit();
</script>
```

When the victim clicks the link then form will be submitted automatically to the honest site and exploitation is successful, victim will be logged in as the attacker and consequences will depend on the website behavior.

- **Search History**
  Many sites allow their users to opt-in to saving their search history and provide an interface for a user to review his or her personal search history. Search queries contain sensitive details about the user's interests and activities and could be used by the attacker to embarrass the user, to steal the user's identity, or to spy on the user. Since the victim logs in as the attacker, the victim's search queries are then stored in the attacker's search history, and the attacker can retrieve the queries by logging into his or her own account.

- **Shopping**
  Merchant sites might save the credit card details in user's profile. In login CSRF attack, when user funds a purchase and enrolls the credit card, the credit card details might be added to the attacker's account.

Vulnerabilities

13.1. http://zero.webappsecurity.com/login.html

Form Action(s)

- /signin.html

Certainty

Request

```
GET /login.html HTTP/1.1
Host: zero.webappsecurity.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Referer: http://zero.webappsecurity.com/feedback.html
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.
77 Safari/537.36
X-Scanner: Netsparker
```

Response

Response Time (ms) : 198.3096 **Total Bytes Received** : 7588 **Body Length** : 7318 **Is Compressed** : No

```
HTTP/1.1 200 OK
Content-Type: text/html;charset=UTF-8
Server: Apache-Coyote/1.1
Content-Language: en-US
Access-Control-Allow-Origin: *
Transfer-Encoding: chunked
Date: Sun, 30 Jul 2023 06:08:58 GMT
Cache-Control: no-cache, max-age=0, must-reval
…
fset">


<div class="row">
    <div class="offset3 span6">
        <div class="page-header">
                <h3>Log in to ZeroBank</h3>
        </div>

        <form id="login_form" action="/signin.html" method="post" class="form-horizontal">

            <div class="form-inputs">
                <div class="control-group">
                    <label class="control-label" for="user_login">Login<
…
```

Remedy

- Send additional information in each HTTP request that can be used to determine whether the request came from an authorized source. This "validation token" should be hard to guess for attacker who does not already have access to the user's account. If a request is missing a validation token or the token does not match the expected value, the server should reject the request.
- If you are posting form in ajax request, custom HTTP headers can be used to prevent CSRF because the browser prevents sites from sending custom HTTP headers to another site but allows sites to send custom HTTP headers to themselves using XMLHttpRequest.
    - For native XMLHttpRequest (XHR) object in JavaScript;

      ```
      xhr = new XMLHttpRequest();
      xhr.setRequestHeader('custom-header', 'valueNULL');
      ```

      For JQuery, if you want to add a custom header (or set of headers) to
      a. **individual request**

```
$.ajax({
    url: 'foo/bar',
    headers: { 'x-my-custom-header': 'some value' }
});
```

b. **every request**

```
$.ajaxSetup({
    headers: { 'x-my-custom-header': 'some value' }
});
OR
$.ajaxSetup({
    beforeSend: function(xhr) {
        xhr.setRequestHeader('x-my-custom-header', 'some value');
    }
});
```

External References

- OWASP Cross-Site Request Forgery (CSRF)
- Robust Defenses for Cross-Site Request Forgery
- Identifying Robust Defenses for Login CSRF

Remedy References

- OWASP Cross-Site Request Forgery (CSRF) Prevention Cheat Sheet

CLASSIFICATION

PCI DSS v3.2	6.5.9
OWASP 2013	A8
OWASP 2017	A5
CWE	352
CAPEC	62
WASC	9
HIPAA	164.306(A)
ISO27001	A.14.2.5

14. [Possible] Phishing by Navigating Browser Tabs

LOW | 1

Netsparker identified possible phishing by navigating browser tabs but was unable to confirm the vulnerability.

Open windows with normal hrefs with the tag `target="_blank"` can modify *window.opener.location* and replace the parent webpage with something else, even on a different origin.

Impact

While this vulnerability doesn't allow script execution, it does allow phishing attacks that silently replace the parent tab. If the links lack `rel="noopener noreferrer"` attribute, a third party site can change the URL of the source tab using *window.opener.location.assign* and trick the users into thinking that they're still in a trusted page and lead them to enter their sensitive data on the malicious website.

Vulnerabilities

14.1. http://zero.webappsecurity.com/

External Links

- https://www.microfocus.com/about/legal/#privacy
- https://www.microfocus.com/about/legal/#privacy

Certainty

Request

```
GET / HTTP/1.1
Host: zero.webappsecurity.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.
77 Safari/537.36
X-Scanner: Netsparker
```

Response

Response Time (ms) : 631.2942 **Total Bytes Received** : 12741 **Body Length** : 12471 **Is Compressed** : No

```
HTTP/1.1 200 OK
Content-Type: text/html;charset=UTF-8
Server: Apache-Coyote/1.1
Content-Language: en-US
Access-Control-Allow-Origin: *
Transfer-Encoding: chunked
Date: Sun, 30 Jul 2023 06:08:38 GMT
Cache-Control: no-cache, max-age=0, must-reval
…
in relation to your use of this Web site.
                    Use of this Web site indicates that you have read and agree to Micro Focus Fortif
y’s Terms of Use found at
                    <a href="https://www.microfocus.com/about/legal/#privacy" target="_blank">https://w
ww.microfocus.com/about/legal/#privacy</a>
                    and Micro Focus Fortify’s Online Privacy Statement found at
                    <a href="https://www.microfocus.com/about/legal/#privacy" target="_blank">https://w
ww.microfocus.com/about/legal/#privacy</a>.

                    <br/><br/>

                    Copyright © 2012-2018, Micro Focus Development Company. All rights reserved.
                </div>
            </div>
        </div>

…
webinspect-dynamic-analysis-dast/overview" },
            "contact_hp_link" : { absolute: true, page: "https://support.fortify.com" },
            "privacy_statement_link": { absolute: true, page: "https://www.microfocus.com/about/legal/#
privacy" },
            "terms_of_use_link": { absolute: true, page: "https://www.microfocus.com/about/legal/" }
        };

        $.each(footerLinks, function(linkId, link) {
            attachClickH
…
```

Remedy

- Add `rel=noopener` to the links to prevent pages from abusing *window.opener*. This ensures that the page cannot access the *window.opener* property in Chrome and Opera browsers.
- For older browsers and in Firefox, you can add `rel=noreferrer` which additionally disables the Referer header.

```
<a href="..." target="_blank" rel="noopener noreferrer">...</a>
```

External References

- Reverse Tabnabbing
- Blankshield & Reverse Tabnabbing Attacks
- Target=" blank" - the most underestimated vulnerability ever

CLASSIFICATION

OWASP 2013	A5
OWASP 2017	A6
CWE	16
WASC	15
ISO27001	A.14.1.2

15. Insecure Transportation Security Protocol Supported (TLS 1.0)

LOW 1 CONFIRMED 1

Netsparker detected that insecure transportation security protocol (TLS 1.0) is supported by your web server.

TLS 1.0 has several flaws. An attacker can cause connection failures and they can trigger the use of TLS 1.0 to exploit vulnerabilities like BEAST (Browser Exploit Against SSL/TLS).

Websites using TLS 1.0 are considered non-compliant by PCI since 30 June 2018.

Impact

Attackers can perform man-in-the-middle attacks and observe the encryption traffic between your website and its visitors.

Vulnerabilities

15.1. https://zero.webappsecurity.com/

CONFIRMED

Request

```
[NETSPARKER] SSL Connection
```

Response

Response Time (ms) : 1 **Total Bytes Received** : 27 **Body Length** : 0 **Is Compressed** : No

```
[NETSPARKER] SSL Connection
```

Actions to Take

We recommended to disable TLS 1.0 and replace it with TLS 1.2 or higher. See Remedy section for more details.

Remedy

Configure your web server to disallow using weak ciphers. You need to restart the web server to enable changes.

- For Apache, adjust the SSLProtocol directive provided by the mod_ssl module. This directive can be set either at the server level or in a virtual host configuration.

```
SSLProtocol +TLSv1.2
```

- For Nginx, locate any use of the directive ssl_protocols in the `nginx.conf` file and remove `TLSv1`.

```
ssl_protocols TLSv1.2;
```

- For Microsoft IIS, you should make some changes on the system registry. **Incorrectly editing the registry may severely damage your system. Before making changes to the registry, you should back up any valued data on your computer.**
    1. Click on Start and then Run, type `regedt32` or `regedit`, and then click OK.
    2. In Registry Editor, locate the following registry key or create if it does not exist:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.0\
```

    3. Locate a key named `Server` or create if it doesn't exist.
    4. Under the `Server` key, locate a DWORD value named `Enabled` or create if it doesn't exist and set its value to "0".
- For lighttpd, put the following lines in your configuration file:

```
ssl.use-sslv2 = "disable"
ssl.use-sslv3 = "disable"
ssl.openssl.ssl-conf-cmd = ("Protocol" => "-TLSv1.1, -TLSv1, -SSLv3") # v1.4.48 or up
ssl.ec-curve = "secp384r1"
```

External References

- How to Disable TLS v1.0
- OWASP - Insecure Configuration Management
- OWASP Top 10 - 2017 A3 - Sensitive Data Exposure
- How to disable PCT 1.0, SSL 2.0, SSL 3.0, or TLS 1.0 in Internet Information Services
- IIS Crypto is a free tool that gives administrators the ability to enable or disable protocols, ciphers, hashes and key exchange algorithms on Windows Server 2003, 2008 and 2012
- Date Change for Migrating from SSL and Early TLS
- Browser Exploit Against SSL/TLS Attack (BEAST)
- Are You Ready for 30 June 2018? Saying Goodbye to SSL/early TLS

CLASSIFICATION

PCI DSS v3.2	6.5.4
OWASP 2013	A6
OWASP 2017	A3
CWE	326
CAPEC	217
WASC	4
HIPAA	164.306
ISO27001	A.14.1.3

16. Misconfigured Access-Control-Allow-Origin Header

LOW | 1

Netsparker detected a possibly misconfigured Access-Control-Allow-Origin header in resource's HTTP response.

Cross-origin resource sharing (CORS) is a mechanism that allows resources on a web page to be requested outside the domain through XMLHttpRequest.

Unless this HTTP header is present, such "cross-domain" requests are forbidden by web browsers, per the same-origin security policy.

Impact

This is generally not appropriate when using the same-origin security policy. The only case where this is appropriate when using the same-origin policy is when a page or API response is considered completely public content and it is intended to be accessible to everyone.

Vulnerabilities

16.1. http://zero.webappsecurity.com/

Access-Control-Allow-Origin

- *

Certainty

Request

```
GET / HTTP/1.1
Host: zero.webappsecurity.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.
77 Safari/537.36
X-Scanner: Netsparker
```

Response

Response Time (ms) : 631.2942 **Total Bytes Received** : 12741 **Body Length** : 12471 **Is Compressed** : No

```
HTTP/1.1 200 OK
Content-Type: text/html;charset=UTF-8
Server: Apache-Coyote/1.1
Content-Language: en-US
Access-Control-Allow-Origin: *
Transfer-Encoding: chunked
Date: Sun, 30 Jul 2023 06:08:38 GMT
Cache-Control: no-cache, max-age=0, must-revalHTTP/1.1 200 OK
Content-Type: text/html;charset=UTF-8
Server: Apache-Coyote/1.1
Content-Language: en-US
Access-Control-Allow-Origin: *
Transfer-Encoding: chunked
Date: Sun, 30 Jul 2023 06:08:38 GMT
Cache-Control: no-cache, max-age=0, must-revalidate, no-store


<!DOCTYPE html>
<html lang="en">
<head>
    <meta charset="utf-
…
```

Remedy

If this page is intended to be accessible to everyone, you don't need to take any action. Otherwise please follow the guidelines for different architectures below in order to set this header and permit outside domain.
Apache

- Add the following line inside either the <directory>, <location>, <files> or <virtualhost> sections of your server config (usually located in `httpd.conf` or `apache.conf`), or within a `.htaccess` file.

```
Header set Access-Control-Allow-Origin "domain"
```

IIS6

1. Open Internet Information Service (IIS) Manager
2. Right click the site you want to enable CORS for and go to Properties
3. Change to the HTTP Headers tab
4. In the Custom HTTP headers section, click Add
5. Enter Access-Control-Allow-Origin as the header name
6. Enter `domain` as the header value

IIS7

- Merge the following xml into the web.config file at the root of your application or site:

```
<?xml version="1.0" encoding="utf-8" ?>
<configuration>
  <system.webserver>
    <httpprotocol>
      <customheaders>
        <add name="Access-Control-Allow-Origin" value="domain" />
      </customheaders>
    </httpprotocol>
  </system.webserver>
</configuration>
```

ASP.NET

- If you don't have access to configure IIS, you can still add the header through ASP.NET by adding the following line to your source pages:

```
Response.AppendHeader("Access-Control-Allow-Origin", "domain");
```

External References

- Cross-Origin Resource Sharing
- HTTP access control (CORS)
- Using CORS

CLASSIFICATION

OWASP 2013	A5
OWASP 2017	A6
CWE	16
WASC	15
ISO27001	A.14.1.2

17. Missing X-Frame-Options Header

LOW | 1

Netsparker detected a missing `X-Frame-Options` header which means that this website could be at risk of a clickjacking attack.

The `X-Frame-Options` HTTP header field indicates a policy that specifies whether the browser should render the transmitted resource within a `frame` or an `iframe`. Servers can declare this policy in the header of their HTTP responses to prevent clickjacking attacks, which ensures that their content is not embedded into other pages or frames.

Impact

Clickjacking is when an attacker uses multiple transparent or opaque layers to trick a user into clicking on a button or link on a framed page when they were intending to click on the top level page. Thus, the attacker is "hijacking" clicks meant for their page and routing them to other another page, most likely owned by another application, domain, or both.

Using a similar technique, keystrokes can also be hijacked. With a carefully crafted combination of stylesheets, iframes, and text boxes, a user can be led to believe they are typing in the password to their email or bank account, but are instead typing into an invisible frame controlled by the attacker.

Vulnerabilities

17.1. http://zero.webappsecurity.com/

Certainty

Request

```
GET / HTTP/1.1
Host: zero.webappsecurity.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.
77 Safari/537.36
X-Scanner: Netsparker
```

Response

Response Time (ms) : 631.2942 **Total Bytes Received** : 12741 **Body Length** : 12471 **Is Compressed** : No

```
HTTP/1.1 200 OK
Content-Type: text/html;charset=UTF-8
Server: Apache-Coyote/1.1
Content-Language: en-US
Access-Control-Allow-Origin: *
Transfer-Encoding: chunked
Date: Sun, 30 Jul 2023 06:08:38 GMT
Cache-Control: no-cache, max-age=0, must-revalidate, no-store


<!DOCTYPE html>
<html lang="en">
<head>
    <meta charset="utf-8">
    <title>Zero - Personal Banking - Loans - Credit Cards</title>
    <meta name="viewport" content="width=device-width, initial-scale=1.0, maximum-scale=1.0, user-scala
ble=no">
    <meta http-equiv="X-UA-Compatible" content="IE=Edge">

    <link type="text/css" rel="stylesheet" href="/resources/css/bootstrap.min.css"/>
    <link type="text/css" rel="stylesheet" href="/resources/css/font-awesome.css"/>
    <link type="text/css" rel="stylesheet" href="/resources/css/main.css"/>

    <script src="/resources/js/jquery-1.8.2.min.js"></script>
        <script src="/resources/js/bootstrap.min.js"></script>

    <script src="/resources/js/placeholders.min.js"></script>
    <script type="text/javascript">
        Placeholders.init({
            live: true, // Apply to future and modified elements too
            hideOnFocus: true // Hide the placeholder when the element receives focus
        });
    </script>
    <script type="text/javascript">
        $(document).ajaxError(function errorHandler(event, xhr, ajaxOptions, thrownError) {
            if (xhr.status == 403) {
                window.location.reload();
            }
        });
    </script>
</head>
<body>
    <div class="wrapper">
    <div class="navbar navbar-fixed-top">
        <div class="navbar-inner">
            <div class="container">
                <a href="/index.html" class="brand">Zero Bank</a>
```

```
                <div>
                    <ul class="nav float-right">
                        <li>    <form action="/search.html"
          class="navbar-search pull-right" style="padding-right: 20px">
        <input type="text" id="se
…
```

Remedy

- Sending the proper X-Frame-Options in HTTP response headers that instruct the browser to not allow framing from other domains.
    - `X-Frame-Options: DENY` It completely denies to be loaded in frame/iframe.
    - `X-Frame-Options: SAMEORIGIN` It allows only if the site which wants to load has a same origin.
    - `X-Frame-Options: ALLOW-FROM` *`URL`* It grants a specific URL to load itself in a iframe. However please pay attention to that, not all browsers support this.
- Employing defensive code in the UI to ensure that the current frame is the most top level window.

External References

- Clickjacking
- Can I Use X-Frame-Options
- X-Frame-Options HTTP Header

Remedy References

- Clickjacking Defense Cheat Sheet

CLASSIFICATION

OWASP 2013	A5
OWASP 2017	A6
CWE	693
CAPEC	103
ISO27001	A.14.2.5

18. Social Security Number Disclosure

LOW 1

Netsparker identified a Social Security Number disclosure.

Impact

Social Security Numbers have been used in identity theft by attackers, since many organizations including businesses, government agencies, medical facilities and educational institutions have been using the Social Security Number as the primary identifier for their record keeping systems.

Vulnerabilities

18.1. http://zero.webappsecurity.com/admin/users.html

SSN

- 536-48-3769
- 607-58-7435
- 247-54-1719
- 578-13-3713
- 449-20-3206
- 008-70-6738
- 574-56-1932
- 330-58-4012

SSN

- 536-48-3769
- 607-58-7435
- 247-54-1719
- 578-13-3713
- 449-20-3206
- 008-70-6738
- 574-56-1932
- 330-58-4012

Certainty

Request

```
GET /admin/users.html HTTP/1.1
Host: zero.webappsecurity.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: JSESSIONID=5CF19C3A
Referer: http://zero.webappsecurity.com/admin/
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.
77 Safari/537.36
X-Scanner: Netsparker
```

Response

Response Time (ms) : 201.0031 **Total Bytes Received** : 11078 **Body Length** : 10808 **Is Compressed** : No

```
HTTP/1.1 200 OK
Content-Type: text/html;charset=UTF-8
Server: Apache-Coyote/1.1
Content-Language: en-US
Access-Control-Allow-Origin: *
Transfer-Encoding: chunked
Date: Sun, 30 Jul 2023 06:09:16 GMT
Cache-Control: no-cache, max-age=0, must-reval
…
                                <td>
                                    VIZ10AWT8VL
                                </td>
                                <td>
                                    536-48-3769
                                </td>
                            </tr>
                            <tr>
                                <td>
                                    Stephen Bowen

…
                                <td>
                                    OTZ07BXM0BE
                                </td>
                                <td>
                                    607-58-7435
                                </td>
                            </tr>
                            <tr>
                                <td>
                                    Linus Moran

…
                                <td>
                                    FKO04SXA7TI
                                </td>
                                <td>
                                    247-54-1719
                                </td>
                            </tr>
                            <tr>
                                <td>
                                    Nero Chan

…
                                <td>
                                    TXJ77CQO5EI
```

```
                </td>
                <td>
                    578-13-3713
                </td>
            </tr>
            <tr>
                <td>
                    Kadeem Higgins

…
                <td>
                    MFC50OQE7VO
                </td>
                <td>
                    449-20-3206
                </td>
            </tr>
            <tr>
                <td>
                    Quinn Burks

…
                <td>
                    HWZ97ZUM3NK
                </td>
                <td>
                    008-70-6738
                </td>
            </tr>
            <tr>
                <td>
                    Davis Thompson

…
                <td>
                    RGD78SHB0TG
                </td>
                <td>
                    574-56-1932
                </td>
            </tr>
            <tr>
                <td>
                    Lester Keller

…
                <td>
                    EIJ79NLT0TP
                </td>
                <td>
                    330-58-4012
                </td>
            </tr>
```

```
                    </tbody>
                </table>
            </div>
        </div>
    </div>
</div>

…
```

Remedy

We strongly advise you not to expose Social Security Numbers via your website.

External References

- Social Security Number - Identity Theft

CLASSIFICATION

PCI DSS v3.2	6.5.3
OWASP 2013	A6
OWASP 2017	A3
CWE	213
CAPEC	118
WASC	13
ISO27001	A.18.1.3

19. Version Disclosure (Apache Coyote)

LOW 1

Netsparker identified a version disclosure (Apache Coyote) in target web server's HTTP response.

This information can help an attacker gain a greater understanding of the systems in use and potentially develop further attacks targeted at the specific version of Apache.

Impact

An attacker might use the disclosed information to harvest specific security vulnerabilities for the version identified.

Vulnerabilities

19.1. http://zero.webappsecurity.com/

Extracted Version

- Apache-Coyote/1.1

Certainty

Request

```
GET / HTTP/1.1
Host: zero.webappsecurity.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.
77 Safari/537.36
X-Scanner: Netsparker
```

Response

Response Time (ms) : 631.2942 **Total Bytes Received** : 12741 **Body Length** : 12471 **Is Compressed** : No

```
HTTP/1.1 200 OK
Content-Type: text/html;charset=UTF-8
Server: Apache-Coyote/1.1
Content-Language: en-US
Access-Control-Allow-Origin: *
Transfer-Encoding: chunked
Date: Sun, 30 Jul 2023 06:08:38 GMT
Cache-Control: no-cache, max-age=0, must-revalHTTP/1.1 200 OK
Content-Type: text/html;charset=UTF-8
Server: Apache-Coyote/1.1

Content-Language: en-US
Access-Control-Allow-Origin: *
Transfer-Encoding: chunked
Date: Sun, 30 Jul 2023 06:08:38 GMT
Cache-Control: no-cache, max-age=0, must-revalidate, no-store


<!DOCTYPE
…
```

Remedy

Configure your web server to prevent information leakage from the SERVER header of its HTTP response.

CLASSIFICATION

OWASP 2013	A5
OWASP 2017	A6
CWE	205
CAPEC	170
WASC	45
HIPAA	164.306(A), 164.308(A)
ISO27001	A.18.1.3

20. Version Disclosure (Apache Module)

LOW 1

Netsparker identified a version disclosure (Apache Module) in target server's HTTP response.

This information can help an attacker gain a greater understanding of the systems in use and potentially develop further attacks targeted at the specific version of Apache.

Impact

An attacker might use the disclosed information to harvest specific security vulnerabilities for the version identified.

Vulnerabilities

20.1. https://zero.webappsecurity.com/

Extracted Version

- mod_jk/1.2.40

Certainty

Request

```
GET / HTTP/1.1
Host: zero.webappsecurity.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: JSESSIONID=5CF19C3A
Referer: https://zero.webappsecurity.com/
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.
77 Safari/537.36
X-Scanner: Netsparker
```

Response

Response Time (ms) : 191.9997 Total Bytes Received : 345 Body Length : 44 Is Compressed : No

```
HTTP/1.1 200 OK
Content-Type: text/html
Server: Apache/2.2.6 (Win32) mod_ssl/2.2.6 OpenSSL/0.9.8e mod_jk/1.2.40

Content-Length: 44
Last-Modified: Sat, 20 Nov 2004 14:16:24 GMT
Accept-Ranges: bytes
Access-Control-Allow-Origin: *
Date: Sun, 30 Jul 2023 06:09:00 GMT
ETag: "24c22-2c-44adde00"

<html><body><h1>It works!</h1></body></html>
```

Remedy

Configure your web server to prevent information leakage from the SERVER header of its HTTP response.

CLASSIFICATION

OWASP 2013	A5
OWASP 2017	A6
CWE	205
CAPEC	170
WASC	45
HIPAA	164.306(A), 164.308(A)
ISO27001	A.18.1.3

21. Version Disclosure (Apache)

LOW 1

Netsparker identified a version disclosure (Apache) in the target web server's HTTP response.

This information might help an attacker gain a greater understanding of the systems in use and potentially develop further attacks targeted at the specific version of Apache.

Impact

An attacker might use the disclosed information to harvest specific security vulnerabilities for the version identified.

Vulnerabilities

21.1. https://zero.webappsecurity.com/

Extracted Version

- 2.2.6

Certainty

Request

```
GET / HTTP/1.1
Host: zero.webappsecurity.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: JSESSIONID=5CF19C3A
Referer: https://zero.webappsecurity.com/
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.
77 Safari/537.36
X-Scanner: Netsparker
```

Response

Response Time (ms) : 191.9997 Total Bytes Received : 345 Body Length : 44 Is Compressed : No

```
HTTP/1.1 200 OK
Content-Type: text/html
Server: Apache/2.2.6 (Win32) mod_ssl/2.2.6 OpenSSL/0.9.8e mod_jk/1.2.40

Content-Length: 44
Last-Modified: Sat, 20 Nov 2004 14:16:24 GMT
Accept-Ranges: bytes
Access-Control-Allow-Origin: *
Date: Sun, 30 Jul 2023 06:09:00 GMT
ETag: "24c22-2c-44adde00"

<html><body><h1>It works!</h1></body></html>
```

Remedy

Configure your web server to prevent information leakage from the SERVER header of its HTTP response.

Remedy References

- Apache ServerTokens Directive

CLASSIFICATION

OWASP 2013	A5
OWASP 2017	A6
CWE	205
CAPEC	170
WASC	45
HIPAA	164.306(A), 164.308(A)
ISO27001	A.18.1.3

22. Version Disclosure (mod_ssl)

LOW 1

Netsparker identified that the target web server is disclosing the mod_ssl version in its HTTP response. This information might help an attacker gain a greater understanding of the systems in use and potentially develop further attacks targeted at the specific version of mod_ssl.

Impact

An attacker might use the disclosed information to harvest specific security vulnerabilities for the version identified.

Vulnerabilities

22.1. https://zero.webappsecurity.com/

Extracted Version

- 2.2.6

Certainty

Request

```
GET / HTTP/1.1
Host: zero.webappsecurity.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: JSESSIONID=5CF19C3A
Referer: https://zero.webappsecurity.com/
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.
77 Safari/537.36
X-Scanner: Netsparker
```

Response

Response Time (ms) : 191.9997 Total Bytes Received : 345 Body Length : 44 Is Compressed : No

```
HTTP/1.1 200 OK
Content-Type: text/html
Server: Apache/2.2.6 (Win32) mod_ssl/2.2.6 OpenSSL/0.9.8e mod_jk/1.2.40

Content-Length: 44
Last-Modified: Sat, 20 Nov 2004 14:16:24 GMT
Accept-Ranges: bytes
Access-Control-Allow-Origin: *
Date: Sun, 30 Jul 2023 06:09:00 GMT
ETag: "24c22-2c-44adde00"

<html><body><h1>It works!</h1></body></html>
```

Remedy

Configure your web server to prevent information leakage from the SERVER header of its HTTP response. To apply configuration, first make sure you have headers_module installed.
Add the following line to load the headers module in the httpd.conf

```
LoadModule headers_module modules/mod_headers.so
```

After headers_module is loaded, edit or include the following lines of config in the httpd.conf

```
ServerSignature Off
ServerTokens Prod

<IfModule mod_headers.c>
    Header unset Server
</IfModule>
```

Remedy References

- Apache Module mod_headers

CLASSIFICATION

OWASP 2013	A5
OWASP 2017	A6
CWE	205
CAPEC	170
WASC	45
HIPAA	164.306(A), 164.308(A)
ISO27001	A.18.1.3

23. Version Disclosure (OpenSSL)

LOW 1

Netsparker identified a version disclosure (OpenSSL) in target web server's HTTP response.

This information can help an attacker gain a greater understanding of the systems in use and potentially develop further attacks targeted at the specific version of OpenSSL.

Impact

An attacker might use the disclosed information to harvest specific security vulnerabilities for the version identified.

Vulnerabilities

23.1. https://zero.webappsecurity.com/

Extracted Version

- 0.9.8e

Certainty

Request

```
GET / HTTP/1.1
Host: zero.webappsecurity.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: JSESSIONID=5CF19C3A
Referer: https://zero.webappsecurity.com/
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.
77 Safari/537.36
X-Scanner: Netsparker
```

Response

Response Time (ms) : 191.9997 Total Bytes Received : 345 Body Length : 44 Is Compressed : No

```
HTTP/1.1 200 OK
Content-Type: text/html
Server: Apache/2.2.6 (Win32) mod_ssl/2.2.6 OpenSSL/0.9.8e mod_jk/1.2.40

Content-Length: 44
Last-Modified: Sat, 20 Nov 2004 14:16:24 GMT
Accept-Ranges: bytes
Access-Control-Allow-Origin: *
Date: Sun, 30 Jul 2023 06:09:00 GMT
ETag: "24c22-2c-44adde00"

<html><body><h1>It works!</h1></body></html>
```

Remedy

Configure your web server to prevent information leakage from the SERVER header of its HTTP response.

CLASSIFICATION

OWASP 2013	A5
OWASP 2017	A6
CWE	205
CAPEC	170
WASC	45
HIPAA	164.306(A), 164.308(A)
ISO27001	A.18.1.3

24. Version Disclosure (Tomcat)

LOW 1

Netsparker identified a version disclosure (Tomcat) in target web server's HTTP response.

This information can help an attacker gain a greater understanding of the systems in use and potentially develop further attacks targeted at the specific version of Tomcat.

Impact

An attacker might use the disclosed information to harvest specific security vulnerabilities for the version identified.

Vulnerabilities

24.1. http://zero.webappsecurity.com/resources/

Extracted Version

- 7.0.70

Certainty

Request

```
GET /resources/ HTTP/1.1
Host: zero.webappsecurity.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.
77 Safari/537.36
X-Scanner: Netsparker
```

Response

Response Time (ms) : 395.3092 **Total Bytes Received** : 1216 **Body Length** : 949 **Is Compressed** : No

```
HTTP/1.1 404 Not Found
Content-Type: text/html;charset=utf-8
Server: Apache-Coyote/1.1
Content-Length: 949
Content-Language: en
Access-Control-Allow-Origin: *
Date: Sun, 30 Jul 2023 06:08:57 GMT
Cache-Control: no-cache, max-age=0, must-revalidate, no-store

<html><head><title>Apache Tomcat/7.0.70 - Error report</title><style><!--H1 {font-family:Tahoma,Arial,s
ans-serif;color:white;background-color:#525D76;font-size:22px;} H2 {font-family:Tahoma,Arial,sans-seri
f;color:white;background-color:#525D76;font-size:16px;} H3 {font-family:Tahoma,Arial,sans-serif;color:w
hite;background-color:#525D76;font-size:14px;} BODY {font-family:Tahoma,Arial,sans-serif;color:black;ba
ckground-color:white;} B {font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;} P
 {font-family:Tahoma,Arial,sans-serif;background:white;color:black;font-size:12px;}A {color : black;}A.
name {color : black;}HR {color : #525D76;}--></style> </head><body><h1>HTTP Status 404 - </h1><HR size
="1" noshade="noshade"><p><b>type</b> Status report</p><p><b>message</b> <u></u></p><p><b>description</
b> <u>The requested resource is not available.</u></p><HR size="1" noshade="noshade"><h3>Apache Tomcat/
7.0.70</h3></body></html>
```

Remedy

Configure your web server to prevent information leakage from the `X-Powered-By` header of its HTTP response.

Remedy References

- OWASP Securing Tomcat

CLASSIFICATION

OWASP 2013	A5
OWASP 2017	A6
CWE	205
CAPEC	170
WASC	45
HIPAA	164.306(A), 164.308(A)
ISO27001	A.18.1.3

25. Content Security Policy (CSP) Not Implemented

BEST PRACTICE | 1

CSP is an added layer of security that helps to mitigate mainly Cross-site Scripting attacks.

CSP can be enabled instructing the browser with a Content-Security-Policy directive in a response header;

```
Content-Security-Policy: script-src 'self';
```

or in a meta tag;

```
<meta http-equiv="Content-Security-Policy" content="script-src 'self';">
```

In the above example, you can restrict script loading only to the same domain. It will also restrict inline script executions both in the element attributes and the event handlers. There are various directives which you can use by declaring CSP:

- **script-src:** Restricts the script loading resources to the ones you declared. By default, it disables inline script executions unless you permit to the evaluation functions and inline scripts by the unsafe-eval and unsafe-inline keywords.
- **base-uri:** Base element is used to resolve relative URL to absolute one. By using this CSP directive, you can define all possible URLs which could be assigned to base-href attribute of the document.
- **frame-ancestors**: It is very similar to X-Frame-Options HTTP header. It defines the URLs by which the page can be loaded in an iframe.
- **frame-src / child-src**: frame-src is the deprecated version of child-src. Both define the sources that can be loaded by iframe in the page. (Please note that frame-src was brought back in CSP 3)
- **object-src** : Defines the resources that can be loaded by embedding such as Flash files, Java Applets.
- **img-src**: As its name implies, it defines the resources where the images can be loaded from.
- **connect-src**: Defines the whitelisted targets for XMLHttpRequest and WebSocket objects.
- **default-src**: It is a fallback for the directives that mostly ends with -src suffix. When the directives below are not defined, the value set to default-src will be used instead:
    - child-src
    - connect-src
    - font-src
    - img-src
    - manifest-src
    - media-src
    - object-src
    - script-src
    - style-src

When setting the CSP directives, you can also use some CSP keywords:

- **none**: Denies loading resources from anywhere.
- **self** : Points to the document's URL (domain + port).
- **unsafe-inline**: Permits running inline scripts.
- **unsafe-eval**: Permits execution of evaluation functions such as eval().

In addition to CSP keywords, you can also use wildcard or only a scheme when defining whitelist URLs for the points. Wildcard can be used for subdomain and port portions of the URLs:

```
Content-Security-Policy: script-src https://*.example.com;
Content-Security-Policy: script-src https://example.com:*;
Content-Security-Policy: script-src https:;
```

It is also possible to set a CSP in Report-Only mode instead of forcing it immediately in the migration period. Thus you can see the violations of the CSP policy in the current state of your web site while migrating to CSP:

```
Content-Security-Policy-Report-Only: script-src 'self'; report-uri: https://example.com;
```

Impact

There is no direct impact of not implementing CSP on your website. However, if your website is vulnerable to a Cross-site Scripting attack CSP can prevent successful exploitation of that vulnerability. By not implementing CSP you'll be missing out this extra layer of security.

Vulnerabilities

25.1. http://zero.webappsecurity.com/

Certainty

Request

```
GET / HTTP/1.1
Host: zero.webappsecurity.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.
77 Safari/537.36
X-Scanner: Netsparker
```

Response

Response Time (ms) : 631.2942 **Total Bytes Received** : 12741 **Body Length** : 12471 **Is Compressed** : No

```
HTTP/1.1 200 OK
Content-Type: text/html;charset=UTF-8
Server: Apache-Coyote/1.1
Content-Language: en-US
Access-Control-Allow-Origin: *
Transfer-Encoding: chunked
Date: Sun, 30 Jul 2023 06:08:38 GMT
Cache-Control: no-cache, max-age=0, must-revalidate, no-store


<!DOCTYPE html>
<html lang="en">
<head>
    <meta charset="utf-8">
    <title>Zero - Personal Banking - Loans - Credit Cards</title>
    <meta name="viewport" content="width=device-width, initial-scale=1.0, maximum-scale=1.0, user-scala
ble=no">
    <meta http-equiv="X-UA-Compatible" content="IE=Edge">

    <link type="text/css" rel="stylesheet" href="/resources/css/bootstrap.min.css"/>
    <link type="text/css" rel="stylesheet" href="/resources/css/font-awesome.css"/>
    <link type="text/css" rel="stylesheet" href="/resources/css/main.css"/>

    <script src="/resources/js/jquery-1.8.2.min.js"></script>
        <script src="/resources/js/bootstrap.min.js"></script>

    <script src="/resources/js/placeholders.min.js"></script>
    <script type="text/javascript">
        Placeholders.init({
            live: true, // Apply to future and modified elements too
            hideOnFocus: true // Hide the placeholder when the element receives focus
        });
    </script>
    <script type="text/javascript">
        $(document).ajaxError(function errorHandler(event, xhr, ajaxOptions, thrownError) {
            if (xhr.status == 403) {
                window.location.reload();
            }
        });
    </script>
</head>
<body>
    <div class="wrapper">
    <div class="navbar navbar-fixed-top">
        <div class="navbar-inner">
            <div class="container">
                <a href="/index.html" class="brand">Zero Bank</a>
```

```
                <div>
                    <ul class="nav float-right">
                        <li>    <form action="/search.html"
          class="navbar-search pull-right" style="padding-right: 20px">
        <input type="text" id="se
…
```

Actions to Take

- Enable CSP on your website by sending the `Content-Security-Policy` in HTTP response headers that instruct the browser to apply the policies you specified.
- Apply the whitelist and policies as strict as possible.
- Rescan your application to see if Netsparker identifies any weaknesses in your policies.

Remedy

Enable CSP on your website by sending the `Content-Security-Policy` in HTTP response headers that instruct the browser to apply the policies you specified.

External References

- An Introduction to Content Security Policy
- Content Security Policy (CSP) HTTP Header
- Content Security Policy (CSP)

CLASSIFICATION

CWE	16
WASC	15
ISO27001	A.14.2.5

26. Expect-CT Not Enabled

BEST PRACTICE | 1

Netsparker identified that Expect-CT is not enabled.

Certificate Transparency is a technology that makes impossible (or at least very difficult) for a CA to issue an SSL certificate for a domain without the certificate being visible to the owner of that domain.

Google announced that, starting with April 2018, if it runs into a certificate that is not seen in Certificate Transparency (CT) Log, it will consider that certificate invalid and reject the connection. Thus sites should serve certificate that takes place in CT Logs. While handshaking, sites should serve a valid Signed Certificate Timestamp (SCT) along with the certificate itself.

Expect-CT can also be used for detecting the compatibility of the certificates that are issued before the April 2018 deadline. For instance, a certificate that was signed before April 2018, for 10 years it will be still posing a risk and can be ignored by the certificate transparency policy of the browser. By setting Expect-CT header, you can prevent misissused certificates to be used.

Vulnerabilities

26.1. https://zero.webappsecurity.com/

Certainty

Request

```
GET / HTTP/1.1
Host: zero.webappsecurity.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: JSESSIONID=5CF19C3A
Referer: https://zero.webappsecurity.com/
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.
77 Safari/537.36
X-Scanner: Netsparker
```

Response

Response Time (ms) : 191.9997 **Total Bytes Received** : 345 **Body Length** : 44 **Is Compressed** : No

```
HTTP/1.1 200 OK
Content-Type: text/html
Server: Apache/2.2.6 (Win32) mod_ssl/2.2.6 OpenSSL/0.9.8e mod_jk/1.2.40
Content-Length: 44
Last-Modified: Sat, 20 Nov 2004 14:16:24 GMT
Accept-Ranges: bytes
Access-Control-Allow-Origin: *
Date: Sun, 30 Jul 2023 06:09:00 GMT
ETag: "24c22-2c-44adde00"

<html><body><h1>It works!</h1></body></html>
```

Remedy

Configure your web server to respond with Expect-CT header.

```
Expect-CT: enforce, max-age=7776000, report-uri="https://ABSOLUTE_REPORT_URL"
```

Note: We strongly suggest you to use Expect-CT header in **report-only mode** first. If everything goes well and your certificate is ready, go with the Expect-CT enforce mode. To use **report-only mode** first, omit **enforce** flag and see the browser's behavior with your deployed certificate.

```
Expect-CT: max-age=7776000, report-uri="https://ABSOLUTE_REPORT_URL"
```

External References

- Expect-CT Extension for HTTP
- Expect-CT HTTP Header
- Expect-CT Header

CLASSIFICATION

CWE	16
WASC	15
ISO27001	A.14.1.2

27. Missing X-XSS-Protection Header

BEST PRACTICE | 1

Netsparker detected a missing `X-XSS-Protection` header which means that this website could be at risk of a Cross-site Scripting (XSS) attacks.

Impact

This issue is reported as additional information only. There is no direct impact arising from this issue.

Vulnerabilities

27.1. http://zero.webappsecurity.com/

Certainty

Request

```
GET / HTTP/1.1
Host: zero.webappsecurity.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.
77 Safari/537.36
X-Scanner: Netsparker
```

Response

Response Time (ms) : 631.2942 **Total Bytes Received** : 12741 **Body Length** : 12471 **Is Compressed** : No

```
HTTP/1.1 200 OK
Content-Type: text/html;charset=UTF-8
Server: Apache-Coyote/1.1
Content-Language: en-US
Access-Control-Allow-Origin: *
Transfer-Encoding: chunked
Date: Sun, 30 Jul 2023 06:08:38 GMT
Cache-Control: no-cache, max-age=0, must-revalidate, no-store


<!DOCTYPE html>
<html lang="en">
<head>
    <meta charset="utf-8">
    <title>Zero - Personal Banking - Loans - Credit Cards</title>
    <meta name="viewport" content="width=device-width, initial-scale=1.0, maximum-scale=1.0, user-scala
ble=no">
    <meta http-equiv="X-UA-Compatible" content="IE=Edge">

    <link type="text/css" rel="stylesheet" href="/resources/css/bootstrap.min.css"/>
    <link type="text/css" rel="stylesheet" href="/resources/css/font-awesome.css"/>
    <link type="text/css" rel="stylesheet" href="/resources/css/main.css"/>

    <script src="/resources/js/jquery-1.8.2.min.js"></script>
        <script src="/resources/js/bootstrap.min.js"></script>

    <script src="/resources/js/placeholders.min.js"></script>
    <script type="text/javascript">
        Placeholders.init({
            live: true, // Apply to future and modified elements too
            hideOnFocus: true // Hide the placeholder when the element receives focus
        });
    </script>
    <script type="text/javascript">
        $(document).ajaxError(function errorHandler(event, xhr, ajaxOptions, thrownError) {
            if (xhr.status == 403) {
                window.location.reload();
            }
        });
    </script>
</head>
<body>
    <div class="wrapper">
    <div class="navbar navbar-fixed-top">
        <div class="navbar-inner">
            <div class="container">
                <a href="/index.html" class="brand">Zero Bank</a>
```

```
                <div>
                    <ul class="nav float-right">
                        <li>    <form action="/search.html"
          class="navbar-search pull-right" style="padding-right: 20px">
        <input type="text" id="se
…
```

Remedy

Add the X-XSS-Protection header with a value of "1; mode= block".

- ```
  X-XSS-Protection: 1; mode=block
  ```

External References

- Internet Explorer 8 Security Features - MSDN
- X-XSS-Protection HTTP Header
- Internet Explorer 8 XSS Filter

CLASSIFICATION

CWE	16
WASC	15
HIPAA	164.308(A)
ISO27001	A.14.2.5
  ```

28. Referrer-Policy Not Implemented

BEST PRACTICE | 1

Netsparker detected that no Referrer-Policy header implemented.

Referrer-Policy is a security header designed to prevent cross-domain Referer leakage.

Impact

Referer header is a request header that indicates the site which the traffic originated from. If there is no adequate prevention in place, the URL itself, and even sensitive information contained in the URL will be leaked to the cross-site.

The lack of Referrer-Policy header might affect privacy of the users and site's itself

Vulnerabilities

28.1. http://zero.webappsecurity.com/

Certainty

Request

```
GET / HTTP/1.1
Host: zero.webappsecurity.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.
77 Safari/537.36
X-Scanner: Netsparker
```

Response

Response Time (ms) : 631.2942 **Total Bytes Received** : 12741 **Body Length** : 12471 **Is Compressed** : No

```
HTTP/1.1 200 OK
Content-Type: text/html;charset=UTF-8
Server: Apache-Coyote/1.1
Content-Language: en-US
Access-Control-Allow-Origin: *
Transfer-Encoding: chunked
Date: Sun, 30 Jul 2023 06:08:38 GMT
Cache-Control: no-cache, max-age=0, must-revalidate, no-store


<!DOCTYPE html>
<html lang="en">
<head>
    <meta charset="utf-8">
    <title>Zero - Personal Banking - Loans - Credit Cards</title>
    <meta name="viewport" content="width=device-width, initial-scale=1.0, maximum-scale=1.0, user-scala
ble=no">
    <meta http-equiv="X-UA-Compatible" content="IE=Edge">

    <link type="text/css" rel="stylesheet" href="/resources/css/bootstrap.min.css"/>
    <link type="text/css" rel="stylesheet" href="/resources/css/font-awesome.css"/>
    <link type="text/css" rel="stylesheet" href="/resources/css/main.css"/>

    <script src="/resources/js/jquery-1.8.2.min.js"></script>
        <script src="/resources/js/bootstrap.min.js"></script>

    <script src="/resources/js/placeholders.min.js"></script>
    <script type="text/javascript">
        Placeholders.init({
            live: true, // Apply to future and modified elements too
            hideOnFocus: true // Hide the placeholder when the element receives focus
        });
    </script>
    <script type="text/javascript">
        $(document).ajaxError(function errorHandler(event, xhr, ajaxOptions, thrownError) {
            if (xhr.status == 403) {
                window.location.reload();
            }
        });
    </script>
</head>
<body>
    <div class="wrapper">
    <div class="navbar navbar-fixed-top">
        <div class="navbar-inner">
            <div class="container">
                <a href="/index.html" class="brand">Zero Bank</a>
```

```
                <div>
                    <ul class="nav float-right">
                        <li>    <form action="/search.html"
          class="navbar-search pull-right" style="padding-right: 20px">
        <input type="text" id="se
…
```

Actions to Take

In a response header:

```
Referrer-Policy: no-referrer | same-origin | origin | strict-origin | no-origin-when-downgrading
```

In a META tag

```
<meta name="Referrer-Policy" value="no-referrer | same-origin"/>
```

In an element attribute

```
<a href="http://crosssite.example.com" rel="noreferrer"></a>
```

or

```
<a href="http://crosssite.example.com" referrerpolicy="no-referrer | same-origin | origin | strict-
origin | no-origin-when-downgrading"></a>
```

Remedy

Please implement a Referrer-Policy by using the Referrer-Policy response header or by declaring it in the meta tags. It's also possible to control referrer information over an HTML-element by using the rel attribute.

External References

- Referrer Policy
- Referrer Policy - MDN
- Referrer Policy HTTP Header
- A New Security Header: Referrer Policy
- Can I Use Referrer-Policy

CLASSIFICATION

OWASP 2013	A6
OWASP 2017	A3
CWE	200
ISO27001	A.14.2.5

29. SameSite Cookie Not Implemented

BEST PRACTICE | 1

Cookies are typically sent to third parties in cross origin requests. This can be abused to do CSRF attacks. Recently a new cookie attribute named *SameSite* was proposed to disable third-party usage for some cookies, to prevent CSRF attacks.

Same-site cookies allow servers to mitigate the risk of CSRF and information leakage attacks by asserting that a particular cookie should only be sent with requests initiated from the same registrable domain.

Vulnerabilities

29.1. http://zero.webappsecurity.com/bank/

Identified Cookie(s)

- JSESSIONID

Cookie Source

- HTTP Header

Certainty

Request

```
GET /bank/ HTTP/1.1
Host: zero.webappsecurity.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.
77 Safari/537.36
X-Scanner: Netsparker
```

Response

Response Time (ms) : 223.9967 **Total Bytes Received** : 330 **Body Length** : 0 **Is Compressed** : No

```
HTTP/1.1 302 Found
Set-Cookie: JSESSIONID=B11E0B1A; Path=/; HttpOnly

Content-Type: text/plain
Server: Apache-Coyote/1.1
Content-Length: 0
Access-Control-Allow-Origin: *
Location: http://zero.webappsecurity.com/login.html
Date: Sun, 30 Jul 2023 06:08:59 GMT
Cache-Control: no-cache, max-age=0, must-revalidate, no-store
```

Remedy

The server can set a same-site cookie by adding the `SameSite=...` attribute to the `Set-Cookie` header. There are three possible values for the `SameSite` attribute:

- Lax: In this mode, the cookie will only be sent with a top-level get request.

```
Set-Cookie: key=value; SameSite=Lax
```

- Strict: In this mode, the cookie will not be sent with any cross-site usage even if the user follows a link to another website.

```
Set-Cookie: key=value; SameSite=Strict
```

- None: In this mode, the cookie will be sent with the cross-site requests. Cookies with `SameSite=None` must also specify the `Secure` attribute to transfer them via a secure context. Setting a `SameSite=None` cookie without the `Secure` attribute will be rejected by the browsers.

```
Set-Cookie: key=value; SameSite=None; Secure
```

External References

- Security Cookies - SameSite Attribute - Netsparker
- Using the Same-Site Cookies Attribute to Prevent CSRF Attacks
- Same-site Cookies
- Preventing CSRF with the same-site cookie attribute

- SameSite cookies explained
- Get Ready for New SameSite=None; Secure Cookie Settings

CLASSIFICATION

CWE	16
WASC	15
ISO27001	A.14.2.5

30. [Possible] Login Page Identified

INFORMATION 1

Netsparker identified a login page on the target website.

Impact

This issue is reported as additional information only. There is no direct impact arising from this issue.

Vulnerabilities

30.1. http://zero.webappsecurity.com/login.html

form.id

- login_form

window.location.pathname

- /login.html

checkbox.id

- user_remember_me

input.id

- user_login

Certainty

Request

```
GET /login.html HTTP/1.1
Host: zero.webappsecurity.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Referer: http://zero.webappsecurity.com/feedback.html
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.
77 Safari/537.36
X-Scanner: Netsparker
```

Response

Response Time (ms) : 198.3096 **Total Bytes Received** : 7588 **Body Length** : 7318 **Is Compressed** : No

```
HTTP/1.1 200 OK
Content-Type: text/html;charset=UTF-8
Server: Apache-Coyote/1.1
Content-Language: en-US
Access-Control-Allow-Origin: *
Transfer-Encoding: chunked
Date: Sun, 30 Jul 2023 06:08:58 GMT
Cache-Control: no-cache, max-age=0, must-reval
…
            <div class="top_offset">


<div class="row">
    <div class="offset3 span6">
        <div class="page-header">
                <h3>Log in to ZeroBank</h3>
        </div>

        <form id="login_form" action="/signin.html" method="post" class="form-horizontal"><form id="log
in_form" action="/signin.html" method="post" class="form-horizontal">

            <div class="form-inputs">
                <div class="control-group">
                    <label class="control-label" for="user_login">Login</label>
                    <div class=
…
```

CLASSIFICATION

OWASP Proactive Controls	C6

31. Apache Web Server Identified

INFORMATION 1

Netsparker identified a web server (Apache) in the target web server's HTTP response.

Impact

This issue is reported as additional information only. There is no direct impact arising from this issue.

Vulnerabilities

31.1. http://zero.webappsecurity.com/

Certainty

Request

```
GET / HTTP/1.1
Host: zero.webappsecurity.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.
77 Safari/537.36
X-Scanner: Netsparker
```

Response

Response Time (ms) : 631.2942 **Total Bytes Received** : 12741 **Body Length** : 12471 **Is Compressed** : No

```
HTTP/1.1 200 OK
Content-Type: text/html;charset=UTF-8
Server: Apache-Coyote/1.1
Content-Language: en-US
Access-Control-Allow-Origin: *
Transfer-Encoding: chunked
Date: Sun, 30 Jul 2023 06:08:38 GMT
Cache-Control: no-cache, max-age=0, must-revalHTTP/1.1 200 OK
Content-Type: text/html;charset=UTF-8
Server: Apache-Coyote/1.1
Content-Language: en-US
Access-Control-Allow-Origin: *
Transfer-Encoding: chunked
Date: Sun, 30 Jul 2023 06:08:38 GMT
Cache-Control: no-cache, max-age=0, must-revalidate, no-store


...
```

External References

- Apache ServerTokens Directive

CLASSIFICATION

CWE	200
WASC	13
OWASP Proactive Controls	C7
ISO27001	A.18.1.3

CVSS 3.0 SCORE

Base	5.3 (Medium)
Temporal	5.1 (Medium)
Environmental	5.1 (Medium)

CVSS Vector String

CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N/E:H/RL:O/RC:C

CVSS 3.1 SCORE

Base	5.3 (Medium)
Temporal	5.1 (Medium)
Environmental	5.1 (Medium)

CVSS Vector String

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N/E:H/RL:O/RC:C

32. Default Page Detected (Apache)

INFORMATION 1

Netsparker detected the Apache default installation page.

This issue is reported for information only. If there is any other vulnerability identified regarding this resource, Netsparker will report it as a separate issue.

Vulnerabilities

32.1. https://zero.webappsecurity.com/

Certainty

Request

```
GET / HTTP/1.1
Host: zero.webappsecurity.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: JSESSIONID=5CF19C3A
Referer: https://zero.webappsecurity.com/
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.
77 Safari/537.36
X-Scanner: Netsparker
```

Response

Response Time (ms) : 191.9997 **Total Bytes Received** : 345 **Body Length** : 44 **Is Compressed** : No

```
HTTP/1.1 200 OK
Content-Type: text/html
Server: Apache/2.2.6 (Win32) mod_ssl/2.2.6 OpenSSL/0.9.8e mod_jk/1.2.40
Content-Length: 44
Last-Modified: Sat, 20 Nov 2004 14:16:24 GMT
Accept-Ranges: bytes
Access-Control-Allow-Origin: *
Date: Sun, 30 Jul 2023 06:09:00 GMT
ETag: "24c22-2c-44adde00"

<html><body><h1>It works!</h1></body></html>
```

CLASSIFICATION

CWE	200
WASC	13
OWASP Proactive Controls	C7
ISO27001	A.18.1.3

CVSS 3.0 SCORE

Base	5.3 (Medium)
Temporal	5.1 (Medium)
Environmental	5.1 (Medium)

CVSS Vector String

CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N/E:H/RL:O/RC:C

CVSS 3.1 SCORE

Base	5.3 (Medium)
Temporal	5.1 (Medium)
Environmental	5.1 (Medium)

CVSS Vector String

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N/E:H/RL:O/RC:C

33. Default Page Detected (Tomcat)

INFORMATION 1

Netsparker detected the default Tomcat page.

This issue is reported for information only. If there is any other vulnerability identified regarding this resource, Netsparker will report it as a separate issue.

Vulnerabilities

33.1. http://zero.webappsecurity.com/docs/index.html

Certainty

Request

```
GET /docs/index.html HTTP/1.1
Host: zero.webappsecurity.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: JSESSIONID=5CF19C3A
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.
77 Safari/537.36
X-Scanner: Netsparker
```

Response

Response Time (ms) : 211.5906 **Total Bytes Received** : 19630 **Body Length** : 19368 **Is Compressed** : No

```
HTTP/1.1 200 OK
Content-Type: text/html
Server: Apache-Coyote/1.1
Content-Length: 19368
Last-Modified: Wed, 15 Jun 2016 16:40:46 GMT
Accept-Ranges: bytes
Access-Control-Allow-Origin: *
Date: Sun, 30 Jul 2023 06:09:04 GMT
ETag: W/"19368
…
anges: bytes
Access-Control-Allow-Origin: *
Date: Sun, 30 Jul 2023 06:09:04 GMT
ETag: W/"19368-1466008846000"

<html><head><META http-equiv="Content-Type" content="text/html; charset=iso-8859-1"><title>Apache Tomca
t 7 (7.0.70) - Documentation Index</title><meta name="author" content="Craig R. McClanahan"><meta name
="author" content="Remy Maucherat"><meta name="author" content="Yoav Shapira"><style type="text/css" me
dia="print">
    .noPrint {display: none;}
    td#mainBody {width: 100%;}
</style><s
…
```

CLASSIFICATION

CWE	200
WASC	13
OWASP Proactive Controls	C7
ISO27001	A.18.1.3

CVSS 3.0 SCORE

Base	4.3 (Medium)
Temporal	4.1 (Medium)
Environmental	4.1 (Medium)

CVSS Vector String

CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:N/E:H/RL:O/RC:C

CVSS 3.1 SCORE

Base	4.3 (Medium)
Temporal	4.1 (Medium)
Environmental	4.1 (Medium)

CVSS Vector String

CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:N/E:H/RL:O/RC:C

34. Email Address Disclosure

INFORMATION 1

Netsparker identified an Email Address Disclosure.

Impact

Email addresses discovered within the application can be used by both spam email engines and also brute-force tools. Furthermore, valid email addresses may lead to social engineering attacks.

Vulnerabilities

34.1. http://zero.webappsecurity.com/resources/css/font-awesome.css

Email Address(es)

- dave@davegandy.com

Certainty

Request

```
GET /resources/css/font-awesome.css HTTP/1.1
Host: zero.webappsecurity.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Referer: http://zero.webappsecurity.com/
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.
77 Safari/537.36
X-Scanner: Netsparker
```

Response

Response Time (ms) : 199.1134 **Total Bytes Received** : 22118 **Body Length** : 21752 **Is Compressed** : No

```
HTTP/1.1 200 OK
Content-Type: text/css;charset=UTF-8
Server: Apache-Coyote/1.1
Expires: Wed, 30 Aug 2023 06:08:57 GMT
Content-Length: 4132
Last-Modified: Mon, 11 Feb 2013 10:57:32 GMT
Accept-Ranges: bytes
Access-Control-Allow-Origin: *
Content-Encoding:
Date: Sun, 30 Jul 2023 06:08:57 GMT
ETag: W/"21752-1360580252000"
Cache-Control:
…
 Awesome 3.0, but much appreciated:
 *    "Font Awesome by Dave Gandy - http://fortawesome.github.com/Font-Awesome"

 *  Contact
 *  ----------------------------------------------------
 *  Email: dave@davegandy.com
 *  Twitter: http://twitter.com/fortaweso_me
 *  Work: Lead Product Designer @ http://kyruus.com
 */
@font-face {
    font-family: 'FontAwesome';
    src: url('../font/fontawesome-webfont.eot?v=3.0.1
…
```

Remedy

Use generic email addresses such as contact@ or info@ for general communications and remove user/people-specific email addresses from the website; should this be required, use submission forms for this purpose.

External References

- Wikipedia - Email Spam

CLASSIFICATION

CWE	200
CAPEC	118
WASC	13
OWASP Proactive Controls	C7
ISO27001	A.9.4.1

CVSS 3.0 SCORE

Base	5.3 (Medium)
Temporal	5.3 (Medium)
Environmental	5.3 (Medium)

CVSS Vector String

CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N

CVSS 3.1 SCORE

Base	5.3 (Medium)
Temporal	5.3 (Medium)
Environmental	5.3 (Medium)

CVSS Vector String

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

35. Forbidden Resource

INFORMATION 1 CONFIRMED 1

Netsparker identified a forbidden resource.

Access to this resource has been denied by the web server. This is generally not a security issue, and is reported here for informational purposes.

Impact

This issue is reported as additional information only. There is no direct impact arising from this issue.

Vulnerabilities

35.1. http://zero.webappsecurity.com/cgi-bin/

CONFIRMED

Request

```
GET /cgi-bin/ HTTP/1.1
Host: zero.webappsecurity.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Referer: http://zero.webappsecurity.com/cgi-bin/
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.
77 Safari/537.36
X-Scanner: Netsparker
```

Response

Response Time (ms) : 223.9696 **Total Bytes Received** : 1165 **Body Length** : 961 **Is Compressed** : No

```
HTTP/1.1 403 Forbidden

Content-Type: text/html;charset=utf-8
Server: Apache-Coyote/1.1
Content-Length: 961
Content-Language: en
Access-Control-Allow-Origin: *
Date: Sun, 30 Jul 2023 06:08:58 GMT

<html><head><title>Apache Tomcat/7.0.70 - Error report</title><style><!--H1 {font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:22px;} H2 {font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:16px;} H3 {font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:14px;} BODY {font-family:Tahoma,Arial,sans-serif;color:black;background-color:white;} B {font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;} P {font-family:Tahoma,Arial,sans-serif;background:white;color:black;font-size:12px;}A {color : black;}A.name {color : black;}HR {color : #525D76;}--></style> </head><body><h1>HTTP Status 403 - </h1><HR size="1" noshade="noshade"><p><b>type</b> Status report</p><p><b>message</b> <u></u></p><p><b>description</b> <u>Access to the specified resource has been forbidden.</u></p><HR size="1" noshade="noshade"><h3>Apache Tomcat/7.0.70</h3></body></html>
```

CLASSIFICATION

OWASP Proactive Controls	C8
ISO27001	A.8.1.1

36. OPTIONS Method Enabled

INFORMATION 1 CONFIRMED 1

Netsparker detected that `OPTIONS` method is allowed. This issue is reported as extra information.

Impact

Information disclosed from this page can be used to gain additional information about the target system.

Vulnerabilities

36.1. http://zero.webappsecurity.com/

CONFIRMED

Allowed methods

- GET, HEAD, POST, PUT, DELETE, TRACE, OPTIONS, PATCH

Request

```
OPTIONS / HTTP/1.1
Host: zero.webappsecurity.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: JSESSIONID=5CF19C3A
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.
77 Safari/537.36
X-Scanner: Netsparker
```

Response

Response Time (ms) : 197.8171 **Total Bytes Received** : 283 **Body Length** : 0 **Is Compressed** : No

```
HTTP/1.1 200 OK
Content-Type: text/plain
Server: Apache-Coyote/1.1
Allow: GET, HEAD, POST, PUT, DELETE, TRACE, OPTIONS, PATCH
Content-Length: 0
Access-Control-Allow-Origin: *
Date: Sun, 30 Jul 2023 06:09:00 GMT
Cache-Control: no-cache, max-age=0, must-revalidate, no-store
```

Remedy

Disable `OPTIONS` method in all production systems.

External References

- Testing for HTTP Methods and XST (OWASP-CM-008)
- HTTP/1.1: Method Definitions

CLASSIFICATION

OWASP 2013	A5
OWASP 2017	A6
CWE	16
CAPEC	107
WASC	14
ISO27001	A.14.1.2

Show Scan Detail

Enabled Security Checks	: Apache Struts S2-045 RCE, Apache Struts S2-046 RCE, BREACH Attack, Code Evaluation, Code Evaluation (Out of Band), Command Injection, Command Injection (Blind), Content Security Policy, Content-Type Sniffing, Cookie, Cross Frame Options Security, Cross-Origin Resource Sharing (CORS), Cross-Site Request Forgery, Cross-site Scripting, Cross-site Scripting (Blind),

Cross-site Scripting (DOM based),
Custom Script Checks (Active),
Custom Script Checks (Passive),
Custom Script Checks (Per Directory),
Custom Script Checks (Singular),
Drupal Remote Code Execution,
Expect Certificate Transparency (Expect-CT),
Expression Language Injection,
File Upload,
Header Analyzer,
Heartbleed,
HSTS,
HTML Content,
HTTP Header Injection,
HTTP Methods,
HTTP Status,
HTTP.sys (CVE-2015-1635),
IFrame Security,
Insecure JSONP Endpoint,
Insecure Reflected Content,
JavaScript Libraries,
Local File Inclusion,
Login Page Identifier,
Mixed Content,
Open Redirection,
Referrer Policy,
Reflected File Download,
Remote File Inclusion,
Remote File Inclusion (Out of Band),
Reverse Proxy Detection,
RoR Code Execution,
Server-Side Request Forgery (DNS),
Server-Side Request Forgery (IP Combinations),
Server-Side Request Forgery (Pattern Based),
Server-Side Template Injection,
Signatures,
SQL Injection (Blind),
SQL Injection (Boolean),
SQL Injection (Error Based),
SQL Injection (Out of Band),
SSL,
Static Resources (All Paths),
Static Resources (Only Root Path),
Unicode Transformation (Best-Fit Mapping),
WAF Identifier,
Web App Fingerprint,
Web Cache Deception,
WebDAV,
Windows Short Filename,
XML External Entity,
XML External Entity (Out of Band)

URL Rewrite Mode : Heuristic

Detected URL Rewrite Rule(s)	: None
Excluded URL Patterns	: (log|sign)\-?(out|off) exit endsession gtm\.js WebResource\.axd ScriptResource\.axd
Authentication	: None
Scheduled	: No
Additional Website(s)	: None

This report created with 5.8.2.28358-master-3d7991d
https://www.netsparker.com