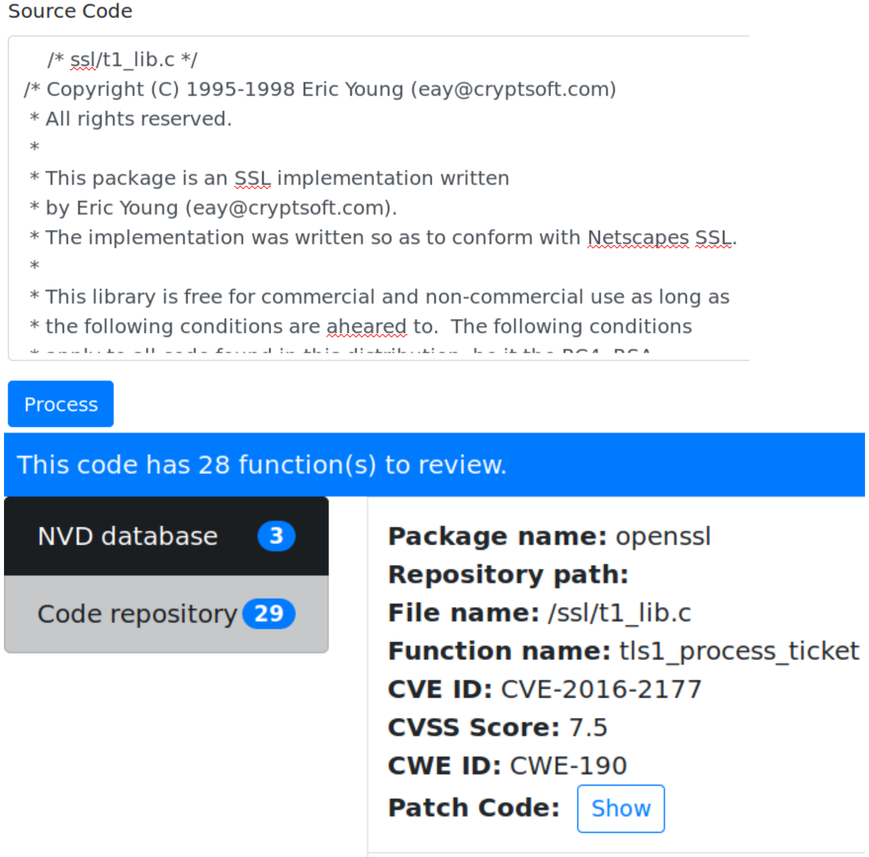
Example Result

Example Result: Code Matched 3 Vulnerabilities

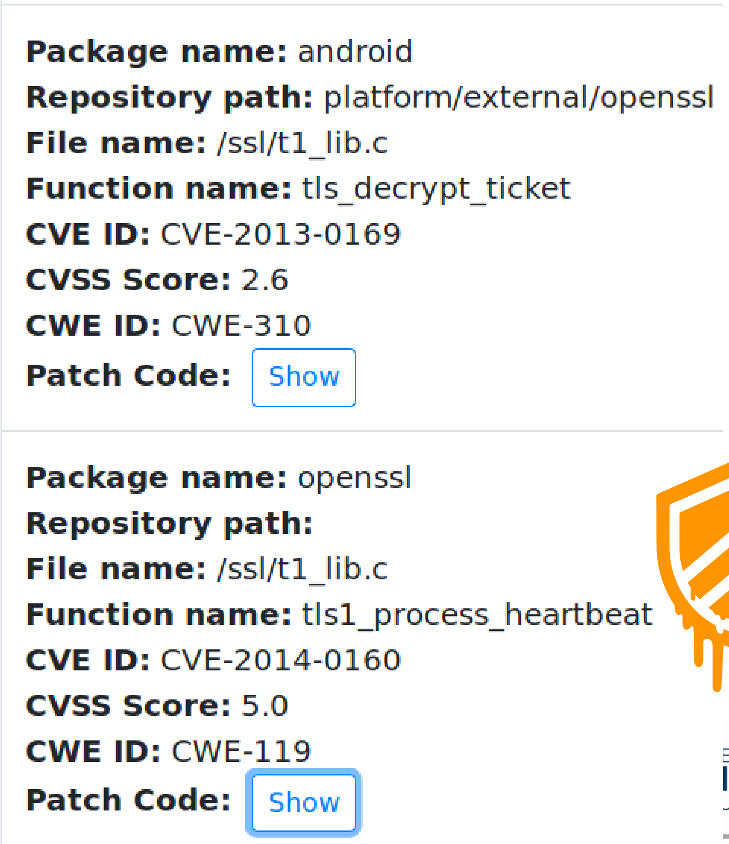


Source Code

```
    /* ssl/t1_lib.c */
/* Copyright (C) 1995-1998 Eric Young (eay@cryptsoft.com)
 * All rights reserved.
 *
 * This package is an SSL implementation written
 * by Eric Young (eay@cryptsoft.com).
 * The implementation was written so as to conform with Netscapes SSL.
 *
 * This library is free for commercial and non-commercial use as long as
 * the following conditions are aheared to.  The following conditions
 * apply to all code found in this distribution, be it the RC4, RSA
```

This code has 28 function(s) to review.

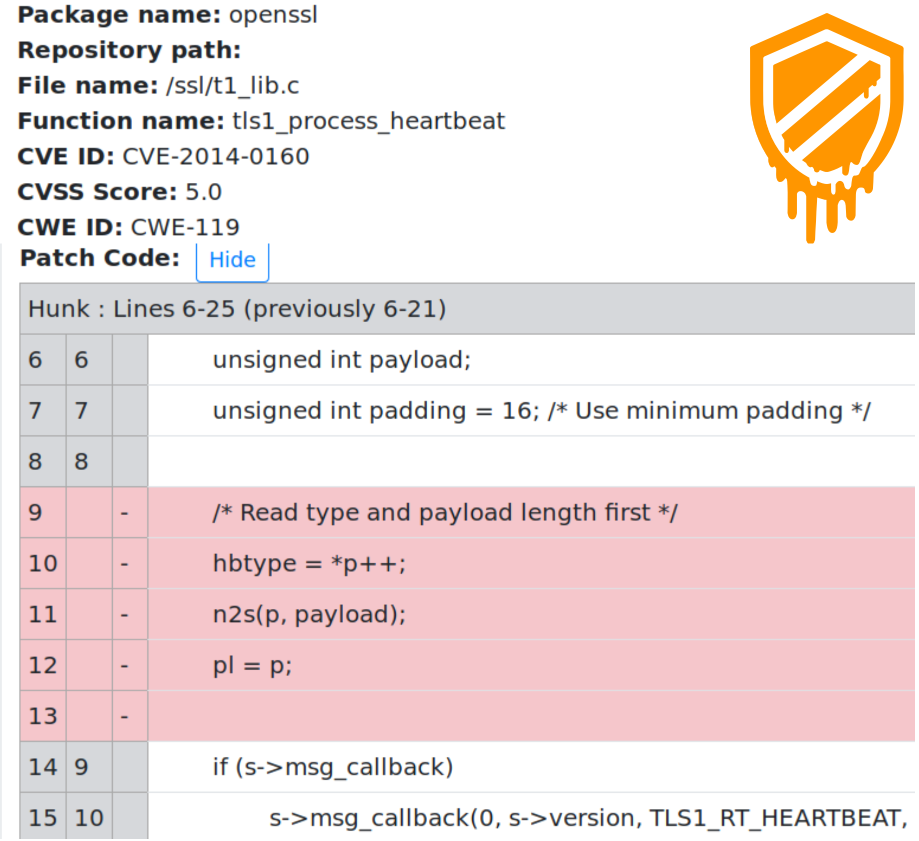
Package name: openssl
Repository path:
File name: /ssl/t1_lib.c
Function name: tls1_process_ticket
CVE ID: CVE-2016-2177
CVSS Score: 7.5
CWE ID: CWE-190
Patch Code: Show



Package name: android
Repository path: platform/external/openssl
File name: /ssl/t1_lib.c
Function name: tls_decrypt_ticket
CVE ID: CVE-2013-0169
CVSS Score: 2.6
CWE ID: CWE-310
Patch Code: Show

Package name: openssl
Repository path:
File name: /ssl/t1_lib.c
Function name: tls1_process_heartbeat
CVE ID: CVE-2014-0160
CVSS Score: 5.0
CWE ID: CWE-119
Patch Code: Show

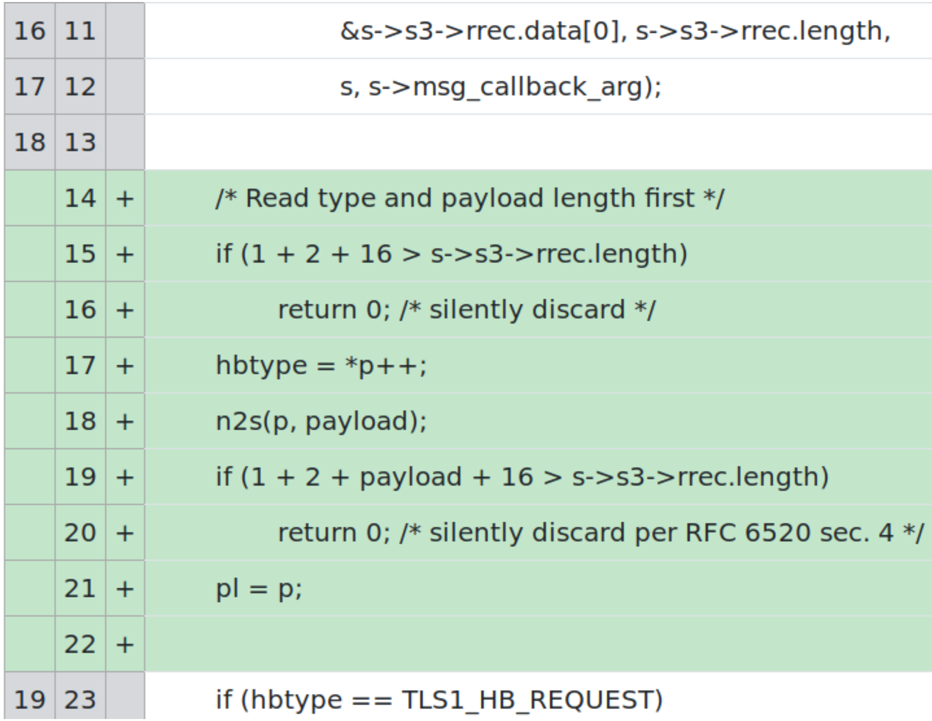
Example Result: A Matched Vulnerability And Its Fix



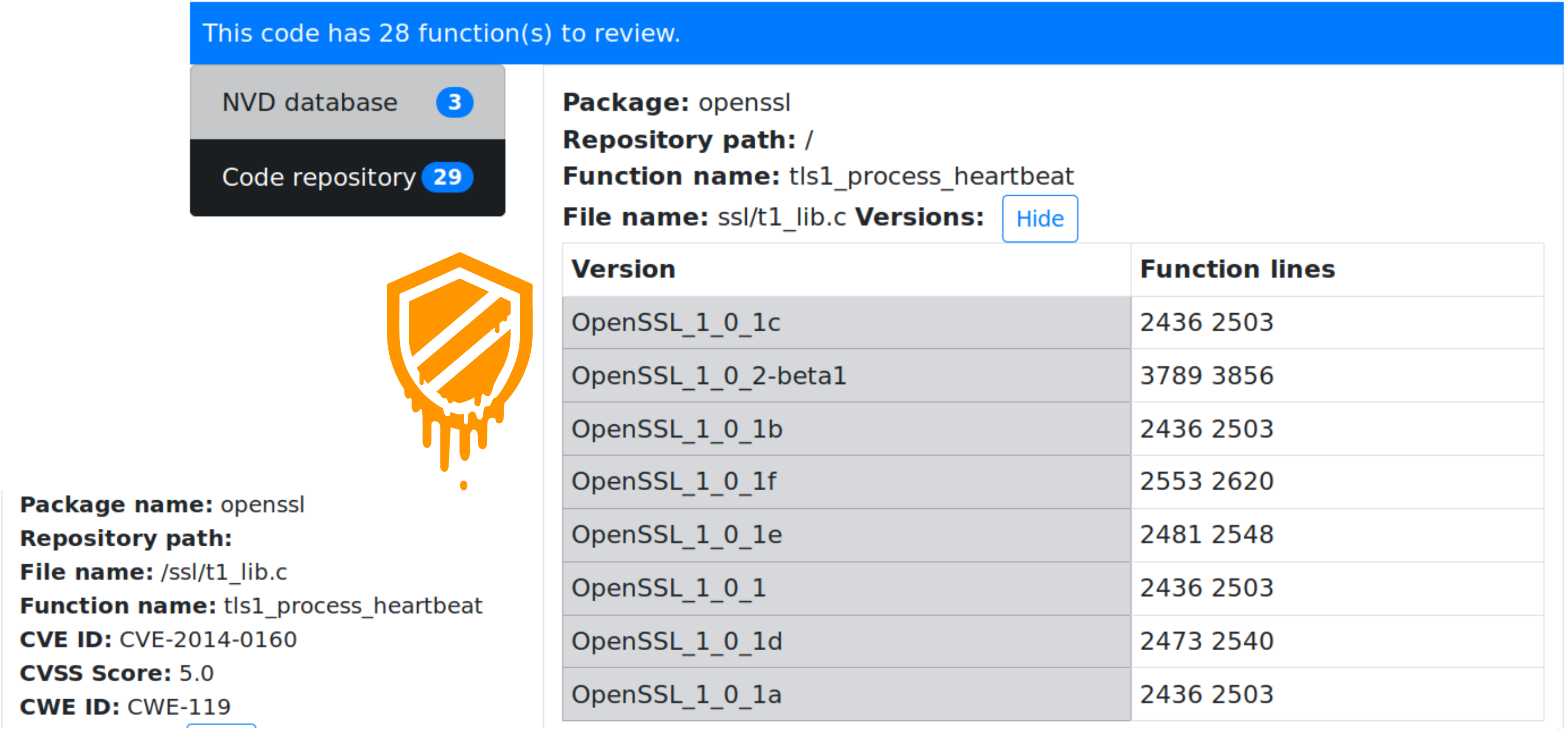
Package name: openssl
Repository path:
File name: /ssl/t1_lib.c
Function name: tls1_process_heartbeat
CVE ID: CVE-2014-0160
CVSS Score: 5.0
CWE ID: CWE-119
Patch Code: Hide

Hunk : Lines 6-25 (previously 6-21)

6	6		unsigned int payload;
7	7		unsigned int padding = 16; /* Use minimum padding */
8	8		
9		-	/* Read type and payload length first */
10		-	hbtype = *p++;
11		-	n2s(p, payload);
12		-	pl = p;
13		-	
14	9		if (s->msg_callback)
15	10		s->msg_callback(0, s->version, TLS1_RT_HEARTBEAT,
16	11		&s->s3->rrec.data[0], s->s3->rrec.length,
17	12		s, s->msg_callback_arg);
18	13		
	14	+	/* Read type and payload length first */
	15	+	if (1 + 2 + 16 > s->s3->rrec.length)
	16	+	return 0; /* silently discard */
	17	+	hbtype = *p++;
	18	+	n2s(p, payload);
	19	+	if (1 + 2 + payload + 16 > s->s3->rrec.length)
	20	+	return 0; /* silently discard per RFC 6520 sec. 4 */
	21	+	pl = p;
	22	+	
19	23		if (hbtype == TLS1_HB_REQUEST)



Example Result: Versions that are vulnerable



This code has 28 function(s) to review.

Package: openssl
Repository path: /
Function name: tls1_process_heartbeat
File name: ssl/t1_lib.c **Versions:** Hide

Version	Function lines
OpenSSL_1_0_1c	2436 2503
OpenSSL_1_0_2-beta1	3789 3856
OpenSSL_1_0_1b	2436 2503
OpenSSL_1_0_1f	2553 2620
OpenSSL_1_0_1e	2481 2548
OpenSSL_1_0_1	2436 2503
OpenSSL_1_0_1d	2473 2540
OpenSSL_1_0_1a	2436 2503

Package name: openssl
Repository path:
File name: /ssl/t1_lib.c
Function name: tls1_process_heartbeat
CVE ID: CVE-2014-0160
CVSS Score: 5.0
CWE ID: CWE-119