Alpine Linux - Bug #5209

Bug # 5206 (Closed): openssl: Multiple vulnerabilities (CVE-2016-0702, CVE-2016-0799, CVE-2016-0797, CVE-2016-0798, CVE-2016-0705, CVE-2016-0800)

[3.1] openssl: Multiple vulnerabilities (CVE-2016-0702, CVE-2016-0799, CVE-2016-0797, CVE-2016-0798, CVE-2016-0705, CVE-2016-0800)

03/01/2016 03:01 PM - Alicha CH

Status:	Closed	**Start date:**	03/01/2016
Priority:	Normal	**Due date:**	
Assignee:	Timo Teräs	**% Done:**	100%
Category:	Security	**Estimated time:**	0.00 hour
Target version:	3.1.5		
Affected versions:		**Security IDs:**	

Description

CVE-2016-0702:

A side-channel attack was found which makes use of cache-bank conflicts
on the Intel Sandy-Bridge microarchitecture which could lead to the recovery of RSA keys.
The ability to exploit this issue is limited as it relies on an attacker who has control
of code in a thread running on the same hyper-threaded core as the victim thread which is performing decryptions.

Fixed in OpenSSL 1.0.1s (**Affected 1.0.1r**, 1.0.1q, 1.0.1p, 1.0.1o, 1.0.1n, 1.0.1m, 1.0.1l,
1.0.1k, 1.0.1j, 1.0.1i, 1.0.1h, 1.0.1g, 1.0.1f, 1.0.1e, 1.0.1d, 1.0.1c, 1.0.1b, 1.0.1a, 1.0.1)

Fixed in OpenSSL 1.0.2g (**Affected 1.0.2f**, 1.0.2e, 1.0.2d, 1.0.2c, 1.0.2b, 1.0.2a, 1.0.2)

CVE-2016-0799:

The internal |fmtstr| function used in processing a "%s" format string in the
BIO_*printf functions could overflow while calculating the length of a string and cause an OOB
read when printing very long strings.

Fixed in OpenSSL 1.0.1s (**Affected 1.0.1r**, 1.0.1q, 1.0.1p, 1.0.1o, 1.0.1n, 1.0.1m, 1.0.1l, 1.0.1k, 1.0.1j,
1.0.1i, 1.0.1h, 1.0.1g, 1.0.1f, 1.0.1e, 1.0.1d, 1.0.1c, 1.0.1b, 1.0.1a, 1.0.1)

Fixed in OpenSSL 1.0.2g (**Affected 1.0.2f**, 1.0.2e, 1.0.2d, 1.0.2c, 1.0.2b, 1.0.2a, 1.0.2)

CVE-2016-0797:

In the BN_hex2bn function the number of hex digits is calculated using an int value |i|.
Later |bn_expand| is called with a value of |i * 4|. For large values of |i| this can result in |bn_expand|
not allocating any memory because |i * 4| is negative.

Fixed in OpenSSL 1.0.1s (**Affected 1.0.1r**, 1.0.1q, 1.0.1p, 1.0.1o, 1.0.1n, 1.0.1m, 1.0.1l, 1.0.1k, 1.0.1j,
1.0.1i, 1.0.1h, 1.0.1g, 1.0.1f, 1.0.1e, 1.0.1d, 1.0.1c, 1.0.1b, 1.0.1a, 1.0.1)

Fixed in OpenSSL 1.0.2g (**Affected 1.0.2f**, 1.0.2e, 1.0.2d, 1.0.2c, 1.0.2b, 1.0.2a, 1.0.2)

CVE-2016-0798:

The SRP user database lookup method SRP_VBASE_get_by_user had confusing memory management semantics;
the returned pointer was sometimes newly allocated, and sometimes owned by the callee. The calling code has no way
of distinguishing these two cases. Specifically, SRP servers that configure a secret seed to hide valid login
information are vulnerable to a memory leak: an attacker connecting with an invalid username can cause a memory
leak of around 300 bytes per connection.

Fixed in OpenSSL 1.0.1s (**Affected 1.0.1r**, 1.0.1q, 1.0.1p, 1.0.1o, 1.0.1n, 1.0.1m, 1.0.1l, 1.0.1k, 1.0.1j,
1.0.1i, 1.0.1h, 1.0.1g, 1.0.1f, 1.0.1e, 1.0.1d, 1.0.1c, 1.0.1b, 1.0.1a, 1.0.1)

Fixed in OpenSSL 1.0.2g (**Affected 1.0.2f**, 1.0.2e, 1.0.2d, 1.0.2c, 1.0.2b, 1.0.2a, 1.0.2)

CVE-2016-0705:

A double free bug was discovered when OpenSSL parses malformed DSA private keys and could lead to a DoS attack or memory corruption for applications that receive DSA private keys from untrusted sources.

Fixed in OpenSSL 1.0.1s (**Affected 1.0.1r**, 1.0.1q, 1.0.1p, 1.0.1o, 1.0.1n, 1.0.1m, 1.0.1l, 1.0.1k, 1.0.1j, 1.0.1i, 1.0.1h, 1.0.1g, 1.0.1f, 1.0.1e, 1.0.1d, 1.0.1c, 1.0.1b, 1.0.1a, 1.0.1)

Fixed in OpenSSL 1.0.2g (**Affected 1.0.2f**, 1.0.2e, 1.0.2d, 1.0.2c, 1.0.2b, 1.0.2a, 1.0.2)

CVE-2016-0800:

A cross-protocol attack was discovered that could lead to decryption of TLS sessions by using a server supporting SSLv2 and EXPORT cipher suites as a Bleichenbacher RSA padding oracle. Note that traffic between clients and non-vulnerable servers can be decrypted provided another server supporting SSLv2 and EXPORT ciphers (even with a different protocol such as SMTP, IMAP or POP) shares the RSA keys of the non-vulnerable server.

Fixed in OpenSSL 1.0.1s (**Affected 1.0.1r**, 1.0.1q, 1.0.1p, 1.0.1o, 1.0.1n, 1.0.1m, 1.0.1l, 1.0.1k, 1.0.1j, 1.0.1i, 1.0.1h, 1.0.1g, 1.0.1f, 1.0.1e, 1.0.1d, 1.0.1c, 1.0.1b, 1.0.1a, 1.0.1)

Fixed in OpenSSL 1.0.2g (**Affected 1.0.2f**, 1.0.2e, 1.0.2d, 1.0.2c, 1.0.2b, 1.0.2a, 1.0.2)

References:

https://www.openssl.org/news/vulnerabilities.html

Associated revisions

Revision efbf7307 - 03/01/2016 04:32 PM - Natanael Copa

main/openssl: security upgrade to 1.0.2g

CVE-2016-0800 [High severity]
CVE-2016-0705 [Low severity]
CVE-2016-0798 [Low severity]
CVE-2016-0797 [Low severity]
CVE-2016-0799 [Low severity]
CVE-2016-0702 [Low severity]

fixes #5209

History

#1 - 03/01/2016 04:34 PM - Natanael Copa

- Status changed from New to Resolved

- % Done changed from 0 to 100

Applied in changeset alpine:efbf730779953b8c4073582ae450f4e21632e763.

#2 - 03/02/2016 09:07 AM - Alicha CH

- Category set to Security

- Status changed from Resolved to Closed