# Alpine Linux - Bug #6756

Bug # 6755 (Closed): openssl: Multiple issues (CVE-2017-3731, CVE-2017-3732, CVE-2016-7055)

## [3.5] openssl: Multiple issues (CVE-2017-3731, CVE-2017-3732, CVE-2016-7055)

01/27/2017 09:40 AM - Alicha CH

| | | | |
|---|---|---|---|
| **Status:** | Closed | **Start date:** | 01/27/2017 |
| **Priority:** | Normal | **Due date:** | |
| **Assignee:** | | **% Done:** | 100% |
| **Category:** | Security | **Estimated time:** | 0.00 hour |
| **Target version:** | 3.5.2 | | |
| **Affected versions:** | | **Security IDs:** | |

**Description**

# CVE-2017-3731: Truncated packet could crash via OOB read

If an SSL/TLS server or client is running on a 32-bit host, and a specific
cipher is being used, then a truncated packet can cause that server or client
to perform an out-of-bounds read, usually resulting in a crash.

For OpenSSL 1.1.0, the crash can be triggered when using CHACHA20/POLY1305;
users should upgrade to 1.1.0d

For Openssl 1.0.2, the crash can be triggered when using RC4-MD5; users who have
not disabled that algorithm should update to 1.0.2k

### Fixed In Version:

**openssl 1.0.2k**, openssl 1.1.0d

### Reference:

https://www.openssl.org/news/secadv/20170126.txt

# CVE-2017-3732: BN_mod_exp may produce incorrect results on x86_64

There is a carry propagating bug in the x86_64 Montgomery squaring procedure. No
EC algorithms are affected. Analysis suggests that attacks against RSA and DSA
as a result of this defect would be very difficult to perform and are not
believed likely.

### Fixed In Version:

**openssl 1.0.2k**, openssl 1.1.0d

### Reference:

https://www.openssl.org/news/secadv/20170126.txt

# CVE-2016-7055: Montgomery multiplication may produce incorrect results

There is a carry propagating bug in the Broadwell-specific Montgomery
multiplication procedure that handles input lengths divisible by, but
longer than 256 bits. Analysis suggests that attacks against RSA, DSA
and DH private keys are impossible. This is because the subroutine in
question is not used in operations with the private key itself and an input
of the attacker's direct choice.

### Fixed In Version:

**openssl 1.0.2k**, openssl 1.1.0c

## Reference:

https://www.openssl.org/news/secadv/20170126.txt

### History

**#1 - 01/27/2017 09:55 AM - Alicha CH**

fixed in alpine:7abfb24fbe3c77b8d5d64832e928da044de29c7f

**#2 - 01/27/2017 09:56 AM - Alicha CH**

*- Status changed from New to Resolved*

*- % Done changed from 0 to 100*

**#3 - 01/27/2017 10:03 AM - Alicha CH**

*- Category set to Security*

*- Status changed from Resolved to Closed*