Systems Affected

- OpenSSL 1.0.1 through 1.0.1f
- OpenSSL 1.0.2-beta

Overview

A vulnerability in OpenSSL could allow a remote attacker to expose sensitive data, possibly including user authentication credentials and secret keys, through incorrect memory handling in the TLS heartbeat extension.

Description

OpenSSL versions 1.0.1 through 1.0.1f contain a flaw in its implementation of the TLS/DTLS heartbeat functionality. This flaw allows an attacker to retrieve private memory of an application that uses the vulnerable OpenSSL library in chunks of 64k at a time. Note that an attacker can repeatedly leverage the vulnerability to retrieve as many 64k chunks of memory as are necessary to retrieve the intended secrets. The sensitive information that may be retrieved using this vulnerability include:

- Primary key material (secret keys)
- Secondary key material (user names and passwords used by vulnerable services)
- Protected content (sensitive data used by vulnerable services)
- Collateral (memory addresses and content that can be leveraged to bypass exploit mitigations)

Exploit code is publicly available for this vulnerability. Additional details may be found in CERT/CC Vulnerability Note VU#720951.

Impact

This flaw allows a remote attacker to retrieve private memory of an application that uses the vulnerable OpenSSL library in chunks of 64k at a time.

Solution

OpenSSL 1.0.1g has been released to address this vulnerability. Any keys generated with a vulnerable version of OpenSSL should be considered compromised and regenerated and deployed after the patch has been applied. US-CERT recommends system administrators consider implementing Perfect Forward Secrecy to mitigate the damage that may be caused by future private key disclosures.

References

- OpenSSL Security Advisory
- The Heartbleed Bug(link is external)
- CERT/CC Vulnerability Note VU#720951
- Perfect Forward Secrecy
- RFC2409 Section 8 Perfect Forward Secrecy

Revisions

- Initial Publication