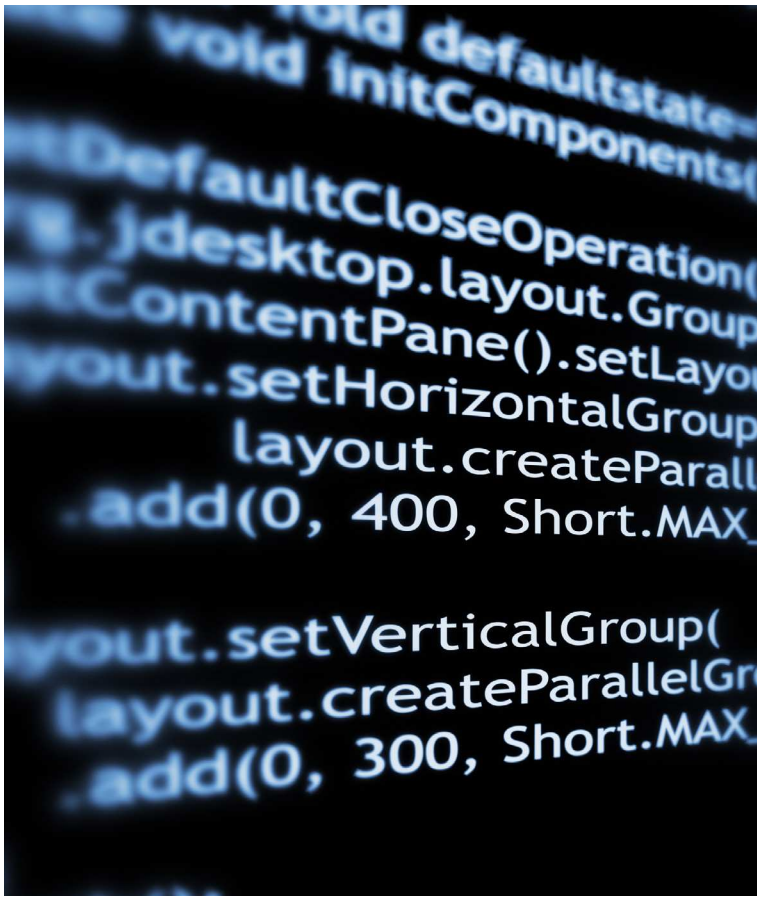
Mitigations for OpenSSL TLS/DTLS Heartbeat Extension Vulnerability

A serious vulnerability (CVE-2014-0160) exists in OpenSSL's implementation of the TLS/DTLS heartbeat extension. Exploitation of this vulnerability results in a leak of memory contents. Such exploitation may compromise encryption keys, authentication keys, user credentials, and other data from TLS/DTLS clients and servers. The affected versions of OpenSSL software are versions 1.0.1 through 1.0.1f. Versions prior to 1.0.1 are unaffected and versions 1.0.1g and later have implemented a fix for the vulnerability.

Mitigation Actions:

- Upgrade affected TLS/DTLS clients and servers to OpenSSL version 1.0.1g. Alternatively, affected versions of OpenSSL may be recompiled with the option "-DOPENSSL_NO_HEARTBEATS".
- Numerous operating systems and client and server software incorporate OpenSSL. If you use TLS/DTLS you may be vulnerable depending on if OpenSSL is used within the software and depending on the version of OpenSSL used. Contact your software vendor to determine whether your software is vulnerable and, if so, for an update that fixes the vulnerability.
- For any systems that are affected by this vulnerability, use TLS/DTLS, and have exposure to Internet connectivity for potential exploitation of this vulnerability, revoke and reissue certificates and other credentials utilized on those systems *after applying the update.*



Contact Information

Industry Inquiries: 410-854-6091

USG/IC Client Advocates: 410-854-4790

DoD/Military/COCOM Client Advocates: 410-854-4200

General Inquiries: **niasc@nsa.gov**