WHITEPAPER

SYNOPSYS®

# Diary of a Heartbleed

# TABLE OF CONTENTS

... a variety of consequences might occur such as crashes, denial of service, security exposures, degradation of service, thrashing, or anomalous behavior.

Our fuzzing team has used this technique before and have several other open source vulnerabilities. These include:

- Numerous flaws in ASN.1/SNMP in 2001/2002
- Apache IPv6-URI flaw in 2004
- Numerous flaws in image formats in 2005
- Numerous flaws in XML libraries in 2009
- Several flaws in Linux Kernel IPv4 and SCTP in 2010
- RSA signature verification vulnerability in strongSwan in 2012
- Several OpenSSL and GnuTLS vulnerabilities in 2004, 2008, 2012, and 2014

## What is the Heartbeat protocol?

In a typical SSL connection, the client and server establish a secure (meaning encrypted) line of communication. The peer sends a heartbeat request and the other peer responds by sending a copy of the request's payload. The use of the Heartbeat extension is negotiated during the TLS handshake. During this process, the client may send a Datagram Transport Layer Security (DTLS) message to make sure the other peer is still alive.

Heartbleed is notØ Ø Ø Ø Ø Ø Ø Ø Ø Ø Ø Ø Ø Ø Ø Ø Ø Ø ä ä eḾ tæ