Threat Update Service* Advisory

Protection Pack 2014-04-09-03 Released April 9, 2014

Purpose: The Corero Security Active Response Team has issued this Prevention Advisory to protect customers against known attacks targeting the OpenSSL Heartbeat Vulnerability.

Issue: TLS and DTLS implementations in OpenSSL do not properly handle Heartbeat extension packets, thereby allowing a remote attacker to gain access to sensitive information, like private keys, from process memory via specially crafted Heartbeat requests.

Recommended Action: Apply the specified Protection Pack (or any later one) and ensure the associated rule is used to inspect traffic to the affected product infrastructure.

Issue Identifier	CVE-2014-0160
Advisory	http://git.openssl.org/gitweb/?p=openssl.git;a=commit;h=96db9023b881d7cd9f379b0c154650d6c108e9a3
Risk Assessment	Critical Vulnerability
Threat Impact	Remotely exploitable vulnerability that could allow an attacker to gain access to sensitive information on an unprotected system.
Affected Products	OpenSSL 1.0.1 before 1.0.1g
Corero Products	IPS and DDS 5500 E-Series v6.60 (build 047 and later), v6.61 (build 021 and later), v6.62 (build 007 and later), v6.80 (build 035 and later).
Associated Rule	tln-106850
Associated Rule Set	This rule has to be specifically configured.

* previously called TopResponse

http://support.corero.com Corero Network Security, Inc.
One Cabot Road, Hudson, MA 01749 +1 978.212.1500 • Fax +1 978.212.1600
• USA • Japan • Asia Pacific • EMEA