Threat Update Service* Advisory

Protection Pack 2014-06-16-01 Released June 16, 2014

Purpose: The Corero Security Active Response Team has issued this Prevention Advisory to protect customers against known attacks targeting the OpenSSL DTLS Fragment CVE-2014-0195 Buffer Overflow DoS Vulnerability.

Issue: OpenSSL does not properly validate fragment lengths in DTLS ClientHello messages. This could allow an attacker to cause a denial of service on the affected system via a long non-initial fragment.

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-2014-0195
Advisory	https://git.openssl.org/gitweb/?p=openssl.git;a=commit;h=1632ef744872edc2aa2a53d487d3e79c965a4ad3
Risk Assessment	Critical Vulnerability
Threat Impact	Remotely exploitable vulnerability that could allow an attacker to cause a denial of service on an unprotected system.
Affected Products	OpenSSL before 0.9.8za, 1.0.0 before 1.0.0m, and 1.0.1 before 1.0.1h
Corero Products	IPS 5500 EC-Series and IPS 5500 ES-Series v6.60 (build 047 and later), v6.61 (build 021 and later), v6.82 (build 003 and later), v6.80 (build 035 and later).
Associated Rule	tln-106888
Associated Rule Set	This rule needs to be enabled manually and requires special configuration.

* 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 Copyright 2014. All Rights Reserved.