Threat Update Service* Advisory

Protection Pack 2014-06-27-02 Released June 27, 2014

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

Issue: An injection vulnerability exists in OpenSSL. This could allow an attacker to carry out a man-in-the-middle attack by injecting arbitrary ChangeCipherSpec messages and hijacking sessions.

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-2014-0224
Advisory	https://access.redhat.com/site/blogs/766093/posts/908133
Risk Assessment	Important Vulnerability
Threat Impact	Remotely exploitable vulnerability that could allow an attacker to hijack sessions and obtain sensitive information.
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 / DDS 5500 EC-Series and IPS / DDS 5500 ES-Series v6.60 (build 047 and later), v6.61 (build 021 and later), v6.80 (build 035 and later), v6.82 (build 003 and later).
Associated Rule	tln-022195
Associated Rule Set	This rule needs to be manually enabled 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