Threat Update Service* Advisory

Protection Pack 2013-11-11-01 Released November 11, 2013

Purpose: The Corero Security Active Response Team has issued this Prevention Advisory to protect customers against known attacks targeting the Apple Motion Remote Integer Overflow Vulnerability.

Issue: An integer overflow vulnerability exists in the OZDocument::parseElement function in Apple Motion. This could allow a remote attacker to cause a denial of service via a very small or very large value in the subview attribute of a viewer element in a .motn file.

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-2013-6114
Advisory	http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2013-6114
Risk Assessment	Critical Vulnerability
Threat Impact	Remotely exploitable vulnerability that could allow an attacker to cause a denial of service.
Affected Products	Apple Motion 5.0.7
Corero Products	IPS 5500 E-Series v5.34 (build 005 and later), v6.60 (build 047 and later), v6.61 (build 021 and later), v6.80 (build 035 and later).
Associated Rule	tln-106736
Associated Rule Set	This rule is automatically enabled in the “Recommended Client Protection” rule set.

\

* previously called TopResponse

https://support.corero.com Corero Network Security, Inc.
One Cabot Road, Hudson, MA 01749 +1 978.212.1500 • Fax +1 978.212.1600