Threat Update Service* Advisory

Protection Pack 2014-01-23-01 Released January 23, 2014

Purpose: The Corero Security Active Response Team has issued this Prevention Advisory to protect customers against known attacks targeting the Mozilla Firefox exposedProps XCS CVE-2013-1710 Code Execution Vulnerability.

Issue: A remote code execution vulnerability exists in the crypto.generateCRMFRequest function in Mozilla Firefox. This could allow the attacker to execute arbitrary code on the affected system via a crafted Certificate Request Message Format (CRMF) request.

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-2013-1710
Advisory	http://www.mozilla.org/security/announce/2013/mfsa2013-69.html
Risk Assessment	Important Vulnerability
Threat Impact	Remotely exploitable vulnerability that could allow an attacker to execute arbitrary code on an unprotected system.
Affected Products	Mozilla Firefox before 23.0 Firefox ESR 17.x before 17.0.8 Thunderbird before 17.0.8 Thunderbird ESR 17.x before 17.0.8 SeaMonkey before 2.20
Corero Products	IPS 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-025228
Associated Rule Set	This rule is automatically enabled in the “Recommended Client Protection” rule set.

* previously called TopResponse

