Threat Update Service* Advisory

Protection Pack 2014-12-04-04 Released December 5, 2014

Purpose: The Corero Security Active Response Team has issued this Prevention Advisory to protect customers against known attacks targeting the F5 Networks BIG-IP XML External Entity Injection Vulnerability.

Issue: An XML external entity injection vulnerability exists in the configuration utility in F5 BIG-IP LTM. This could allow an attacker to read arbitrary files and cause a denial of service via a crafted request using (1) viewList or (2) deal elements. An attacker who successfully exploited this vulnerability could take complete control of an affected system.

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-2014-6032
Advisory	https://support.f5.com/kb/en-us/solutions/public/15000/600/sol15605.html
Risk Assessment	Critical Vulnerability
Threat Impact	Remotely exploitable vulnerability that could allow an attacker to execute arbitrary code on an unprotected system.
Affected Products	F5 BIG-IP LTM, ASM, GTM, Link Controller and other products
Corero Products	IPS 5500 EC-Series and IPS 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-106987
Associated Rule Set	This rule is automatically enabled in the “Recommended Server Protection” rule set.

* previously called TopResponse

