Threat Update Service* Advisory

Protection Pack 2014-05-22-02 Released May 23, 2014

Purpose: The Corero Security Active Response Team has issued this Prevention Advisory to protect customers against known attacks targeting the F5 iControl CVE-2014-2928 Remote Command Execution Vulnerability.

Issue: A remote command execution vulnerability exists in the F5 iControl API. This could allow an attacker to execute arbitrary code on the victim's machine via shell metacharacters in the hostname element in a SOAP request. 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-2014-2928
Advisory	http://support.f5.com/kb/en-us/solutions/public/15000/200/sol15220.html
Risk Assessment	Critical Vulnerability
Threat Impact	Remotely exploitable vulnerability that could allow an attacker to execute arbitrary commands on an unprotected system.
Affected Products	The iControl API in F5 BIG-IP LTM, APM, ASM, GTM, Link Controller, and PSM 10.0.0 through 10.2.4 and 11.0.0 through 11.5.1, BIG-IP AAM 11.4.0 through 11.5.1, BIG-IP AFM and PEM 11.3.0 through 11.5.1, BIG-IP Analytics 11.0.0 through 11.5.1, BIG-IP Edge Gateway, WebAccelerator, WOM 10.1.0 through 10.2.4 and 11.0.0 through 11.3.0, Enterprise Manager 2.1.0 through 2.3.0 and 3.0.0 through 3.1.1, and BIG-IQ Cloud, Device, and Security 4.0.0 through 4.3.0
Corero Products	IPS 5500 EC-Series and IPS 5500 ES-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-106870
Associated Rule Set	This rule is automatically enabled in the "Strict Server Protection" rule set.

* previously called TopResponse

