Apache Struts 2 FreeMarker tag Remote Code Execution (CVE-2017-12611)

Gal Goldshtein, 2017-10-09

In the recent days, another 0-day remote code execution vulnerability in Apache Struts 2 has been published (CVE-2017-12611). This time the vulnerability's root cause is not a bug in the Struts 2 framework, but a feature of the FreeMarker Template Language, which is a popular template language being commonly used in Apache Struts and other Java based projects, being misused by the application developers. The feature allows developers to bind the values of the parameters that are being passed to the server by the application users to the application inner declared variables. This evaluation of the user's input allows attackers to send an Object Graph Navigation Language (OGNL) expressions which are supported by the Struts 2 framework to the server and their evaluation may lead to malicious code being executed on the server. Examples for such misuse of this feature can be found in the original bulletin posted by the Apache Struts 2 team (S2-053).

A few proof of concept exploits for this vulnerability have already been published and are available for download over the web.

Mitigating the 0-day with BIG-IP ASM

BIG-IP ASM customers under any supported BIG-IP version are already protected against this 0-day vulnerability, as the exploitation attempt will be detected by the existing JAVA code injection and command execution attack signatures which can be found in signature sets that include "Command Execution" and "Server Side Code Injection" attack types or "Java Servlets/JSP" System.

The existing signatures are being proactive by detecting any attacker's code injection or OS command execution attempts, without relying on specific 0day trigger that might allow the attacker to push this payload, making the application protection resistant to many future 0day vulnerabilities.

At least 10 attack signatures were triggered by each attempt to exploit a protected Struts 2 application using the already available exploits, following are few of the ASM logs of the blocked attempts:

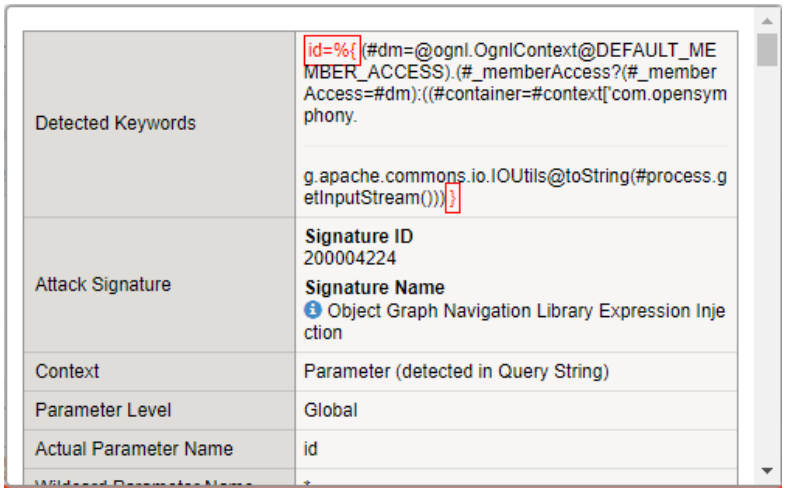
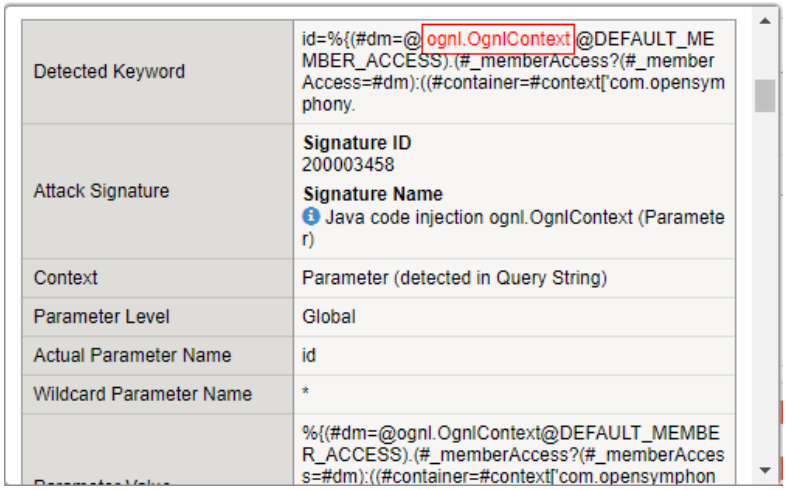
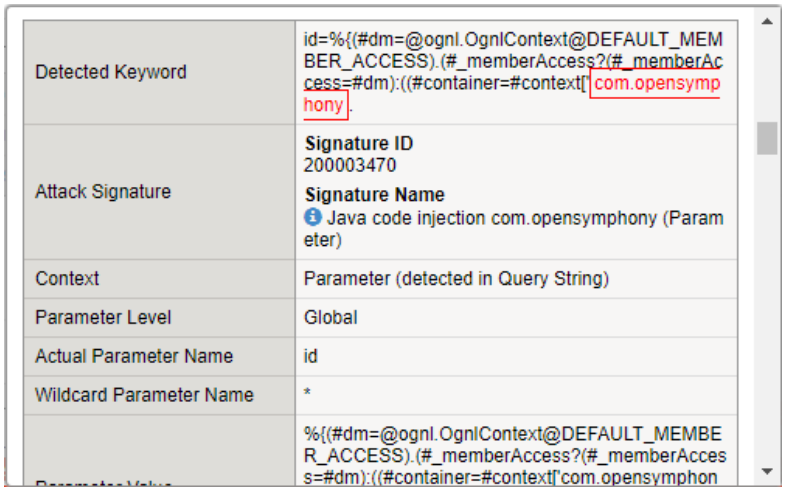


Figure 1: *Exploit blocked with Attack Signature (200004224)*



Detected Keyword	id=%{(#dm=@ognl.OgnlContext@DEFAULT_MEMBER_ACCESS).(#_memberAccess?(#_memberAccess=#dm):((#container=#context['com.opensymphony.
Attack Signature	**Signature ID** 200003458 **Signature Name** Java code injection ognl.OgnlContext (Parameter)
Context	Parameter (detected in Query String)
Parameter Level	Global
Actual Parameter Name	id
Wildcard Parameter Name	*
	%{(#dm=@ognl.OgnlContext@DEFAULT_MEMBER_ACCESS).(#_memberAccess?(#_memberAccess=#dm):((#container=#context['com.opensymphon

Figure 2: *Exploit blocked with Attack Signature (200003458)*



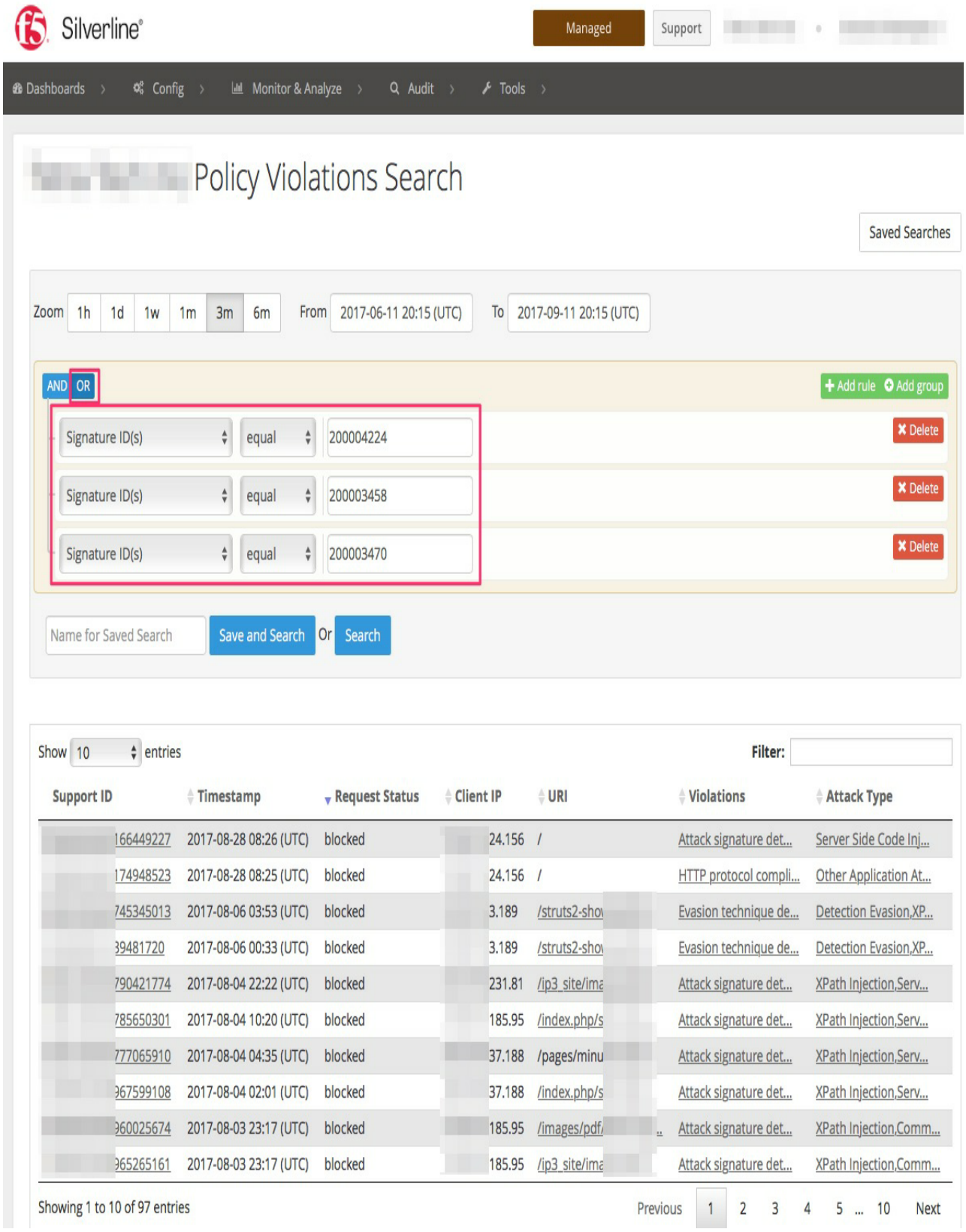
Detected Keyword	id=%{(#dm=@ognl.OgnlContext@DEFAULT_MEMBER_ACCESS).(#_memberAccess?(#_memberAccess=#dm):((#container=#context['com.opensymphony.
Attack Signature	**Signature ID** 200003470 **Signature Name** Java code injection com.opensymphony (Parameter)
Context	Parameter (detected in Query String)
Parameter Level	Global
Actual Parameter Name	id
Wildcard Parameter Name	*
	%{(#dm=@ognl.OgnlContext@DEFAULT_MEMBER_ACCESS).(#_memberAccess?(#_memberAccess=#dm):((#container=#context['com.opensymphon

Figure 3: *Exploit blocked with Attack Signature (200003470)*

Mitigating the 0-day with F5 Silverline WAF

Much like on-prem BIG-IP ASM customers, F5 Silverline WAF customers are already protected against this 0-day vulnerability. The exploitation attempt will be detected by the existing JAVA code injection and command execution attack signatures built within Silverline WAF standard policies.

The following is a WAF Policy Violations Search that shows blocked requests that match the Signature IDs representative of CVE-2017-12611:


Silverline
Managed
Support
Dashboards
Config
Monitor & Analyze
Audit
Tools
Policy Violations Search
Saved Searches
Zoom 1h 1d 1w 1m 3m 6m
From 2017-06-11 20:15 (UTC)
To 2017-09-11 20:15 (UTC)
AND OR
+ Add rule
Add group
Signature ID(s) equal 200004224
Signature ID(s) equal 200003458
Signature ID(s) equal 200003470
Delete
Delete
Delete
Name for Saved Search
Save and Search
Or
Search
Show 10 entries
Filter:
Support ID
Timestamp
Request Status
Client IP
URI
Violations
Attack Type
166449227 2017-08-28 08:26 (UTC) blocked 24.156 / Attack signature det... Server Side Code Inj...
174948523 2017-08-28 08:25 (UTC) blocked 24.156 / HTTP protocol compli... Other Application At...
745345013 2017-08-06 03:53 (UTC) blocked 3.189 /struts2-sho Evasion technique de... Detection Evasion,XP...
39481720 2017-08-06 00:33 (UTC) blocked 3.189 /struts2-sho Evasion technique de... Detection Evasion,XP...
790421774 2017-08-04 22:22 (UTC) blocked 231.81 /ip3_site/ima Attack signature det... XPath Injection,Serv...
785650301 2017-08-04 10:20 (UTC) blocked 185.95 /index.php/s Attack signature det... XPath Injection,Serv...
777065910 2017-08-04 04:35 (UTC) blocked 37.188 /pages/minu Attack signature det... XPath Injection,Serv...
967599108 2017-08-04 02:01 (UTC) blocked 37.188 /index.php/s Attack signature det... XPath Injection,Serv...
960025674 2017-08-03 23:17 (UTC) blocked 185.95 /images/pdf/ .. Attack signature det... XPath Injection,Comm...
965265161 2017-08-03 23:17 (UTC) blocked 185.95 /ip3_site/ima Attack signature det... XPath Injection,Comm...
Showing 1 to 10 of 97 entries
Previous 1 2 3 4 5 ... 10 Next

F5 Networks, Inc. | 401 Elliot Avenue West, Seattle, WA 98119 | 888-882-4447 | f5.com

F5 Networks, Inc.
Corporate Headquarters
info@f5.com

F5 Networks
Asia-Pacific
apacinfo@f5.com

F5 Networks Ltd.
Europe/Middle-East/Africa
emeainfo@f5.com

F5 Networks
Japan K.K.
f5j-info@f5.com