S2-062

Summary

Forced OGNL evaluation, when evaluated on raw not validated user input in tag attributes, may lead to remote code execution - same as S2-061.

Who should read this	All Struts 2 developers and users
Impact of vulnerability	Possible Remote Code Execution vulnerability
Maximum security rating	Important
Recommendation	Upgrade to Struts 2.5.30 or greater
Affected Software	Struts 2.0.0 - Struts 2.5.29
Reporters	Chris McCown
CVE Identifier	CVE-2021-31805

Problem

The fix issued for CVE-2020-17530 (S2-061) was incomplete. Still some of the tag's attributes could perform a double evaluation if a developer applied forced OGNL evaluation by using the `%{...}` syntax. Using forced OGNL evaluation on untrusted user input can lead to a Remote Code Execution and security degradation.

Solution

Avoid using forced OGNL evaluation on untrusted user input as recommended in the Security Guide! You can upgrade to Struts 2.5.30 or greater which checks if expression evaluation won't lead to the double evaluation, yet this isn't ultimate solution and still forced expression evaluation can lead to security degradation.

DISCLAIMER

Struts won't accept double evaluation issues caused by not validated end-user input (owing to developer error) anymore as vulnerability. We accepted this one as vulnerability because it's about an error in our previously accepted vulnerability. We welcome and appreciate reports in this regard to minimize developer error effect albeit!

Backward compatibility

No issues expected when upgrading to Struts 2.5.30

Workaround

Do not use forced OGNL evaluation in the tag's attributes based on untrusted/unvalidated user input, please follow out recommendations from the Security Guide.