S2-008

Summary

Multiple critical vulnerabilities in Struts2

Who should read this	All Struts 2 developers
Impact of vulnerability	Remote command execution and arbitrary file overwrite, Strict DMI does not work correctly
Maximum security rating	Critical
Recommendation	Developers should immediately upgrade to Struts 2.3.1.1 or read the following solution instructions carefully for a configuration change to mitigate the vulnerability
Affected Software	Struts 2.1.0 - Struts 2.3.1
Original JIRA Ticket	WW-3729
Reporter	Johannes Dahse, SEC Consult Vulnerability Lab and Bruce Phillips (blog post)
CVE Identifier	
Original Description	Reported directly to security@struts.a.o and Struts 2 Security Vulnerability - Dynamic Method Invocation

Problem

To prevent attackers calling arbitrary methods within parameters the flag `xwork.MethodAccessor.denyMethodExecution` is set to `true` and the `SecurityMemberAccess` field `allowStaticMethodAccess` is set to `false` by default. Also, to prevent access to context variables an improved character whitelist for parameter names is applied in the `ParameterInterceptor` since Struts 2.2.1.1:

```
acceptedParamNames = "[a-zA-Z0-9\.][()_']+";
```

Under certain circumstances these restrictions can be bypassed to execute malicious Java code.

1. **Remote command execution in Struts <= 2.2.1.1 (`ExceptionDelegator`)**
   When an exception occurs while applying parameter values to properties, the value is evaluated as an OGNL expression. For example, this occurs when setting a string value to an integer property. Since the values are not filtered an attacker can abuse the power of the OGNL language to execute arbitrary Java code leading to remote command execution. This issue has been reported (https://issues.apache.org/jira/browse/WW-3668) and was fixed in Struts 2.2.3.1. However the ability to execute arbitrary Java code has been overlooked.
2. **Remote command execution in Struts <= 2.3.1 (`CookieInterceptor`)**
   The character whitelist for parameter names is not applied to the `CookieInterceptor`. When Struts is configured to handle cookie names, an attacker can execute arbitrary system commands with static method access to Java functions. Therefore the flag `allowStaticMethodAccess` can be set to true within the request.
3. **Arbitrary File Overwrite in Struts <= 2.3.1 (`ParameterInterceptor`)**
   While accessing the flag `allowStaticMethodAccess` within parameters is prohibited since Struts 2.2.3.1 an attacker can still access public constructors with only one parameter of type String to create new Java objects and access their setters with only one parameter of type String. This can be abused in example to create and overwrite arbitrary files. To inject forbidden characters into a filename an uninitialized string property can be used.
4. **Remote command execution in Struts <= 2.3.1 (`DebuggingInterceptor`)**
   While not being a security vulnerability itself, please note that applications running in developer mode and using the `DebuggingInterceptor` are prone to remote command execution as well. While applications should never run in developer mode during production, developers should be aware that doing so not only has performance issues (as documented) but also a critical security impact.

Solution

It is strongly recommended to upgrade to Struts 2.3.1.1, which contains the corrected classes.

Update to Struts 2.3.1 and apply a stronger `acceptedParamNames` filter to the `ParameterInterceptor` and `CookieInterceptor`:

```
acceptedParamNames = "[a-zA-Z0-9\.][()_']+";
```