Yet Another Java Service Wrapper Bugs

Install java, groovy and native applications as services or daemons

Brought to you by: john1900, rzorzorzo

#166 XXE Vulnerability in JnlpSupport of YAJSW

Milestone: All
Status: closed-fixed
Owner: rzo
Labels: None
Priority: 7
Updated: 2020-09-20
Created: 2019-08-27
Creator: Alexandru Gabriel Blanaru
Private: No

The code in JnlpSupport takes a file as parameter in the constructor and creates a Document from it using a DocumentBuilderFactory and DocumentBuilder instance without making any checks for XXE.

Vulnerable code is in the parseJnlp function:

```
private Document parseJnlp(final InputStream in) throws ParserConfigurationException, SAXException, IOException {
Document doc = null;
final DocumentBuilderFactory factory = DocumentBuilderFactory.newInstance();
factory.setValidating(false);
factory.setNamespaceAware(false);
final DocumentBuilder builder = factory.newDocumentBuilder();
doc = builder.parse(in);
return doc;
}
```

Any services which use this wrapper are potentially vulnerable.

In depth Proof-of-Concept using Ghidra Reverse Engineering Framework's Server:
https://github.com/purpleracc00n/Exploits-and-PoC/blob/master/XXE%20in%20YAJSW%E2%80%99s%20JnlpSupport%20affects%20Ghidra%20Server.md

I would suggest applying the OWASP guidance regarding this kind of issues:
https://cheatsheetseries.owasp.org/cheatsheets/XML_External_Entity_Prevention_Cheat_Sheet.html

Discussion

Alexandru Gabriel Blanaru - *2019-08-27*

Note: The Proof-of-Concept repository will be available after the fix is issued.

rzo - *2020-09-20*

fixed release: 12.15

rzo - *2020-09-20*

- **status:** open --> closed-fixed

Log in to post a comment.