New issue

Jump to bottom

XXE Vulnerability in JnlpSupport of YAJSW affects Ghidra Server #943

Closed **purpleracc00n** opened this issue on Aug 27, 2019 · 2 comments

Labels **Feature: Server** **Type: Security**

purpleracc00n commented on Aug 27, 2019 • edited

Describe the bug
XXE vulnerability in YAJSW's JnlpSupport affects Ghidra Server.

An insecure way to parse XML input was found in JnlpSupport class from Yet Another Java Service Wrapper used by Ghidra (up to latest version).

To Reproduce
Steps to reproduce the behavior:

1. Create an XXE payload file and set the extension of the file to ".jnlp"
2. Go to <path_to_ghidra>/server/ghidraSvr
3. Modify "WRAPPER_CONF" value to point to the ".jnlp" file
4. Run ghidraSvr using "$ sudo ./ghidraSvr start"
5. XXE exploit in the ".jnlp" file gets executed

Expected behavior
Extended XML Entities should be disabled.

Environment:

- OS: Kali Linux, Debian 4.19.37-2kali1 (2019-05-15)
- Java Version: 11.0
- Ghidra Version: 9.0.4

Additional context
I understand the vulnerable code is actually part of a separate library, however I considered this of interest and I suggest adding a filter so no ".jnlp" configuration files are allowed as values for "WRAPPER_CONF", at least until YAJSW patches this problem.

More PoC (Available after the fix is confirmed): https://github.com/purpleracc00n/Exploits-and-PoC/blob/master/XXE%20in%20YAJSW%E2%80%99s%20JnlpSupport%20affects%20Ghidra%20Server.md

purpleracc00n added the Type: Bug label on Aug 27, 2019

ryanmkurtz added **Type: Security** **Feature: Server** and removed Type: Bug labels on Sep 20, 2019

ghidra1 commented on Nov 17, 2020 Collaborator

I am rather confused by the write-up. Could you please explain how this is exploitable without modification to files contained within the Ghidra installation. If modification to files contained within the installation is considered possible, then any jar could be replaced and do just about anything.

ryanmkurtz closed this as completed on Dec 22, 2021

ryanmkurtz commented on Dec 22, 2021 Collaborator

If an attacker has write-access to the Ghidra installation directory, we do not consider malicious behavior that results from manipulation of those Ghidra files a vulnerability.

Assignees
No one assigned

Labels
Feature: Server **Type: Security**

Projects
None yet

Milestone
No milestone

Development
No branches or pull requests

3 participants