

A pre-authenticated RCE exploit for Inductive Automation Ignition

GPL-3.0 license

36 stars 8 forks

Star

Notifications

<> Code

Issues 1

Pull requests

Actions

Projects

Security

...

main

Go to file



stevenseeley updated to add RCE cve ...

on Jul 18 18

[View code](#)

README.md

Randy

What

This is a pre-authenticated RCE exploit for Inductive Automation Ignition that impacts versions $\leq 8.1.16$. We failed to exploit the bugs at Pwn2Own Miami 2022 because we had a sloppy exploit and no debug environment, but since then we have found the time and energy to improve it!

Authors

Chris Anastasio and Steven Seeley (mr_me) of Incite Team

Build

1. Build with `mvn clean compile assembly:single -DskipTests`

Tested

The exploit was tested against [8.1.16](#) using the Windows 64-bit Installer which you can [download here](#) (SHA1: f135d32228793c73c4cdd88561cdbdb44b19290c) but it has known to work against other older versions as well.

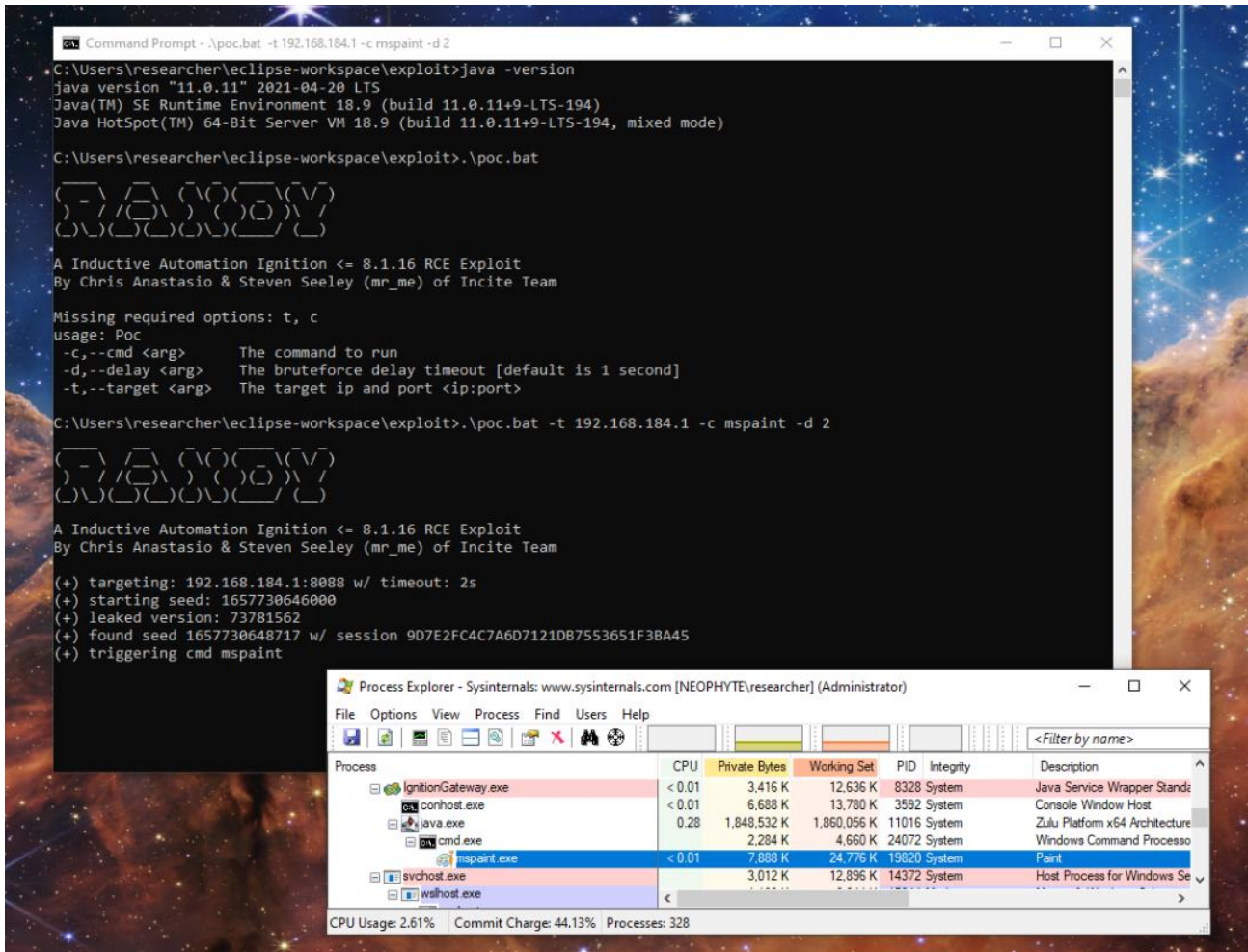
Notes

- At the time of release, no CVE's were assigned to the bugs
- This exploit takes advantage of two vulnerabilities that have been [patched](#):
 - [CVE-2022-35890 - GatewaySessionManagerImpl Authentication Bypass](#)
 - [CVE-2022-36126 - ScriptInvoke Remote Code Execution](#)
- The exploit requires an admin user to be logged into the gateway. During testing it was found that sessions live forever unless a user explicitly logs out.
- The exploit should be ran from a Windows host (due to the `SecureRandom` seed prediction attack).
- The exploit targets Ignition deployed under Windows, since `SecureRandom` is not so secure under that environment.
- The exploit was tested with Java v11.0.11.

Run

Run the exploit with `java -cp target/andy-0.0.1-SNAPSHOT.jar com.srcincite.ia.exploit.Poc`

Example



Releases

No releases published

Packages

No packages published

Contributors 2



stevenseeley (mr_me) of 360 Vulnerability Research Institute



sourceincite Source Incite

Languages

● **Java** 99.4% ● **Batchfile** 0.6%