Bug Bytes #152 – SSRF via Gateway actuator, Flickr account takeover & Writeup of NSO's iMessage RCE

BY ANNA HAMMOND · DECEMBER 22, 2021 · LAST UPDATED ON AUGUST 14, 2025

Bug Bytes is a weekly newsletter curated by members of the bug bounty community. The first series is curated by Mariem, better known as **PentesterLand.** Every week, she keeps us up to date with a comprehensive list of write-ups, tools, tutorials and resources.

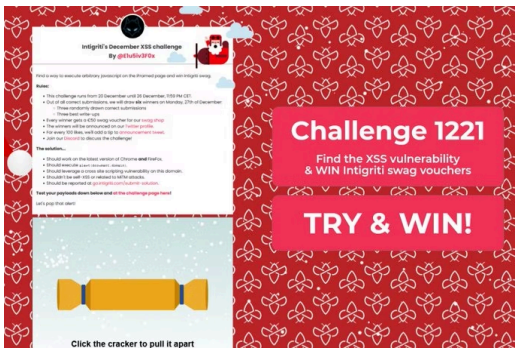
CLICK HERE TO SUBSCRIBE

This issue covers the week from December 13 to 20.

Last Bug Bytes of the year

This is the last Bug Bytes of the year as I am taking a week off to recharge. The next issue will be in the first week of January 2022.

Intigriti news



Intigriti's December XSS challenge By @E1u5iv3F0x

21 things that happened in 2021 at Intigriti: a year of milestones

© Intigriti

Our favorite 5 hacking items

1. Articles of the week

Bring Your Own SSRF – The Gateway Actuator
A deep dive into an NSO zero-click iMessage exploit: Remote Code Execution

@wdahlenb investigated the Spring Boot Gateway actuator (aka '/actuator/gateway') and shares all the details: How the actuator works, why it could be exploited for SSRF and Denial of Service, and why other bug hunters seem to have missed it.

The second article is of an entirely different kind. It is a breakdown by Google's Project Zero of FORCEDENTRY, the infamous NSO zero-click iMessage RCE.
The exploit is sent as a GIF that hides a PDF which uses JBIG2 (an old compression algorithm) to build a virtual CPU. Incredible.

2. Writeup of the week

Flickr Account Takeover (Flickr, $7,550)

@_lauritz_ found weaknesses in Flick's implementation of OpenID Connect, and was able to exploit them to take over any account without user interaction. The writeup details everything and makes for a great read if you are interested in authentication vulnerabilities.

3. Tutorial of the week

Why is Exposing the Docker Socket a Really Bad Idea?

Why does an exposed Docker socket on Linux grant root access to the host?
If this question tickles your curiosity, you will probably enjoy this very detailed and well-written article.

4. Tips of the week

Hashing a URL in Java triggers a DNS lookup, and this has been weaponized to exploit Java deserialization bugs
Enumerating Files Using Server Side Request Forgery and the request Module (via @Agarri_FR)

I read in a Twitter thread that hashing a URL in Java triggers a DNS lookup as part of the hash function. All comments said that this is a really bad won't fix bug, but I couldn't understand why... until I saw @aaditya_purani's explanation.
The DNS lookups triggered by hashing URLs can be used to detect and exploit insecure deserialization bugs (see Triggering a DNS lookup using Java Deserialization for details).

Another old trick that I've just discovered is that the Request Node.js module supports a special URL format, **http://unix:PATH-TO-FILE**, that returns different errors if the file exists or not.
So, if you find an SSRF in a Node.js app that uses Requests, this behavior can be used to enumerate files on the remote file system.

© Intigriti

5. Vulnerabilities of the week

CVE-2021-45046, CVE-2021-4104 & CVE-2021-45105 (new Log4j CVEs)

Last week, I mentioned that the original Log4Shell bug had a bypass that was a Denial of Service. It turned out to also be an RCE. There is also a new Log4j Denial of Service vulnerability, which brings us to a total of four bugs:

CVE	Vulnerability Type	Affected Log4j Versions	Non-Default Config
CVE-2021-44228	RCE	2.0 through 2.14.1	No
CVE-2021-45046	Denial of Service (DoS) and RCE	2.0 through 2.15.0	Yes
CVE-2021-4104	RCE	1.2*	Yes
CVE-2021-45105	Denial of Service (DoS)	2.0-beta9 to 2.16.0	Yes

Source: Tenable blog

CVE-2021-44228 is the most critical since it is the only one that applies to the default configuration.

To help make sense of all the new related resources, here are some that I found particularly interesting or creative:

- @LiveOverflow discusses Log4j features, JNDI and why the bug wasn't discovered earlier
- @LiveOverflow's special announcement for bug bounty hunters
- Video explanation of the Log4j bugs by @gregxsunday
- A written tutorial for those who prefer reading
- Polymorphic Log4J exploit that is a valid JSON REST API request
- log4JFrida: Tool that modifies all characteristics of an Android device to return a Log4j payload instead.
- Log4Shell Everywhere: A fork of Collaborator Everywhere, with the injection parameters changed to payloads for Log4j CVE-2021-44228.
- Log4Shell detection mindmap
- Root cause of CVE-2021-45105

For more, take a look at pentesterland/Log4Shell.

SHARE ON TWITTER

© Intigriti

Other amazing things we stumbled upon this week

Videos

- I became a bug bounty millionaire! (Just for a day)
- How To Exploit a Heap Overflow
- Holiday Mayhem: Hacking Battlegrounds #3
- "December Tip of the Day" series by @hacksplained
- Privilege Escalation series by @0xConda
- Red Teaming – Local Domain Admin Impersonation (Mitm6 & LDAP Relay) (in Arabic)

Webinars

- BHIS | Modern C2 and Data Exfiltration w/ Kyle Avery

Conferences

- CHCon 2021

Tutorials

Medium to advanced

- Use cryptography in mobile apps the right way
- Tunnelling For Offensive Security
- Scanning Shell Scripts With Semgrep
- Quick & Lazy Malware Development

Beginners corner

- Android Application Testing Using Windows 11 and Windows Subsystem for Android
- Creating Lists for Brute Force Attacks Using Python
- OSINT Username generation guide

Writeups

Challenge writeups

- NCC Group's Cryptopals Guided Tour!

© Intigriti

- Clickjacking chained with DOM-Based XSS!
- IDOR, PCAP analysis & RCE? Cap by @Hack The Box
- HackThebox – Static
- SSRF – Lab #2 Basic SSRF against another back-end system, Lab #3 SSRF with blacklist-based input filter & Lab #4 SSRF with whitelist-based input filter

Responsible(ish) disclosure writeups

- Yes, fun browser extensions can have vulnerabilities too! #Web #BrowserExtension
- Proctorio Chrome extension Universal Cross-Site Scripting #Web #BrowserExtension
- Getting root on Ubuntu through wishful thinking #Linux #MemoryCorruption
- Failed02 Pulse Secure VPN and Guacamole WebSocket Hooking #VPN #Websockets

Bug bounty writeups

- Exploiting HTML-to-PDF Converters through HTML Imports
- How I was able to reveal page admin of almost any page on Facebook (Facebook, $4,500)
- Blackbox Cookie Testing — How I Cracked The Admin's Cookie
- GHSL-2021-1053: Path traversal in Grafana REST API – CVE-2021-43813, CVE-2021-43815 (Grafana Labs)
- Zero day path traversal vulnerability in Grafana 8.x allows unauthenticated arbitrary local file read (Aiven Ltd, $1,000)
- RCE in Visual Studio Code's Remote WSL for Fun and Negative Profit (Microsoft)

See more writeups on The list of bug bounty writeups.

Tools

- dns-exfil: Custom DNS logger that can be used for exfiltration (e.g. when testing for Log4Shell)
- WhoEnum: Mass querying whois records
- AD Enum: Python tool to find misconfigurations via LDAP and exploit some of those weaknesses with kerberos
- Reverse Shell Generator & Intro: Bash script to generate reverse shells
- Oh365 User Finder: Python3 o365 User Enumeration Tool

Tips & Tweets

- Advice for struggling bug bounty hunters

© Intigriti

- PNG that has different content when viewed on Apple devices vs other machines
- How to build and run john-jumbo with mpi support using homebrew on macOS with an Apple Silicon chip
- Detecting prototype pollution with CodeQL

Misc. pentest & bug bounty resources

- ThinkstScapes Quarterly – Q4 2021 & Audio roundup
- Introduction to Azure Penetration Testing
- The Hacker Tools
- aufzayed/bugbounty
- CaledoniaProject/awesome-opensource-security

Challenges

- Intigriti's December XSS challenge By @E1u5iv3F0x
- bug-hunting-101 #BinaryExploitation
- Snippet of code vulnerable to XSS. How would you exploit it?

Bug bounty & Pentest news

- Bug bounty
  - CodeQL: Updates to the Bug Slayer bug bounty program
  - Meta: Charting the future of our bug bounty program
  - GitLab: 2021: Smashing bugs and dropping names
- Tool updates
  - Mozilla: Preventing secrets from leaking through Clipboard
  - New WebKit Features in Safari 15.2 (Added support for COOP/COEP HTTP Headers))
  - Improving GitHub code search

Non technical

- A strategy to land your first pentest job
- When is a Scrape a Breach?

© Intigriti

REQUEST A DEMO

intigriti.com/demo

VISIT THE WEBSITE

intigriti.com

GET IN TOUCH

hello@intigriti.com

© Intigriti