Bug Bytes #120 – MacOS pwned, Homebrew RCE & The world's shortest backdoor

BY ANNA HAMMOND · APRIL 28, 2021 · LAST UPDATED ON MARCH 6, 2025

Want to read the latest version? Visit the link below:
https://www.intigriti.com/researchers/blog/bug-bytes/bug-bytes-120-macos-pwned-homebrew-rce-the-worlds-shortest-backdoor

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 19 to 26 of April.

Our favorite 5 hacking items

1. Videos of the week

Why you should Close Your Files | Binary Exploitation 0x02
How SUDO on Linux was HACKED! // CVE-2021-3156

I'm more into Web/API/mobile hacking, but sometimes other types of InfoSec resources are so good it makes me want to change fields! It's the case with these two videos.

The first one is part of a new binary exploitation series by PwnFunction. It provides a beginner friendly introduction to file descriptors, what they are and how they can be abused.

The second video is a walkthrough of CVE-2021-3156 (Baron Samedit), why it wasn't obsvious to detect with fuzzing and was hiding in plain sight for almost a decade. These are interesting but complex topics that only @LiveOverflow could make so fun!

2. Writeups of the week

All Your Macs Are Belong To Us & macOS Gatekeeper Bypass (2021 Edition) (Apple)
Remote code execution in Homebrew by compromising the official Cask repository (Homebrew)

@cedowens found a pretty bad bug that allowed malicious apps to basically bypass MacOS's security mechanisms (File Quarantine, Gatekeeper, and Notarization Requirements). It's already exploited in the wild. @patrickwardle confirmed the findings and published a detailed analysis on the root cause of the bug. Make sure to update your OS before diving into this!

@ryotkak disclosed a Remote Code Execution in Homebrew (a popular macOS package manager). A bug in the git_diff library made it possible to trick a repo's maintainers into approving malicious pull requests. Users who installed the infected package would have had their system compromised.

3. Tools of the week

HTTP Methods Discloser
gsocket.io

HTTP Methods Discloser is a Burp extension to easily check which HTTP methods are available. It replays each request with the OPTIONS verb and adds all methods available in the request's "Comment" column (in the Proxy History). It's a handy tool to be aware of available HTTP verbs for all requests.

gsocket (or Global Socket) is a tookit that allows workstations behind NAT/Firewall to establish a TCP connection with each other "like there is no firewall". It has different applications. One of them is deploying a reverse login shell with a single command, without a server. The shell is accessible remotely through NAT/firewalls. It's powerful, and pretty useful for CTF and pentest!

4. Challenge of the week

Intigriti's 0421 XSS challenge winners and writeups, Source code & Walkthrough by @terjanq (who created the challenge)

This is a hard XSS challenge by XSS and XS-Leaks master @terjanq. The cool thing is that the source code is available to play with even though the challenge has ended. There is also a bunch of writeups and different solutions to guide you.
It's a nice opportunity to learn techniques that @terjanq used for a real WAF bypass.

5. Resource of the week

Offensive Security Guide to SSH Tunnels and Proxies

This is a one-page guide on SSH tunnels and SOCKS proxies. It's a good reference for those engagements where you're short on time and need to quickly remember which tunnel/proxy to use and how to do it.

Other amazing things we stumbled upon this week

Videos

- DON'T BUY MY HOW TO GET STARTED IN BUG BOUNTY COURSE! – Do these 500+ FREE exercises & Blog post
- HOW TO HACK "THE MAINFRAME" ! (for real)
- Hacking Oauth Applications – Pt. 1
- bsidesahmedabad AMA with Farah Hawa
- Hacking WPA3 with Mathy Vanhoef & Retia

Podcasts

- DAY[0] Episode 74 – Bad Patches, Fuzzing Sockets, & 3DS Hacked by Super Mario
- The Mystery of AS8003 – Remembering Dan Kaminski, Project Zero, Unethical Security Research

Webinars

- Attack Detection Fundamentals 2021

Conferences

- INFILTRATE Virtual Speaker Series: Attacking Xerox Multifunction Printers

Slides & Workshop material

- Pen Testing API Security in the Web & Cloud

Tutorials

Medium to advanced

- Exploiting Race conditions with Nuclei & Vulnerable PHP app
- Examining JavaScript Inter-Process Communication in Firefox
- Azure Application Proxy C2
- What's in a private key?
- Spoofing credential dialogs on macOS, Linux and Windows
- Finding Buried Treasure in Server Message Block (SMB)

Beginners corner

- A deep dive into Task Hijacking in Android
- Remote Code Execution on Jinja – SSTI Lab
- Hacking GraphQL for Fun and Profit — Part 1 — Understanding GraphQL Basics & Part 2— Methodology and Examples
- SSH Sniffing (SSH Spying) Methods and Defense
- Smart Contract Security for Pentesters

Writeups

Challenge writeups

- SQL Injection – Lab #8 SQLi attack, querying the database type and version on MySQL & Microsoft #video

Responsible(ish) disclosure writeups

- Hacking 3,000,000 apps at once through CocoaPods
- CVE-2021-27736: XXE in FusionAuth SAML Library & Detection with Burp SAML Raider

- Uncovering and Disclosing a Signature Spoofing Vulnerability in Windows Installer: CVE-2021-26413 #Windows
- CVE-2021-22204: ExifTool vulnerable to arbitrary code execution when parsing malicious images (no PoC yet) #Web
- CVE-2020-36287: Jira information disclosure
- NAME:WRECK
- CVE-2021-21315: Node.JS command injection & PoC

0-day & N-day vulnerabilities

- Check Your Pulse: Suspected APT Actors Leverage Authentication Bypass Techniques and Pulse Secure Zero-Day #LDAP
- Zero-Day Exploits in SonicWall Email Security Lead to Enterprise Compromise #Web
- Microsoft Exchange From Deserialization to Post-Auth RCE (CVE-2021–28482)

Bug bounty writeups

- New Clubhouse Security Vulnerabilities Could Happen to Any Growing Unicorn (Clubhouse)
- CVE-2021-30481: Source engine remote code execution via game invites (Valve, $8,000)
- You Talking To Me? (Google)
- Stored XSS via malicious key value of Synthetics monitor tag when visiting an Insights dashboard with filtering enabled (New Relic, $2,123)
- RCE in 'Copy as Node Request' BApp via code injection (PortSwigger Web Security)
- Brave — Stealing your cookies remotely (Brave, $500)
- Shopify Account Takeover $22500 Bug Bounty (Shopify, $22,500) #video
- Github Open Redirect to Reflected XSS Poc 4000$ (GitHub, $4,000) #video

See more writeups on The list of bug bounty writeups.

Tools

- h1stats: h1 Program Stats Scraper
- EDD & Intro: Domain enumeration tool in .NET
- Marauders Map & Intro: The internal attacker toolkit heavily inspired by SharpPack
- Traitor: Automatic Linux privesc via exploitation of low-hanging fruit e.g. gtfobins

Tips & Tweets

- SSO recon to expand attack surface

- Discovering assets behind a load balancer
- 403/401 bypass techniques
- Hiding “external sender” email warnings with HTML and CSS
- Remote LSASS dump without touching local disk

Misc. pentest & bug bounty resources

- Secure Code Wiki by Payatu
- Top 12 Bug Bounty Browser Extensions
- JSON Web Token Security Cheat Sheet
- WordPress Plugin Security Testing Cheat Sheet
- SQLiZine

Challenges

- Hack the Amazon Interview (ends on May 3)

Articles

- Recorded logins in Burp Scanner
- Remote debuggers as an attack vector
- Unintentionally exposing your organization to MFA bypasses on Azure Active Directory
- Bypassing LSA Protection in Userland & PPLdump
- Exploiting vulnerabilities in Cellebrite UFED and Physical Analyzer from an app’s perspective & Cellebrite Good Times, Come On: Reverse-Engineering Phone Forensics Tools

Bug bounty & Pentest news

- Understanding The Tools/scripts You Use In A Pentest #OSCP
- Dan Kaminsky: Tributes pour in for security researcher who died after short illness
- Stanford student finds glitch in ransomware payment system to save victims $27,000
- Researchers Secure Bug Bounty Payout to Help Raise Funds for Infant’s Surgery
- Ill-advised research on Linux kernel lands computer scientists in hot water
- Tools updates:
  - S3Scanner updated to support “nearly any non-AWS S3-compatible APIs like Dreamhost/DigitalOcean/Linode/etc”
  - Burp Professional / Community 2021.4.2

    - Commix now detects OS command injection in GraphQL
- Upcoming talks:
    - Hunting for IDORs with Katie Paxton-Fear (May 2)
    - May Lightning Conference: Hacking APIs for Beginners (May 12)
    - July Lightning Conference: Beyond the Bounty (JULY 20)

Non technical

- Pentesting: What I should have done
- Ethical conduct in cybersecurity research
- Interview with a bug bounty hunter: Youssef Sammouda

Community pick of the week

Impressive, @pudsec, well done!

Do you also have bug bounty wins, swag and joys to share with other Bug Bytes readers? Tag us on social media, we love to hear from you!