Bug Bytes #88 – How @orange_8361 hacked Facebook (again), Privilege escalation in Microsoft's Netlogon & HTTP request smuggling via HTTP/2

BY ANNA HAMMOND · SEPTEMBER 16, 2020 · LAST UPDATED ON MARCH 6, 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.

This issue covers the week from 04 to 11 of September.

Our favorite 5 hacking items

1. Article of the week

h2c Smuggling: Request Smuggling Via HTTP/2 Cleartext (h2c) & h2cSmuggler

Using HTTP/2 used to mitigate HTTP Request Smuggling vulnerabilities. That was until Jake Miller (@theBumbleSec) came up with this variant that leverages HTTP/2 over cleartext (h2c) connections. The idea is to upgrade the HTTP/1.1 connection to HTTP/2 by sending an h2c upgrade header. If the backend server is compatible, the TCP tunnel created is unmanaged, allowing you to bypass the reverse proxy access controls.
This works on HAProxy, Nuster, and Traefik's default reverse proxy configurations.

The Git repo provides a tool and demo to reproduce the attack.

2. Writeups of the week

How I Hacked Facebook Again! Unauthenticated RCE on MobileIron MDM

[Blog] Zerologon: instantly become domain admin by subverting Netlogon cryptography (CVE-2020-1472), Official testing script & NCC's .NET exploit

Zerologon (CVE-2020-1472) is a CVSS-10 privilege escalation vulnerability in Microsoft's Netlogon authentication process. It is caused by a flaw in the cryptographic implementation of AES encryption. The reason it is making headlines is its ease of exploitation and critical impact: It allows attackers with unauthenticated network access to Domain Controllers, to obtain Domain Admin privileges and take over Active Directory domains.

The second writeup is about @orange_8361's new research on Facebook's MobileIron MDM. He found an RCE using JNDI injection, Authentication bypass and Arbitrary file reading. It is interesting to read how he turns Black box testing into White box testing, and revives his old "Breaking Parser Logic" attack.

3. Videos of the week

Full Time Bug Hunting with Alex Chapman
Interview With @akita_zen || Bug Bounty Methodology, Avoiding Dupes & Staying Zen

@InsiderPhD interviews @ajxchapman about full time bug hunting, with a focus on strategy, risk managament and financial planning. It's cool to get a peak at the life of a full-time bug hunter and how he makes it sustainable.

@farah_hawa01's interview with @akita_zen is about all things recon, methodology, avoind dupes, favorite personal findings, subdomain takeovers, advice for beginners, etc.

4. Resource of the week

XXE bruteforce wordlist

XXE aficionados, this wordlist is for you! Pieter Hiele (@honoki) shared his XXE bruteforce list that includes 65 payloads. It's worth checking out as he knows something about XXE (considering his past writeups).

5. Tools of the week

CloudBrute, ProxyFor & Intro

CloudBrute is a new Go tool for enumerating a target's resources on cloud providers (including Amazon, Google, Microsoft, DigitalOcean, Alibaba, Vultr and Linode). It takes a keyword (for example the domain or company name) and a wordlist, builds a list of potential URLs by doing mutations, then tests which ones are live and accessible based on their status code.

The only API key needed is a free IPINFO key, and a second tool (ProxyFor) was also released to help with bypassing rate and region limitations.

Other amazing things we stumbled upon this week

Videos

- JavaScript Prototype Pollution – Part 1
- Deep Link Route and Validation Bypasses
- 5 Reasons you suck at Bug Bounties
- Axiom – Detailed Tutorial | Step-by-Step Setup & Usage | Automated Recon VPS
- BugBounty: Setting up OOB Bind9 For SSRF
- Bash tricks 07: Standard In

Podcasts

- Security Now – IoT Isolation Strategies – Isolate Your IoT Devices, Threema Goes Open-Source
- Risky Business #598 — China closing the "cyber gap" with USA
- Hacking Into Security #23 – Finding vulnerabilities as a teenager, first job at 17, bug bounties and more, with Shubs – @infosec_au, @notnaffy
- The InfoSec & OSINT Show 24 – Ira Winkler & How to Stop Stupid
- SWN #63 – Argentina Ransomware, WhatsApp Bugs, & Cisco Jabber RCE
- Humans of InfoSec – Emerging Voices: Busra Demir

Webinars & Webcasts

- Discord Hangout: Physical Live Stream
- r2c meetup on writing Semgrep rules
- Webcast: When Worlds Collide: OSS Hunting & Adversarial Simulation #ThreatHunting

Conferences

- NoNameCon 2020, Kyiv
- r2con2020 & Slides

Tutorials

Medium to advanced

- N1QL Injection: Kind of SQL Injection in a NoSQL Database & N1QLMap
- Cross-site Scripting in React Web Applications
- How to Get Large Amounts of S3 Files with Boto3
- IDA Pro Tips to Add to Your Bag of Tricks
- Supply in the Request Shenanigans #AD
- Bypass AMSI by manual modification part II – Invoke-Mimikatz
- Getting Windows Passwords in ClearText

Beginners corner

- Axiom: It Kinda Feels Like Cheating
- Not all attacks are equal: understanding and preventing DoS in web applications

- This Image Is Also a Valid Javascript File
- How to Scan Continuously with Nuclei?
- Dive into Email Security: MTA-STS Policies
- Facial Recognition for Verification (Missing Persons)

Writeups

Challenge writeups

- XSS Challenge Solution – SVG use
- XSS a Paste Service – Pasteurize (web) Google CTF 2020 (video)
- Defeating Google Closure Library Sanitizer

Responsible(ish) disclosure writeups

- F5 BIG-IP Remote Code Execution Exploit – CVE-2020-5902 #Web
- Escalating to Domain Admin in Microsoft's Cloud Hosted Active Directory (Azure AD Domain Services) #AD
- WSUS Attacks Part 1: Introducing PyWSUS & WSUS Attacks Part 2: CVE-2020-1013 a Windows 10 Local Privilege Escalation 1-Day #WSUS #Windows #PrivEsc
- Wekan Authentication Bypass – Exploiting Common Pitfalls Of Meteorjs #Web
- Ubuntu PPP's CVE-2020-15704 Wrap-up #Linux #PrivEsc
- Keycloak DoS – CVE-2020-10758 #Web
- Microsoft Exchange Server DlpUtils AddTenantDlpPolicy Remote Code Execution Vulnerability (CVE-2020-16875) #Exchange #RCE

Bug bounty writeups

- XSS->Fix->Bypass: 10000$ bounty in Google Maps (Google, $10,000)
- Safe Redirect Bypass (Twitter, $560)
- XSS that can pay your Bills (€500)
- Account Takeover via IDOR ($25,000)
- Instagram Web DM bug and Followers bug PoC (video) (Facebook)
- Blind HTTP GET SSRF via website icon fetch (bypass of pull#812) (Bitwarden)
- Stored XSS in markdown when redacting references (GitLab, $5,000)
- Injection of `http.<url>.*` git config settings leading to SSRF (GitLab, $3,000)

See more writeups on The list of bug bounty writeups.

Tools

If you don't have time

- Twistr & Intro: A domain name permutation and enumeration library powered by Rust
- Gooey: Turn (almost) any Python command line program into a full GUI application with one line
- StreamDivert & Intro: Redirecting (specific) TCP, UDP and ICMP traffic to another destination.

More tools, if you have time

- bufferover: Extracting DNS data from bufferover API for penetration testers
- FES: Fast Endpoint Scanner in Rust, based on TomNomNom's meg
- check-put.sh: Script to test for PUT upload method against a list of hosts
- Recon-007 [V1 Beta]: Python tool to automate the bug bounty recon process
- uniqurl: Use uniqurl to filter only unique content from a list of URLs with stdin, making it usable within piped commands
- get-title: multi threaded python tool to get pages's title
- rakkess: Review Access – kubectl plugin to show an access matrix for k8s server resources
- Maigret: Collect a dossier on a person by username from a huge number of sites (Fork of Sherlock)
- Wacker: A WPA3 dictionary cracker
- Bluescan: A powerful Bluetooth scanner for scanning BR/LE devices, LMP, SDP, GATT and vulnerabilities!
- DVS: D(COM) V(ulnerability) S(canner) AKA Devious swiss army knife – Lateral movement using DCOM Objects
- TREVORspray: A featureful Python O365 sprayer based on MSOLSpray which uses the Microsoft Graph API & bypasses microsoft's new anti-password-spraying countermeasures

Misc. pentest & bug bounty resources

- Pentesting/Bug Bounty Mindmap
- BBhacKing/jwt_secrets
- iOS app hacking mindmap
- android-security-awesome
- PHP7 Internals – Become a Wizard

- Windows-Privilege-Escalation-Resources
- 6 Tools You Need To Be Aware Of If You Are Into Device Pentesting | Payatu

Challenges

- brutal.x55.is

Articles

- Spring View Manipulation Vulnerability
- SQL Injection filter bypass to perform blind SQL Injection
- Fuzzing The Front End!
- STALK: Security Analysis of Smartwatches for Kids
- Abusing dynamic groups in Azure AD for privilege escalation
- Protecting Your Malware with blockdlls and ACG

News

Bug bounty & Pentest news

- Response to Voatz's Supreme Court Amicus Brief
- Shodan Search Engine Improvements

Reports

- Understanding the money laundering techniques that support large-scale cyber-heists
- Most cyber-security reports only focus on the cool threats
- State of Cybersecurity Industry Exposure at Dark Web
- BitDefender Mid-Year Threat Landscape Report 2020

Vulnerabilities

- Zerologon attack lets hackers take over enterprise networks: Patch now
- Microsoft addresses critical SharePoint and DNS-related flaws in Patch Tuesday update
- HTTP request smuggling: HTTP/2 opens a new attack tunnel
- Windows 10 themes can be abused to steal Windows passwords
- Difficult-to-execute attack could break TLS encryption in rare circumstances

- New BlindSide attack uses speculative execution to bypass ASLR
- BLURtooth vulnerability lets attackers overwrite Bluetooth authentication keys
- Academics find crypto bugs in 306 popular Android apps, none get patched
- Positive Technologies: vulnerabilities in PAN-OS could threaten internal networks security

Breaches & Attacks

- New cyberattacks targeting U.S. elections
- ZShlayer: New macOS malware variant obfuscates scripts to slip past security tools
- Ransomware And Zoom-Bombing: Cyberattacks Disrupt Back-to-School Plans
- Baka credit card skimmer bundles stealth, anti-detection capabilities, warns Visa
- Attackers Abusing Legitimate Cloud Monitoring Tools to Conduct Cyber Attacks
- DDoS attacks against SwissSign prompt temporary CA switch for ProtonMail
- New CDRThief malware targets VoIP softswitches to steal call detail records
- Malware gang uses .NET library to generate Excel docs that bypass security checks

Other news

- Gartner Predicts 75% of CEOs Will be Personally Liable for Cyber-Physical Security Incidents by 2024
- Consumer advice: Giggle vulnerability
- Evading Censorship from the Server-side
- With a Simple Piece of Paper, Engineers Create Self-Powered, Wireless Keyboard
- Now that's a somewhat unexpected insider threat: Zoombombings mostly blamed on rogue participants, unique solution offered
- Windows 10 now lets you mount Linux ext4 filesystems in WSL 2

Non technical

- 'It was a complete fluke' – Katie Paxton-Fear on her bug bounty baptism and why AI will never fully replace security researchers
- Hacker Spotlight: Interview With dki
- Researcher Spotlight: HX01
- Security by Obscurity is Underrated
- OSINT IRL Stories

- Is Anxiety Freedom Without Direction?
- The top 10 best hacker-themed books of all time
- An overview of targeted attacks and APTs on Linux
- Bug bounty memes

Tweeted this week

We created a collection of our favorite pentest & bug bounty related tweets shared this past week. You're welcome to read them directly on Twitter: Tweets from 09/04/2020 to 09/11/2020.