從 Binary Researcher 到 Bounty Hunter 的致富之路

The Road to Riches: From Binary Researcher to Bounty Hunter

Lays

HITCON PEACE 2022

Lays

We're Hiring!!

- Co-Founder / Research Team Leader of **TrapaSecurity**
  - Vulnerability Research, Windows / Mobile / IoT …
- Focus On
  - Reverse Engineering for 10+ years
  - MSRC Most Valuable Security Researcher 2019 & 2020
  - Acknowledged by Microsoft / Samsung / Google / Trend Micro / NETGEAR / WD / Synology …
- Retired CTF Player
  - **HITCON** / **217** CTF Team
    - DEF CON CTF 25 & 27 2nd
    - WCTF 2017 & 2019 1st
    - Trend Micro CTF 2018 1st
    - …
  - Co-Founder of **Pwnable.tw**

Outline

- 成為 Bounty Hunter 的契機
- 各大 “Binary” Bounty Program 介紹
- 獎金 / 漏洞類型 / 手法
- 回報小技巧

Bug Bounty Program 是什麼?

還輪得到我講?

大家對 Bug Bounty 的印象

- 天才駭客!
  - 再發現 FB 漏洞獲頒 30 萬獎金 張O元 100 萬成就達標！
  - 18 歲大學生找出 Google App Engine 重大 RCE 漏洞，抱走 3.6 萬美元獎金
  - 烏拉圭高中生意外發現Google漏洞，賺到 1 萬美元抓漏獎金
  - Facebook 支付 1 萬美元資安獎金給年僅 10 歲的 IG 小駭客
- 羨慕

Bug Bounty 爭議事件

- 內政部 Bug Bounty
- New eID 數位身分證
- 成大教授: 「資安弱智」
  - 內政部邀駭客揪漏洞 學者批：資安弱智

李忠憲

資安弱智的賞金獵人

是什麼白癡，才會相信真正的駭客會來領你政府微薄的賞金！即使退一萬步[OBJ]，先不論我們最要擔心的駭客 - 中國政府，真正厲害的駭客，會自己跳出來，跟政府說：「我就是駭客」？只為了你那區區賞金？還可能會被政府監管。

我也建議政府辦個「門鎖安全測試」，政府找人設計一個最厲害的鎖，然後公開懸賞解鎖。三個月內沒有人可以拿賞金，那就表示這個鎖安全可靠、天下無敵，政府就可以規定家家戶戶都必須用這個鎖，這樣台灣盜賊就會通通絕跡。

當兵時，有一天隊上有個鎖的鑰匙遍尋不著，一時找不到鎖匠。我就天真的問，有沒有小兵可以幫忙開鎖？當然沒半個人站出來，之後我的資深班長私下跟我說：不會有人站出來啦！他站出來，不就等於告訴大家，他入伍前是做什麼的？

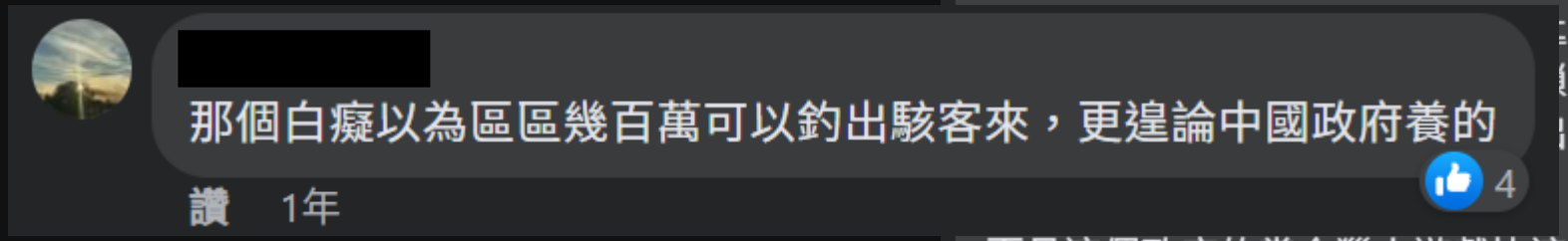
而且這個政府的賞金獵人遊戲比這樣還誇張，他只測試那一支鑰匙，連配對的鑰匙孔座都沒有，這副門鎖的設計，還沒有規定用什麼讀卡機，而讀卡機大部分都是中國設計生產製造[OBJ]的。[OBJ]

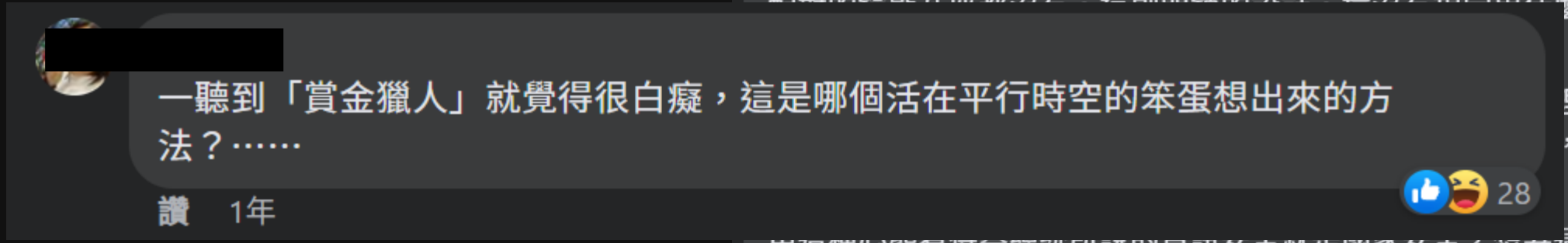
我在國家高速網路與計算中心擔任資訊安全長，負責設計管理經營的網路安全測試平台，我們同仁所設計的雲端駭客攻擊戰爭比賽，還比這個賞金獵人的遊戲實際許多。

用這種心態看待蔡總統所說的資訊安全就是國家安全，想要這樣來說服全體國民，不是資安弱智不然是什麼？

Bug Bounty 爭議事件

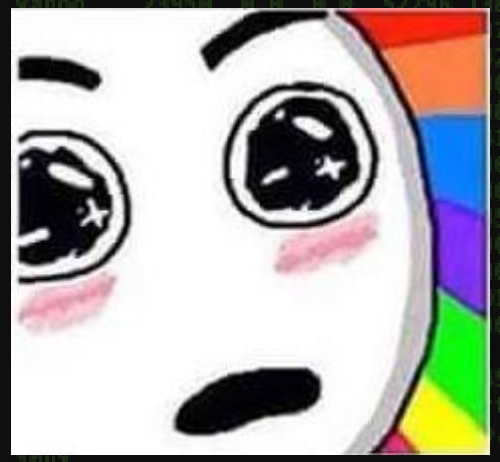
- 內政部 Bug Bounty
- New eID 數位身分證
- 成大教授: 「資安弱智」
  - 內政部邀駭客揪漏洞 學者批：資安弱智





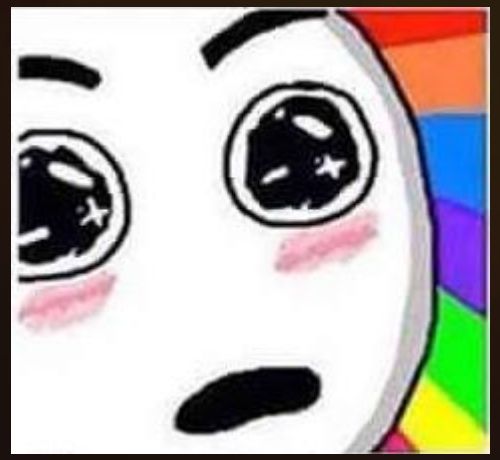
我對 Bug Bounty 最早的印象

- 2013
  - Orange Tsai
    - Yahoo Bug Bounty Part 1 - 台灣 Yahoo Blog 任意檔案下載漏洞
    - Yahoo Bug Bounty Part 2 - *.login.yahoo.com Remote Code Execution 遠端代碼執行漏洞
  - 羨慕
  - 我長大以後也要當 Orange!



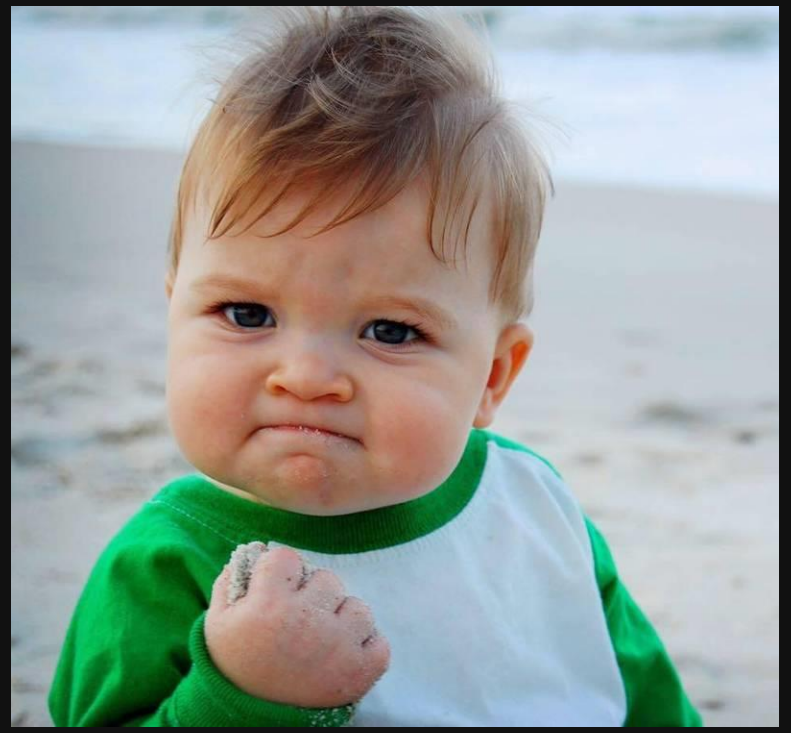
我對 Bug Bounty 最早的印象

- 2013 ~ 2016 年左右
  - 各大企業開始推出針對自家網站的 Bug Bounty Program
- HITCON 2016
  - Bug Bounty 獎金獵人甘苦談 那些年我回報過的漏洞 by Orange Tsai
    - Google, Facebook, Apple, Yahoo, Uber, eBay…
    - 連搭個 Uber 都能賺 $4000 的男人
  - 我長大以後也要當 Orange!



我也要賺錢!

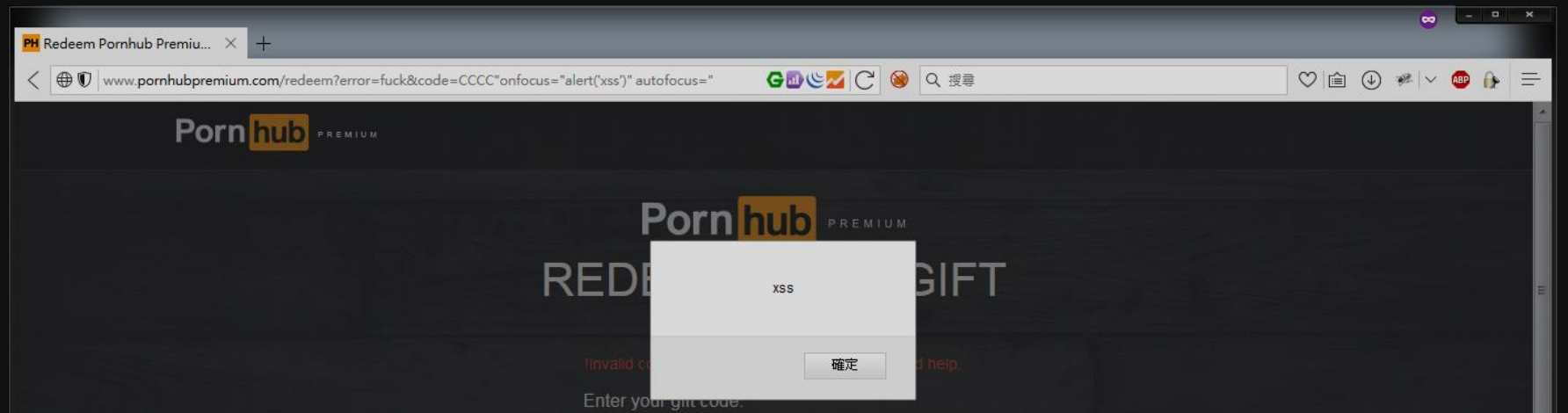
- 馬上打開 HackerOne / Bugcrowd
  - 發現目標幾乎都是網站
- 花了一個晚上在我常用的網站上找洞...



我也要賺錢!

- 馬上打開 HackerOne / Bugcrowd
  - 發現目標幾乎都是網站
- 花了一個晚上在我常用的網站上找洞...

Pornhub XSS!

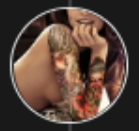


我也要賺錢!

- 馬上打開 HackerOne / Bugcrowd
  - 發現目標幾乎都是網站
- 花了一個晚上在我常用的網站上找洞...

Pornhub XSS!

Duplicated



cyrus closed the report and changed the status to ● Duplicate. Aug 15th (6 years ago)

Hi,

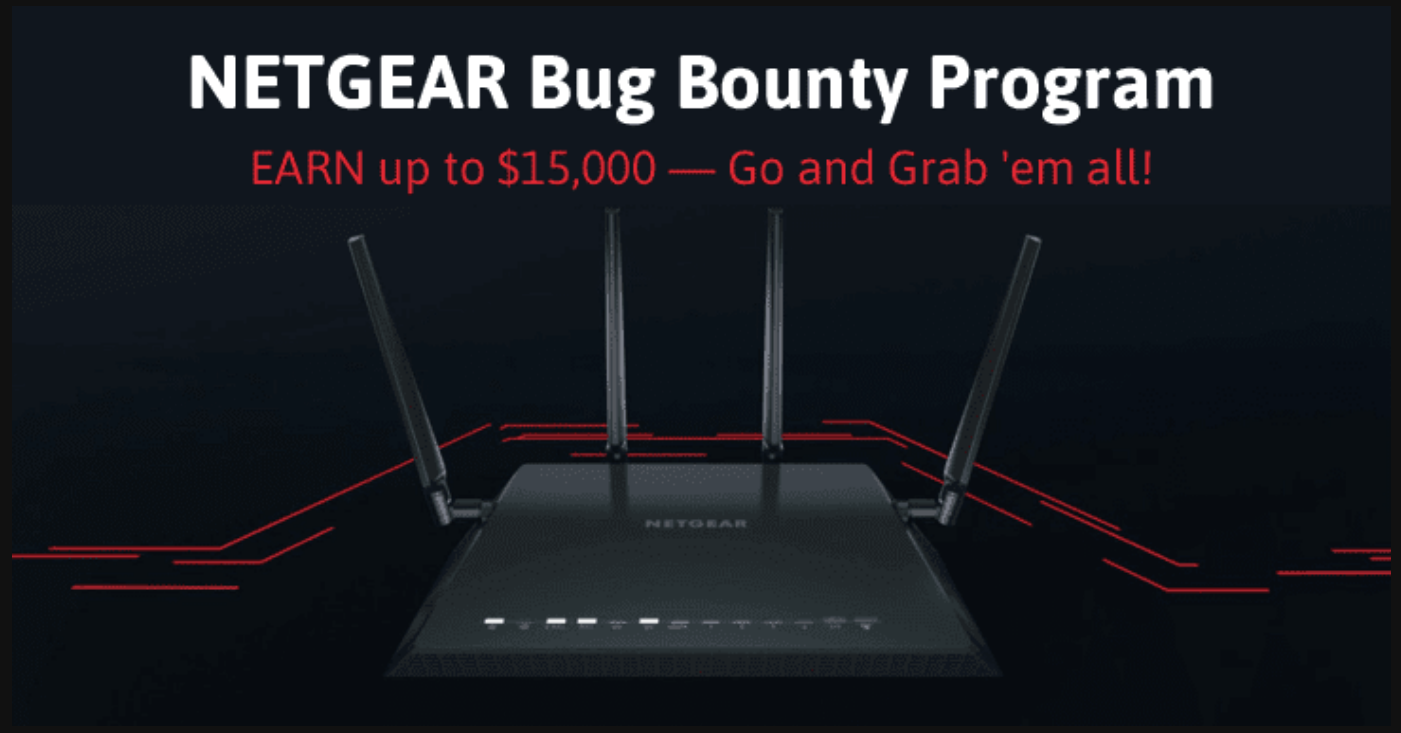
This issue has already been reported by another researcher, therefore I will need to close this case. Thank you.

這種事很講究天份的

- 不擅長 Web Hacking…
- RCE, XSS, LFI, CSRF, SQL Injection 通通都有 Bounty…
- 為什麼就沒有屬於 Binary 的 Bounty 呢！

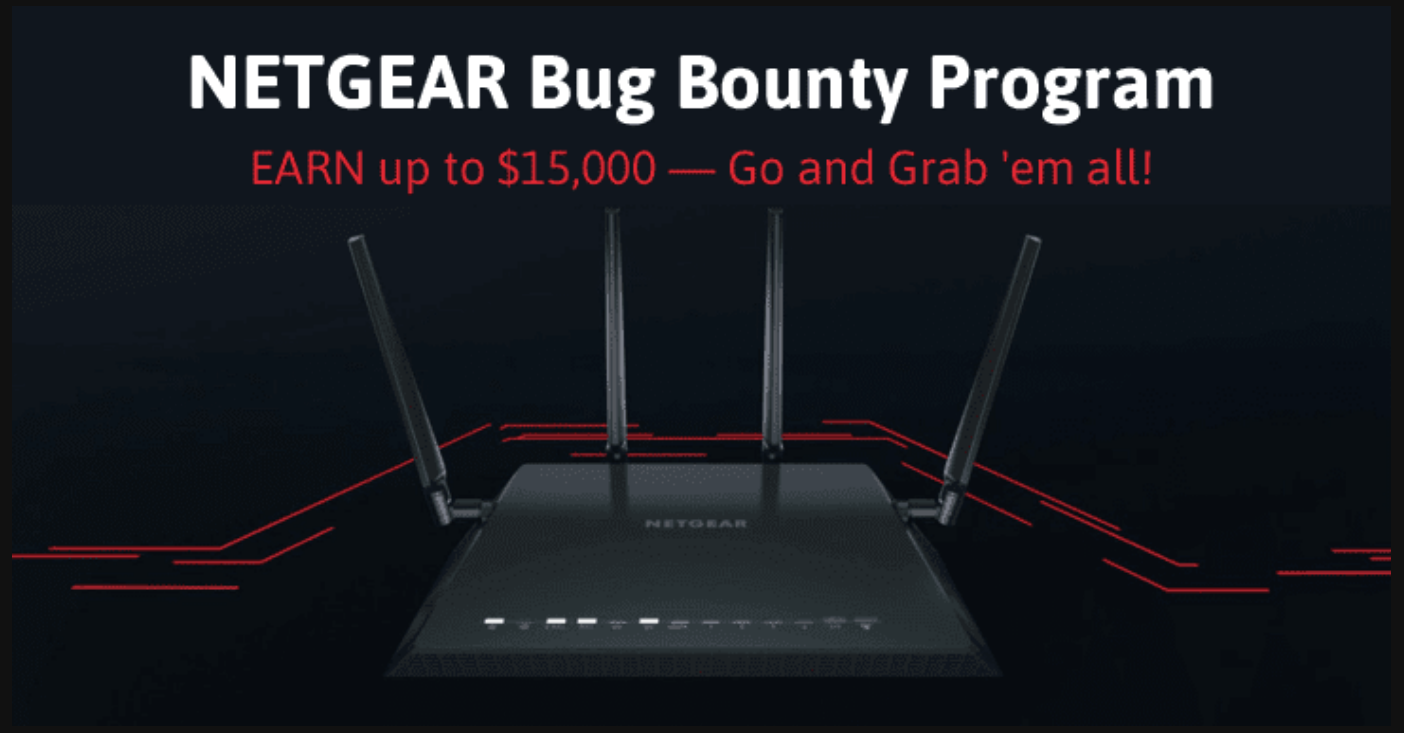
這種事很講究天份的

- 不擅長 Web Hacking…
- RCE, XSS, LFI, CSRF, SQL Injection 通通都有 Bounty…
- 為什麼就沒有屬於 Binary 的 Bounty 呢！
- Orange: 「喔，有啊」



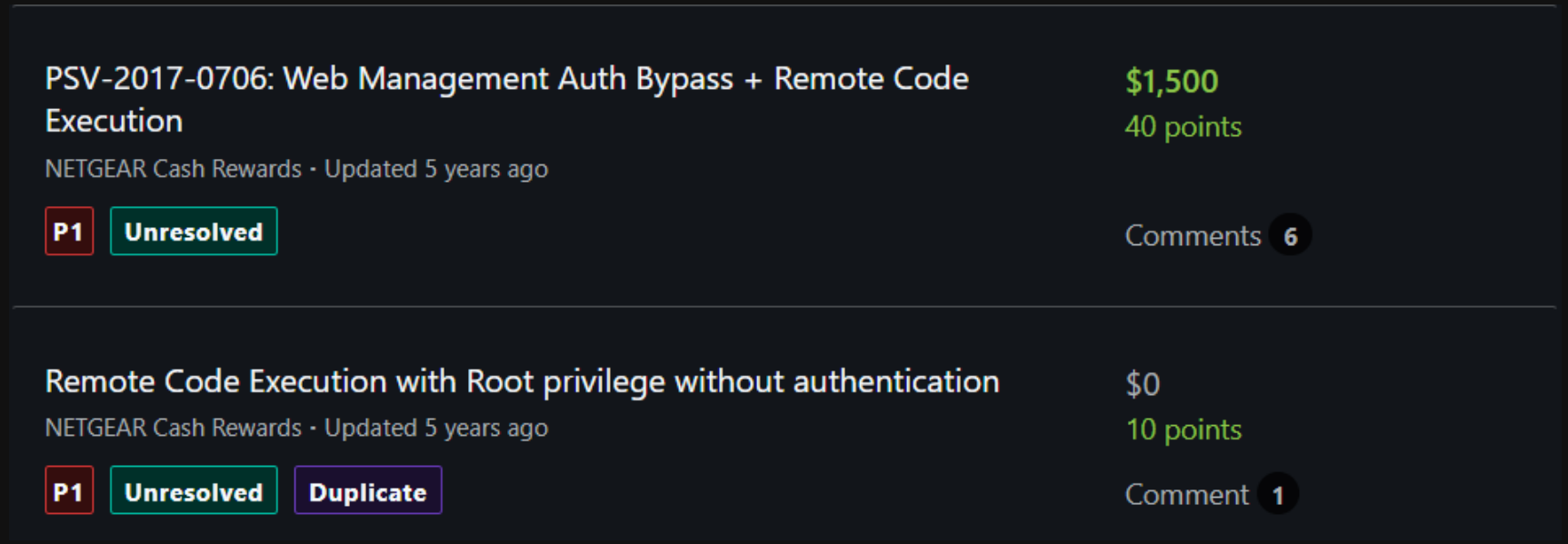
這種事很講究天份的

- 不擅長 Web Hacking...
- RCE, XSS, LFI, CSRF, SQL Injection 通通都有 Bounty...
- 為什麼就沒有屬於 Binary 的 Bounty 呢！
- Orange: 「喔，有啊」



我的第一個 (Binary) Bounty！

- 再度 Duplicated 之後…
- NETGEAR R8500 Pre-Auth RCE
  - $1500 Bounty



我的第一個 (Binary) Bounty！

- 做好事又有錢拿！
  - 好爽
  - 原來做逆向工程也能拿獎金
  - 從此走上不歸路
    - ~~長大也不一定要當 Orange 嘛~~

Binary 與 Web 類型的 Bounty Program 差異

- 門檻較高
  - C++ vs PHP / Assembly vs JavaScript / IDA Pro vs Burp Suite...
- 獎金上限較高
  - 有時候軟體 / 設備的漏洞比網站影響更廣
  - 你的網站還不是跑在 Binary 上
- 規則
  - 大部分 Binary Bounty 不需要 提供完整 Exploit，甚至不需要 Exploitable
- 修補方式差異
  - Web: 通常會緊急修補
    - 請回報者複測後發獎金
  - Binary: 通常在修補前 先發獎金，再花個 3 ~ 5 個月修正，釋出新版
    - 然後再被打一次

有哪些 Binary Bounty Program

Web 麻瓜救星


慈善機構系列
「善良的」漏洞收購計畫
我們不偷不搶

Trend Micro ZDI（Zero Day Initiative）

- 原本是 HP 旗下子公司
  - 2015 被 Trend Micro 收購
- 收購未知漏洞 / 研究成果
  - 整合進相關防禦產品 (TippingPoint IPS)
  - 各大軟體的漏洞都收
- Pwn2Own 主辦方

Trend Micro ZDI（ Zero Day Initiative ）

👍 **Pros**

- 不要求 完整 Exploit
  - PoC 「有機會」 RCE / LPE 就收
  - OOB / Overflow / UaF even Crash is enough!
- 金額不滿意可以拒絕
  - 如果是回報給 Vendor 就是見光死
- 研究員不需要跟 Vendor 溝通細節
  - 會幫忙回報並保留回報者 Credit
  - 會與研究員合作發表研究內容 /公開漏洞細節
- 積分制度
  - 報越多賺越多

ZERO DAY INITIATIVE

https://www.zerodayinitiative.com/

Trend Micro ZDI（Zero Day Initiative）

Category	Targets	Maximum Bounty (USD)
Content Management Systems	Joomla	$25,000
	Drupal	$25,000
	WordPress	$35,000
Application Containers	Docker	$50,000
	Kubernetes	$50,000
Microsoft Enterprise Applications	Microsoft Outlook	$200,000
	Microsoft Exchange	$250,000
Web servers	NGINX	$200,000
	Apache	$200,000
	Microsoft IIS	$200,000
Protocols and Standards	ISC BIND	$200,000
	Microsoft Windows RDP	$200,000
	Microsoft Windows SMB	$200,000
	OpenSSH	$250,000

👎 Cons

- 獎金較低，約為數百到數千美金
  - Targeted Incentive Program 獎金較高
    - $25,000 ~ $200,000
  - 部分 Trend Micro 產品也有 Bonus
- 每天都有大量漏洞等待審核
  - 排隊大概要 4 ~ 8 周
  - 自疫情開始以來越來越慢

ZERO DAY INITIATIVE

https://www.zerodayinitiative.com/

SSD Secure Disclosure

- 收購 Exploit，並做為溝通橋樑
  - 為客戶提供風險情報 / 漏洞防禦方案
  - 提供 Vendor 漏洞細節
  - 提供研究員獎金
- TyphoonPwn 主辦方

https://ssd-disclosure.com/

SSD Secure Disclosure

👍 **Pros**

- 獎金相對於 ZDI 較高
- 研究員不需要跟 Vendor 溝通細節
  - 會幫忙回報並保留回報者 Credit
  - 會與研究員合作發表研究內容 / 公開漏洞細節
- 處理速度較快
- 推薦獎金

https://ssd-disclosure.com/

SSD Secure Disclosure

Targets of interest:

- **Operating systems:** Windows (RCE and PE)
- **Mobile:** iOS (PE from within the Sandbox) / Android / Baseband
- **Web Browsers:** Chrome (RCE or SBX) / Safari / Firefox (RCE)

- **Routers and Routers OS**
  - Fritz!Box
  - Ubiquiti AirCube
  - Netgear, TP-Link, D-Link
  - OpenWRT
  - DD-WRT
- **Web Panels & Mail Servers**
  - cPanel
  - Plesk
  - WHMCS
  - Open-Xchange
  - Zimbra
  - VestaCP
  - aaPanel
  - Microsoft Exchange
  - Froxlor
  - EasyEngine
- **Content Management Systems**
  - WordPress
  - Confluence
  - SharePoint
- **Network Monitoring / Firewalls / Virtualization**
  - SolarWinds Orion
  - Virtualizor
  - SolusVM
  - Zabbix
  - F5 Big-IP
  - Cisco ASA
  - Zyxel Network VPN Firewall
- **Other**
  - Asterisk (VOIP)
  - Anydesk
  - Microsoft Office
  - Wire Mobile and desktop app

👎 Cons

- 要求完整 Exploit
- 針對目標範圍較小
  - 也較常變動
  - ~~而且有 Web~~

https://ssd-disclosure.com/

有錢老爸系列

沒有用錢買不到的 Bug，如果有，那就是錢不夠

Microsoft Bounty Program

👍 Pros

- 產品多，Scope 廣
- 金額非常有誠意 ~$250,000 *Paid!*
- 不需完整 Exploit 也能拿到完整金額
  - 報告正常寫都會拿到表定最高金額
  - 少數項目有 Exploit 會有 Bonus
- 撞洞依然會有 CVE / Credit *Exclusive!*
  - 若與微軟內部撞洞，仍有機會拿到獎金
- 各種福利
  - Hall of Fame (MVSR / Top 100)
    - 免錢序號用到爽
  - 三不五時寄些小禮物
  - 在 Las Vegas 開趴會揪你

Microsoft

https://www.microsoft.com/en-us/msrc/bounty

Microsoft Bounty Program

👎 Cons

- 不同部門風格差異較大
  - 有些小氣，有些大方
- 有點像公務員，不太討論細節
  - 感覺有時候也沒什麼在看報告
  - ~~畢竟人家有 Source Code 嘛~~
- Scope 很謎，有些重要的產品反而沒錢
  - 今年才有 Exchange Server Bounty: RCE $20,000
  - 各部門需各自提出 Bounty Program 所致
- 前兩年被刷怕了，常改規則或降低金額

Microsoft

https://www.microsoft.com/en-us/msrc/bounty

Microsoft Bounty Program (Binary)

• Microsoft Hyper-V	~$250,000
• Mitigation Bypass and Bounty for Defense	~$200,000
• Microsoft Windows Insider Preview	~$100,000
• Microsoft Applications and On-Premises Servers	~$30,000
• Windows Defender Application Guard	~$30,000
• Microsoft Edge (Chromium-based)	~$30,000
• Office Insider	~$15,000
• ElectionGuard	~$15,000

Microsoft

Microsoft Bounty Program (Binary)

Highly Recommend!

• Microsoft Hyper-V	~$250,000
• Mitigation Bypass and Bounty for Defense	~$200,000
• Microsoft Windows Insider Preview	~$100,000
• Microsoft Applications and On-Premises Servers	~$30,000
• Windows Defender Application Guard	~$30,000
• Microsoft Edge (Chromium-based)	~$30,000
• Office Insider	~$15,000
• ElectionGuard	~$15,000

Microsoft

Hyper-V Bounty Program

- VM Escape 最高獎金 $250,000
  - Exploit: $250,000
  - PoC Only: $200,000
  - Info Disclosure: $25,000
  - DOS: $15,000
- 2017 年的我:
  這東西怎麼可能還有洞，錢哪有那麼好賺

- Black Hat USA 2021 - hAFL1: Our Journey of Fuzzing Hyper-V and Discovering a 0-Day
  - CVE-2021-28476: Arbitrary Pointer Dereference in Virtual Network Switch, $200,000 Bounty
- Bi/ug Bounties and HyperV RCE Research (2022)
  - Multiple Bugs, $100,000 Bounty

Microsoft

Hyper-V Bounty Program

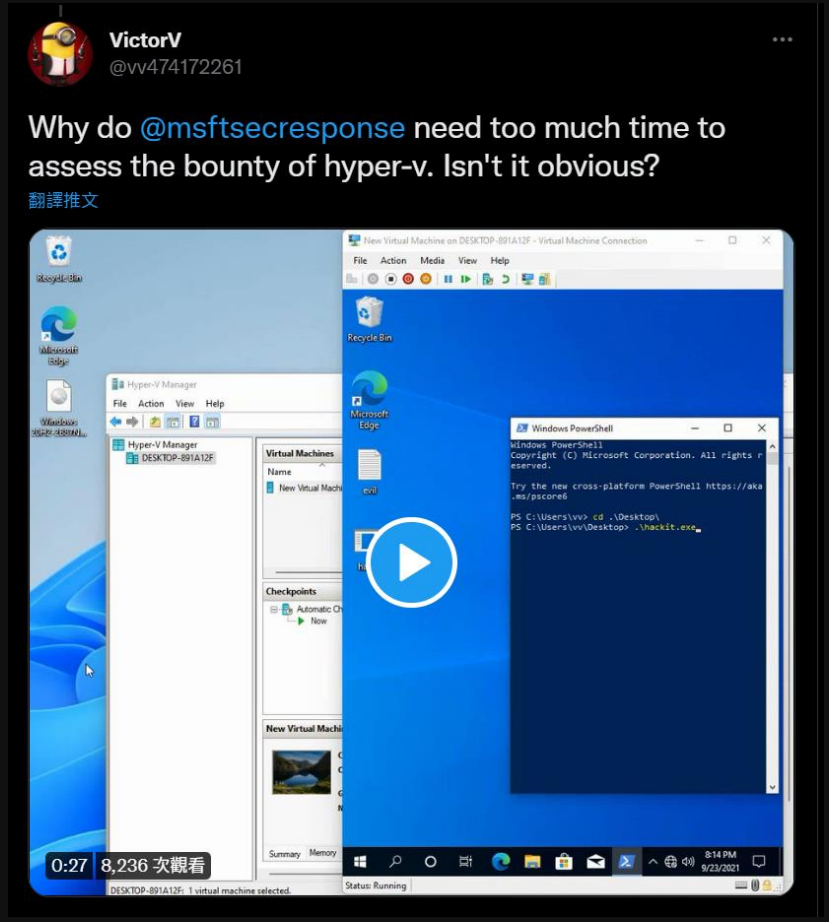
Aug 9, 2022	PETER HLAVATY with Fruit your Game	Windows Hyper-V Remote Code Execution Vulnerability	CVE-2022-34696
Jun 14, 2022	Microsoft WSD CoreNet team	Windows Hyper-V Remote Code Execution Vulnerability	CVE-2022-30163
Apr 12, 2022	Microsoft Offensive Research & Security Engineering (MORSE)	Windows Hyper-V Remote Code Execution Vulnerability	CVE-2022-24537
Apr 12, 2022	rezer0dai with Capo di Frutti	Windows Hyper-V Remote Code Execution Vulnerability	CVE-2022-23257
Apr 12, 2022	rezer0dai with NoBananas NoBugzz	Windows Hyper-V Remote Code Execution Vulnerability	CVE-2022-22009
Apr 12, 2022	rezer0dai with Independent Slavic Voyage	Windows Hyper-V Remote Code Execution Vulnerability	CVE-2022-22008
Feb 8, 2022	rezer0dai with EatingFigs ENooPig	Windows Hyper-V Remote Code Execution Vulnerability	CVE-2022-21995
Oct 12, 2021	Wei in Kunlun Lab	Windows Hyper-V Remote Code Execution Vulnerability	CVE-2021-38672
Jul 13, 2021	Microsoft Platform Security Assurance & Vulnerability Research	Windows Hyper-V Remote Code Execution Vulnerability	CVE-2021-34450
Mar 9, 2021	@rezer0dai	Windows Hyper-V Remote Code Execution Vulnerability	CVE-2021-26867
Oct 13, 2020	HongZhenhao of IceSword Lab	Windows Hyper-V Remote Code Execution Vulnerability	CVE-2020-16891
Apr 14, 2020	Microsoft Virtualization Security Team	Windows Hyper-V Remote Code Execution Vulnerability	CVE-2020-0910
Dec 10, 2019	Microsoft Platform Security Assurance & Vulnerability Research	Windows Hyper-V Remote Code Execution Vulnerability	CVE-2019-1471
Nov 12, 2019	Daniel King (@long123king), MSRC Microsoft	Windows Hyper-V Remote Code Execution Vulnerability	CVE-2019-1398
Nov 12, 2019	Joe Bialek, MSRC Vulnerabilities and Mitigations Team	Windows Hyper-V Remote Code Execution Vulnerability	CVE-2019-1389
Aug 13, 2019	Hyper-V Development Team	Windows Hyper-V Remote Code Execution Vulnerability	CVE-2019-0965

Loaded all 25 rows

Microsoft

Hyper-V Bounty Program

- 爭議
  - 預設環境，完整 Exploit 卻只拿到 $5,000



Hyper-V Bounty Program

- 爭議
  - 微軟: RDP != Hyper-V
  - 更在意影響 Azure 的漏洞

The Hyper-V bounty is focused on:

- Components and features of Hyper-V that are used in server hosting scenarios (both traditional virtual machines and Hyper-V Isolation Containers).
- The assumption that the Virtual Machine is on a separate VLAN than the host so there is no possibility to attack network services that are running on the host.
- The assumption that the host will not be interacting with the Virtual Machine in a manner that is atypical when hosting servers. For example, the host will not use enhanced session mode to interact with the virtual machine.

OUT OF SCOPE SUBMISSIONS AND VULNERABILITIES

Microsoft is happy to receive and review each vulnerability report on a case-by-case basis, but some vulnerability types may not qualify for bounty reward. Here are some of the common low-severity or out of scope issues that typically do not earn bounty rewards:

- Publicly-disclosed vulnerabilities which are already known to Microsoft and the wider security community.
- Hardware and firmware issues.
- Vulnerabilities that can only be triggered by an attacker running code on the host.
- Vulnerabilities that require the Hyper-V VM to send network traffic to host listeners. For example, this includes, without limitation attacks against the hosts TCP, SMB or RPC stack. Attacks against the virtualized network stack (for example, this includes, without limitation VMSwitch) are in scope.
  - Vulnerabilities in host network services may be evaluated under the Windows Insider Preview bounty program.
- Vulnerabilities based on third-party code. For example, this includes, without limitation Docker and Kubernetes.
- Vulnerabilities in deprecated features; for example, this includes, without limitation, RemoteFX.
- Vulnerabilities in Legacy Network Adapter (Generation 1) and Fibre Channel Adapter
- Vulnerabilities that can only be triggered when the guest is connected to via the RDP protocol. For example, this includes, without limitation RDP or Enhanced Session Mode.
  - Vulnerabilities in RDP may be evaluated under the Windows Insider Preview bounty program.
- Vulnerabilities in deprecated features. For example, this includes, without limitation, RemoteFX.
- Vulnerabilities that cannot be triggered when Hyper-V is used to host traditional virtual machines (Generation 1 or 2) or Hyper-V isolation containers.
  - Vulnerabilities that require Windows Defender Applications Guard (WDAG) may be evaluated under the WDAG bounty program.
  - Vulnerabilities that require Windows Sandbox may be evaluated under the Windows Insider Preview bounty program.
- Vulnerabilities that require the following configuration changes to be made by a Hyper-V administrator:
  - Enabling an undocumented feature or undocumented configuration. For example, this includes, without limitation enabling an experimental feature or using an undocumented configuration that intentionally puts the system in an insecure state.
  - Enabling a feature/configuration that is only intended for out-of-scope scenarios. This includes, without limitation enabling a feature only intended for use with WDAG on a traditional VM.

Microsoft Windows Insider Preview Bounty Program

- 要求在 Windows Insider Preview 能觸發
- 2019 ~ 2020 淘金熱潮
  - RCE $30,000 Image / LNK Parsing…
  - EOP $20,000 Kernel LPE / Service EOP / Junction & Mount Point EOP …
  - Kernel Leak $10,000 (PoC Only)
- 應該是微軟發最多錢的 Program

Feb 11, 2020	Shefang Zhong of Qihoo 360 Vulcan Team	Windows Search Indexer Elevation of Privilege Vulnerability	CVE-2020-0666
Jan 14, 2020	Shefang Zhong of Qihoo 360 Vulcan Team	Windows Search Indexer Elevation of Privilege Vulnerability	CVE-2020-0633
Jan 14, 2020	Shefang Zhong of Qihoo 360 Vulcan Team	Windows Search Indexer Elevation of Privilege Vulnerability	CVE-2020-0632
Jan 14, 2020	Shefang Zhong of Qihoo 360 Vulcan Team	Windows Search Indexer Elevation of Privilege Vulnerability	CVE-2020-0631
Jan 14, 2020	Shefang Zhong of Qihoo 360 Vulcan Team	Windows Search Indexer Elevation of Privilege Vulnerability	CVE-2020-0630
Jan 14, 2020	Shefang Zhong of Qihoo 360 Vulcan Team	Windows Search Indexer Elevation of Privilege Vulnerability	CVE-2020-0629
Jan 14, 2020	Shefang Zhong of Qihoo 360 Vulcan Team	Windows Search Indexer Elevation of Privilege Vulnerability	CVE-2020-0628
Jan 14, 2020	Shefang Zhong of Qihoo 360 Vulcan Team	Windows Search Indexer Elevation of Privilege Vulnerability	CVE-2020-0627
Jan 14, 2020	Shefang Zhong of Qihoo 360 Vulcan Team	Windows Search Indexer Elevation of Privilege Vulnerability	CVE-2020-0626
Jan 14, 2020	Shefang Zhong of Qihoo 360 Vulcan Team	Windows Search Indexer Elevation of Privilege Vulnerability	CVE-2020-0625
Jan 14, 2020	zhong_sf of Qihoo 360 Vulcan Team	Windows Search Indexer Elevation of Privilege Vulnerability	CVE-2020-0613
Jan 14, 2020	zhong_sf of Qihoo 360 Vulcan Team	Windows Search Indexer Elevation of Privilege Vulnerability	CVE-2020-0614

Microsoft Windows Insider Preview Bounty Program

- 2020/07 改制之後
  - RCE $30,000 -> $5,000
  - EOP $20,000 -> $2,000
  - 白帽駭客直接在網路公開微軟Windows 11高危險漏洞，只因懸賞獎金打骨折
  - Parser Crash 有個 $5000 還是不錯的

- 難度大提升
  - Pre auth RCE with no user interaction: $100,000
  - 馬上被刷一排
  - 好想當 Yuki Chen

Microsoft

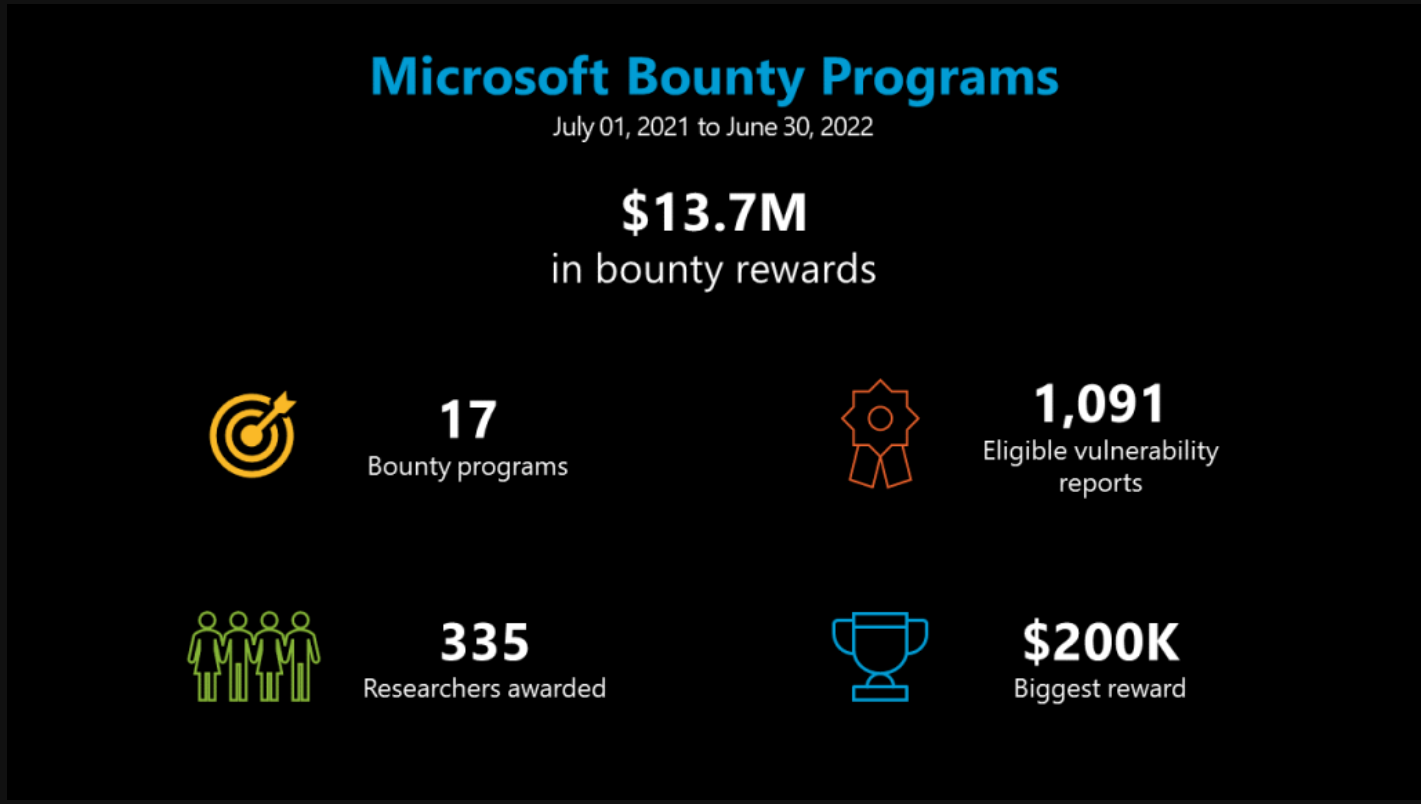
Microsoft Windows Insider Preview Bounty Program

Aug 9, 2022	Yuki Chen with Cyber KunLun	Windows Secure Socket Tunneling Protocol (SSTP) Remote Code Execution Vulnerability	CVE-2022-35766
Aug 9, 2022	Yuki Chen with Cyber KunLun	Windows Secure Socket Tunneling Protocol (SSTP) Remote Code Execution Vulnerability	CVE-2022-35753
Aug 9, 2022	Yuki Chen with Cyber KunLun	Windows Secure Socket Tunneling Protocol (SSTP) Remote Code Execution Vulnerability	CVE-2022-35752
Aug 9, 2022	Yuki Chen with Cyber KunLun	Windows Point-to-Point Protocol (PPP) Denial of Service Vulnerability	CVE-2022-35747
Aug 9, 2022	Yuki Chen with Cyber KunLun	Windows Secure Socket Tunneling Protocol (SSTP) Remote Code Execution Vulnerability	CVE-2022-35745
Aug 9, 2022	Yuki Chen with Cyber KunLun	Windows Point-to-Point Protocol (PPP) Remote Code Execution Vulnerability	CVE-2022-35744
Aug 9, 2022	Yuki Chen with Cyber KunLun	Windows Secure Socket Tunneling Protocol (SSTP) Remote Code Execution Vulnerability	CVE-2022-34714
Aug 9, 2022	Yuki Chen with Cyber KunLun	Windows Secure Socket Tunneling Protocol (SSTP) Remote Code Execution Vulnerability	CVE-2022-34702
Aug 9, 2022	Yuki Chen with Cyber KunLun	Windows Secure Socket Tunneling Protocol (SSTP) Denial of Service Vulnerability	CVE-2022-34701
Jul 12, 2022	Yuki Chen with Cyber KunLun	Windows Network File System Remote Code Execution Vulnerability	CVE-2022-22039
Jul 12, 2022	Yuki Chen with Cyber KunLun	Remote Procedure Call Runtime Remote Code Execution Vulnerability	CVE-2022-22038
Jul 12, 2022	Yuki Chen with Cyber KunLun	Windows Network File System Remote Code Execution Vulnerability	CVE-2022-22029
Jul 12, 2022	Yuki Chen with Cyber KunLun	Windows Network File System Information Disclosure Vulnerability	CVE-2022-22028

Jun 14, 2022	Yuki Chen with Cyber KunLun	Windows Network File System Remote Code Execution Vulnerability	CVE-2022-30136
May 10, 2022	Yuki Chen with Cyber KunLun	Windows LDAP Remote Code Execution Vulnerability	CVE-2022-29141
May 10, 2022	Yuki Chen with Cyber KunLun	Windows LDAP Remote Code Execution Vulnerability	CVE-2022-29139
May 10, 2022	Yuki Chen with Cyber KunLun	Windows LDAP Remote Code Execution Vulnerability	CVE-2022-29137
May 10, 2022	Yuki Chen with Cyber KunLun	Windows LDAP Remote Code Execution Vulnerability	CVE-2022-29131
May 10, 2022	Yuki Chen with Cyber KunLun	Windows LDAP Remote Code Execution Vulnerability	CVE-2022-29130
May 10, 2022	Yuki Chen with Cyber KunLun	Windows LDAP Remote Code Execution Vulnerability	CVE-2022-29129
May 10, 2022	Yuki Chen with Cyber KunLun	Windows LDAP Remote Code Execution Vulnerability	CVE-2022-29128
May 10, 2022	Yuki Chen with Cyber KunLun	Windows LDAP Remote Code Execution Vulnerability	CVE-2022-22014
May 10, 2022	Yuki Chen with Cyber KunLun	Windows LDAP Remote Code Execution Vulnerability	CVE-2022-22013
May 10, 2022	Yuki Chen with Cyber KunLun	Windows LDAP Remote Code Execution Vulnerability	CVE-2022-22012
May 10, 2022	Yuki Chen with Cyber KunLun	Windows Network File System Remote Code Execution Vulnerability	CVE-2022-26937

Microsoft Bounty Program

- Microsoft Bug Bounty Programs Year in Review: $13.7M in Rewards (2022)
  - 2020: 13.7M USD ~= 4.1 億台幣
  - 2021: 13.6M USD ~= 4.1 億台幣
  - 2022: 13.7M USD ~= 4.1 億台幣



Microsoft Edge Bounty Program

- 微軟的新寵兒
  - Edge Security Team 處理相當快速
  - 只有 Edge Only 的 Bug 有獎金
  - 新功能不斷地冒出來
- 獎金比 Google Chromium 略高
  - Edge Sandbox Escape, PoC Only: $30,000
  - Chromium Sandbox Escape, PoC Only: $20,000
- 未完全開源，門檻高但仍是藍海

Microsoft

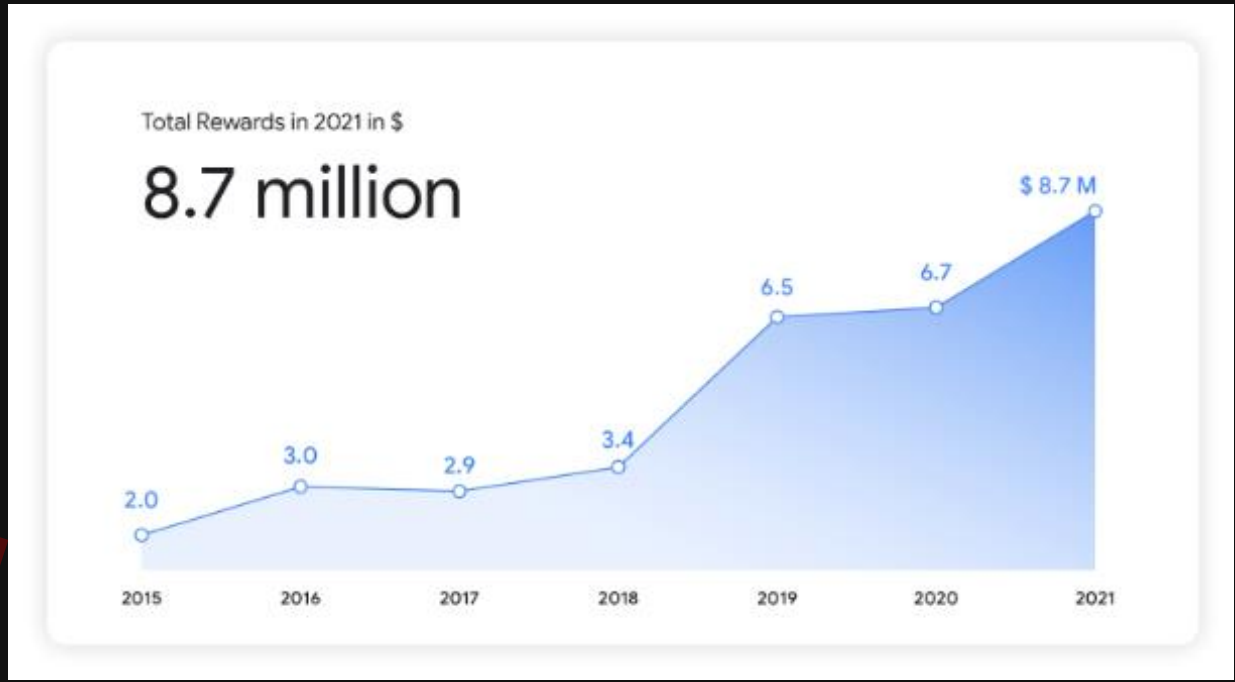
Google

👍 Pros

- 金額蠻有誠意
  - Pixel Titan M ~$1,000,000
- 公開透明 (Chrome / ChromeOS)
- 不需完整 Exploit 也能拿到獎金
- 項目多樣化
  - 借你機器跑 Fuzzer，找到漏洞也有錢
  - 寫 Patch 也有獎金
- 若捐給慈善機構會幫你 Double
- 各種福利
  - Hall of Fame
  - 年度小禮物

Not hunted yet!

Exclusive!



https://bughunters.google.com/

Google

👍 Pros

- 金額蠻有誠意
  - Pixel Titan M ~$1,000,000
- 公開透明 (Chrome / ChromeOS)
- 不需完整 Exploit 也能拿到獎金
- 項目多樣化
  - 借你機器跑 Fuzzer，找到漏洞也有錢
  - 寫 Patch 也有獎金
- 若捐給慈善機構會幫你 Double
- 各種福利
  - Hall of Fame
  - 年度小禮物

Not hunted yet!

Exclusive!

👎 Cons

- 還沒想到

Google

https://bughunters.google.com/

Google Bounty Program (Binary)

- Android and Google Devices Security Reward Program
- Chrome (ChromeOS) Vulnerability Reward Program
- Google Play Security Reward Program Rules
- kCTF VRP

Google

https://bughunters.google.com/

Google Bounty Program (Binary)

- Android and Google Devices Security Reward Program
- Chrome (ChromeOS) Vulnerability Reward Program
- Google Play Security Reward Program Rules
- kCTF VRP

Google

https://bughunters.google.com/

Chrome (ChromeOS) Vulnerability Reward Program

- 公開透明
  - 與工程師直接透過討論串協作
  - crbug.com 上的 Report 會在漏洞修復後的 14 週後公開
- 誠意滿滿
  - Browser Process 僅是 Crash 也有機會拿到獎金 ~$20,000
  - Sandbox Escape Exploit ~$40,000

Google

https://bughunters.google.com/

kCTF VRP

- kCTF is a Kubernetes-based infrastructure for CTF competitions
  - https://google.github.io/kctf/vrp.html
- Linux Kernel Exploit
  - nsjail Escape
  - Kubernetes Escape
  - ~$133,337
- Focus on Exploit Techniques
  - Must read flag on remote machine
  - 1-Day Allowed

Google

https://bughunters.google.com/

Samsung Mobile Rewards Program

👍 Pros

- 金額不錯
  - Bootloader / TrustZone ~$200,000
  - 有完整 Exploit 金額會高一點
- 有 Hall of Fame
- 沒了
- 中規中矩

👎 Cons

- 修完才給錢
  - ~5 months
- 金額 / 規則較不透明
  - $200 ~ $200,000
  - 差不多的漏洞拿過 $90,000 / $20,000 / $15,000
  - 或許跟年度預算有關
- 要扣稅 (22 %)
  - 微軟跟谷歌爸爸的金額都是稅後

https://security.samsungmobile.com/

Samsung Mobile Rewards Program

2021 **2020**

Rank	Name	SVE				
	**Chao Cheng Yu of TeamT5**	SVE-2019-14575	SVE-2019-15872	SVE-2020-16712		
	**hard_____**	SVE-2020-17270 SVE-2020-18356 SVE-2020-18469	SVE-2020-18034 SVE-2020-18392 SVE-2020-18471	SVE-2020-18158 SVE-2020-18418	SVE-2020-18254 SVE-2020-18467	SVE-2020-18271 SVE-2020-18468
It's Me! 	**Shih-Fong Peng of TeamT5**	SVE-2019-16587	SVE-2019-16588	SVE-2019-16589		

Apple (Mobile / Binary)

👍 Pros

- 2016 開始，2019 公開接受回報
- 金額開得很高
  - Network attack without user interaction
    $1,000,000
  - iOS 16 Lockdown Mode
    $2,000,000

> Apple will continue to strengthen Lockdown Mode and add new protections to it over time. To invite feedback and collaboration from the security research community, Apple has also established a new category within the Apple Security Bounty program to reward researchers who find Lockdown Mode bypasses and help improve its protections. Bounties are doubled for qualifying findings in Lockdown Mode, up to a maximum of $2,000,000 — the highest maximum bounty payout in the industry.

👎 Cons

- 封閉不透明
- 在研究員之間評價沒那麼好 (Binary)
  - 送出後只能祈禱
  - 乾脆透過 ZDI Submit 或寧願賣掉 / 公開
- Burned by Apple, researchers mull selling zero days to brokers
- 蘋果抓漏專案風評差：封閉、付款慢、修補也慢

https://developer.apple.com/security-bounty/

Apple (Mobile / Binary)

Jose Rodriguez
@VBarraquito

I will giveaway a very minor Lock Screen Bypass working in iOS 14.8 / 15RC

Apple values reports of issues like this with UP TO $25,000
but for reporting a more serious issue I was awarded with $5,000

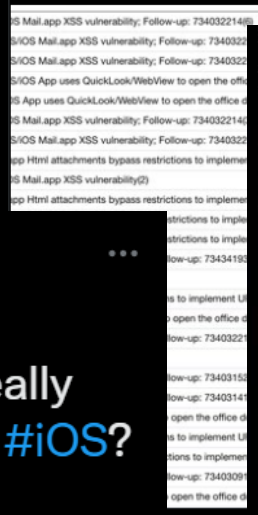
I will send in private a PoC video to who asks for it when iOS 15 is public.

heige
@80vul

Apple's bug bounty is a pretty magical thing! Recently, they awarded me a bounty for a bug I reported in 2020, and I complained about their bug report remediation process at the time

翻譯推文

> **heige** @80vul · 2021年10月14日
> [4] Until 2020, in line with the ethics of security researchers, I re-reported multiple vulnerabilities that affected many years to Apple, but the outcome is still the same. So far only one has been fixed in the latest MacOS. In fact, these vulnerabilities affect MacOS. And iOS.
> 顯示此對話串



Nicolas Brunner
@NicolasBrunner_

@Apple refuses to pay security bounty. Is that really how you want to treat people helping to improve #iOS? Here's my story: medium.com/macoclock/appl... #security #privacy

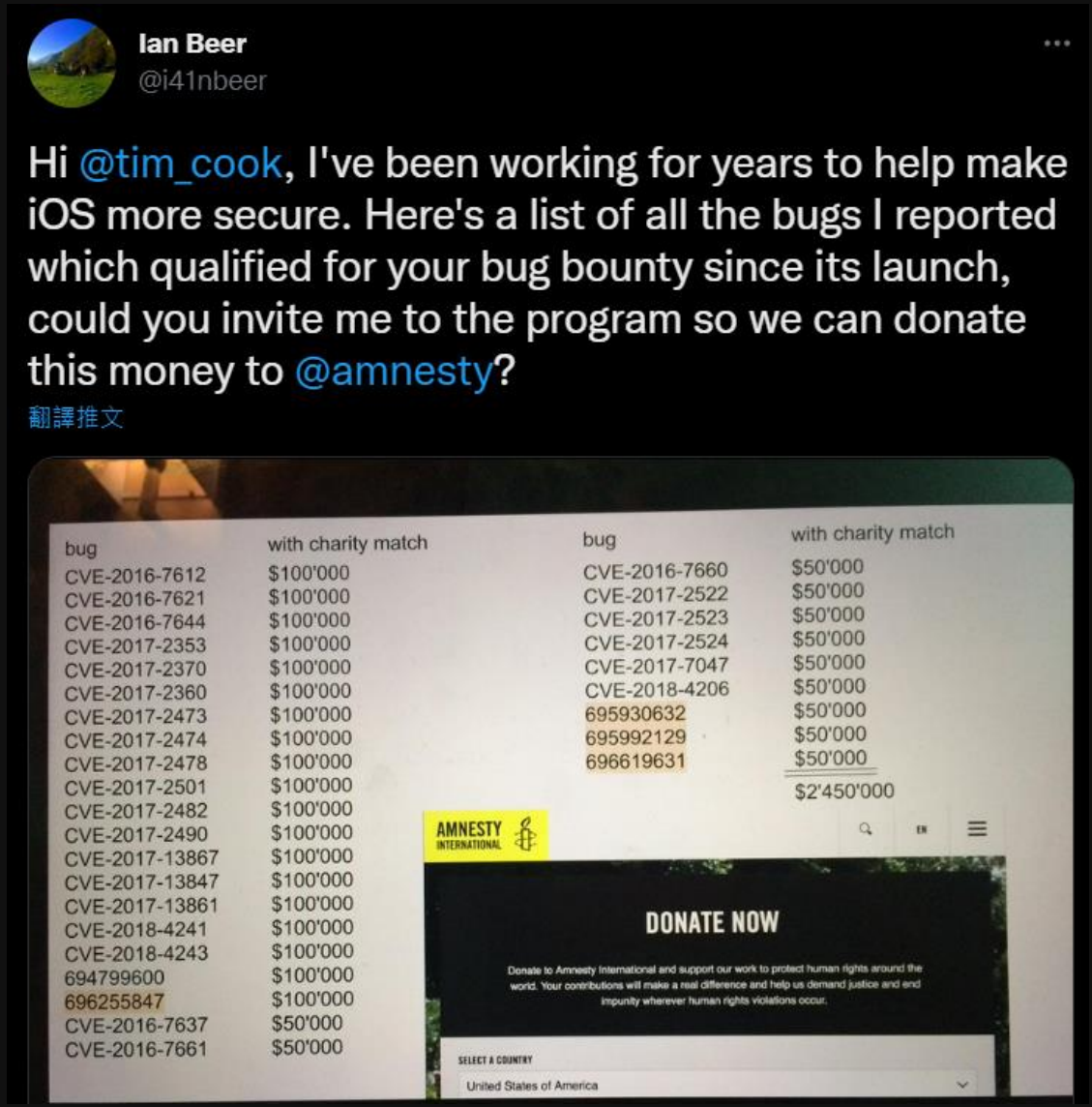
)22年4

Three iOS 0-days revealed by researcher frustrated with Apple's bug bounty arstechnica.com/information-te... **by** @jrssnet

arstechnica.com
Three iOS 0-days revealed by researcher frustrated with Apple's bug b...
Public disclosure comes in wake of other grumblings about Apple's bug bounty behavior.

Apple

- ProjectZero 研究員
  - 邀請 Apple 做公益
  - 沒下文



https://developer.apple.com/security-bounty/

Synology

- 本土優質廠商
  - ~$20,000
  - Bounty Program 經驗良好
  - 產品安全性有感提升，已經成為 Pwn2Own 上相當有挑戰性的目標

https://www.synology.com/security/bounty_program


一夜暴富系列
為了生活拚一把

Pwn2Own

- 駭客最高殿堂
  - 拿 0day 打筆電 / 手機 / 汽車...
  - 單一項目數萬到數十萬美金
  - 跟背後付出的努力比起來其實一點都不好賺...
- Trend Micro ZDI 主辦
  - 與各廠商合作，比賽現場直接將漏洞細節交付給原廠
- 殘酷賽制
  - 抽籤決定順序，跟前面隊伍撞洞就沒錢
  - 廠商有在前一天上 Patch 的習俗
- 成功打下來的設備可以帶回家

Pwn2Own

獎品太多? 打車載回家吧

Pwn2Own

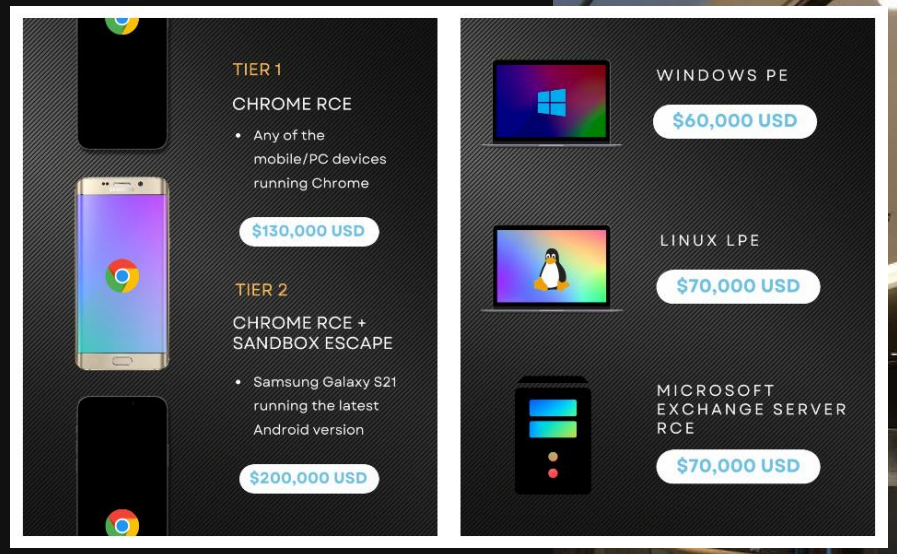
- Pwn2Own Vancouver
  - Browser / Hypervisor / OS / Web Server / Tesla
- Pwn2Own Tokyo/Austin (Mobile)
  - Mobile / NAS / Router / Printer / TV
- Pwn2Own Miami (ICS) *New!*
  - Control Server / OPC UA

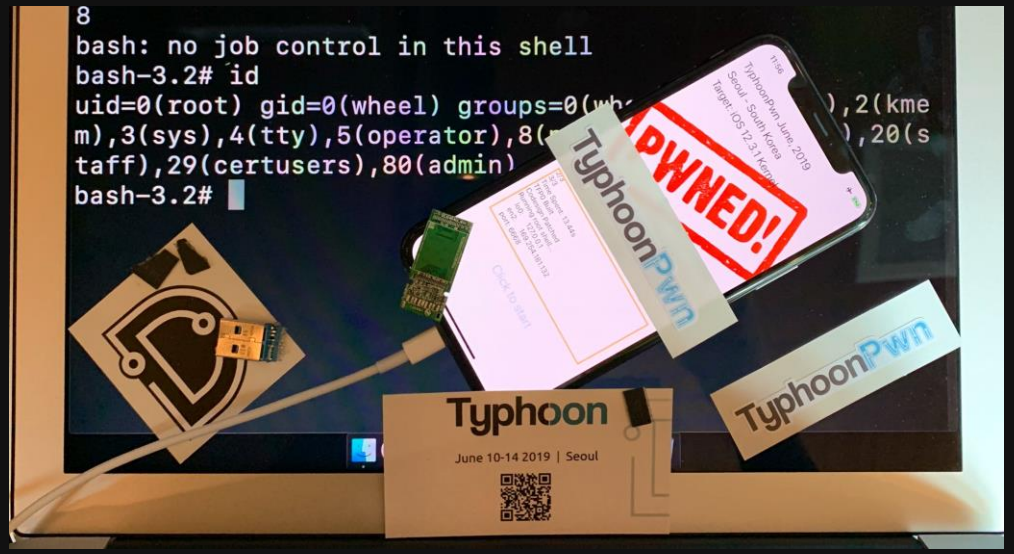
Pwn2Own

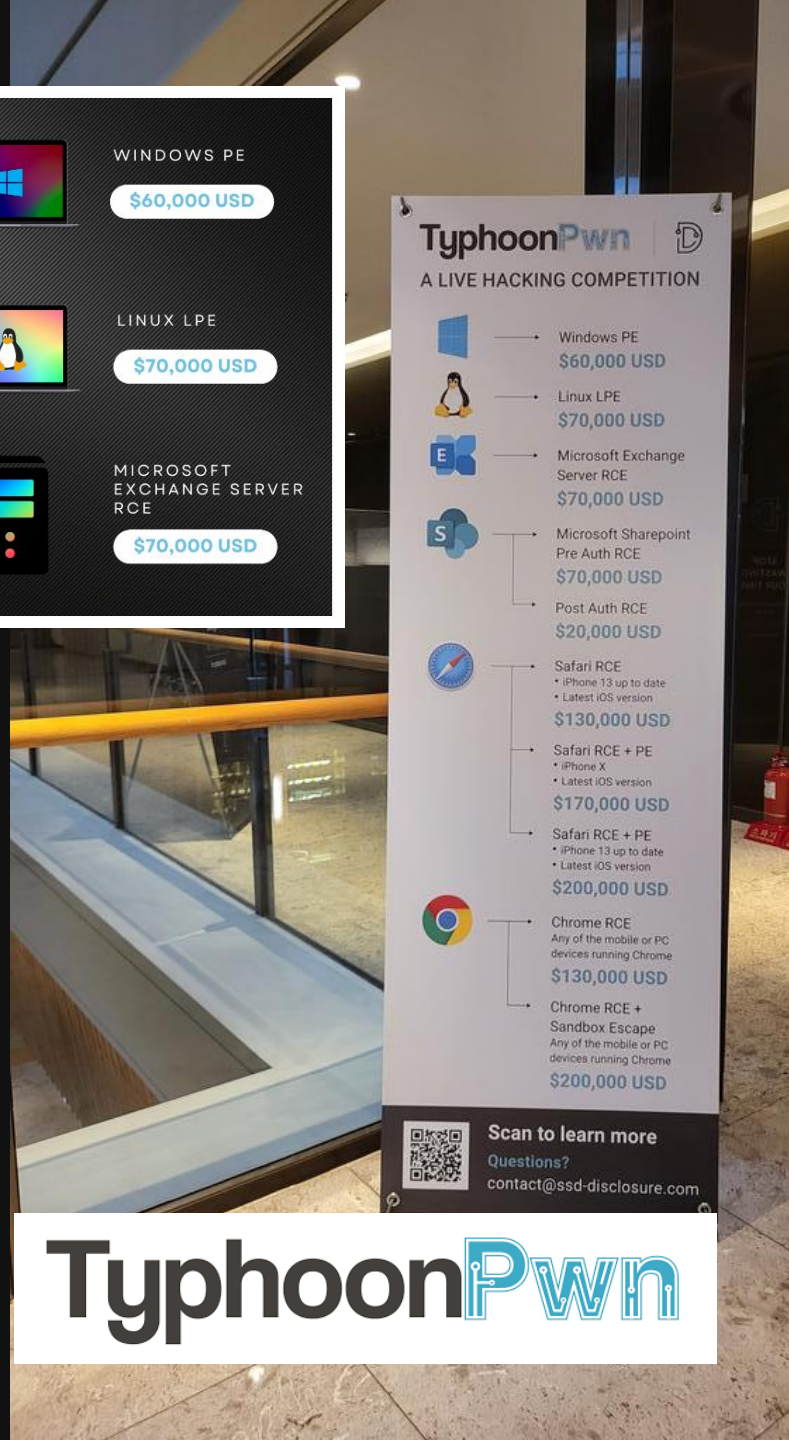
- Pwn2Own Vancouver 2022

TyphoonPwn

- SSD 主辦
  - 在韓國 TyphoonCon 舉辦
  - 類似 Pwn2Own
- Mobile / Browser / OS / Server
  - ~$200,000







TyphoonPwn

TianFu Cup 天府杯

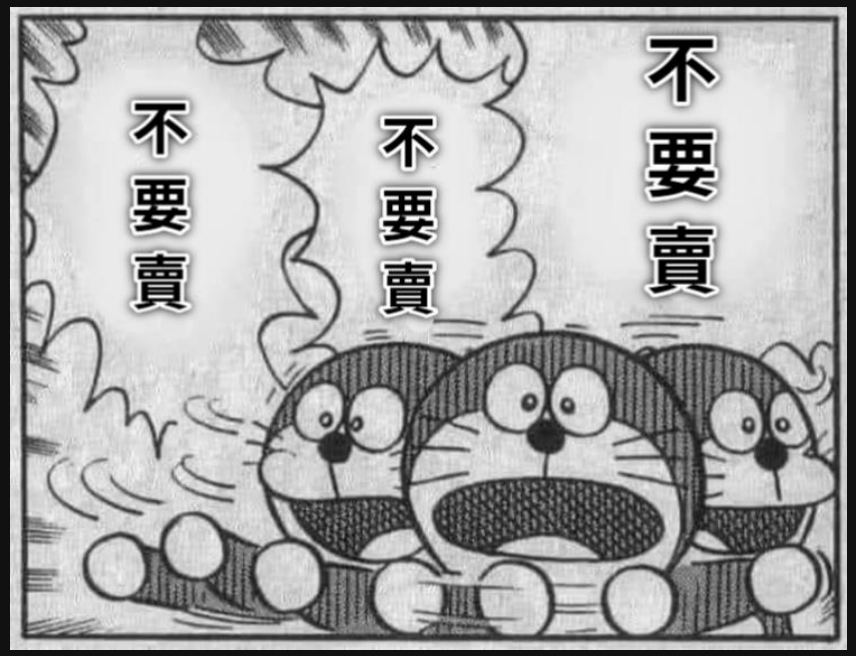
- 中國版本 Pwn2Own
  - 改進賽制，沒那麼殘酷
- 中國各大廠商合辦
  - 與原廠合作，並將漏洞細節交付給原廠

Target	2021TFC Prize(RCE)	2021TFC EXTRA Prize(RCE + Sandbox Escape)	Note
Chrome	$50,000	$150,000	
Safari	$40,000	$75,000	M1:RCE=$60000; M1: RCE+Sandbox=$120000
Adobe PDF Reader	$30,000	$40,000	
Docker-CE	/	$60,000	
Ubuntu 20/CentOS 8	/	$40,000	
Microsoft Exchange Server 2019	$60,000	$200,000	
Windows 10	$20,000	$40,000	
VMware Workstation	/	$80,000	
VMware ESXi	/	$180,000	
Ubuntu + qemu-kvm	$60,000	$150,000	
Parallels Desktop	/	$30,000	
iPhone 12 pro	$120,000	$180,000	Remote Jailbreak : $300000
Domestic mobile phones(Android)	to be updated	to be updated	Please contact us for the details of the brand and model.
Synology DS220j	/	$10,000	
ASUS Router AX56U	/	$10,000	
Domestic vehicle	to be updated	to be updated	

TianFu Cup 天府杯

ZERODIUM

- 漏洞中盤商 != Bug Bounty
  - 價格遠高於各公司獎勵
    - ~$2,500,000
  - 市場價格更高
- 不要輕易出售你的研究
  - Exploit 是武器
  - 無法得知漏洞被如何使用



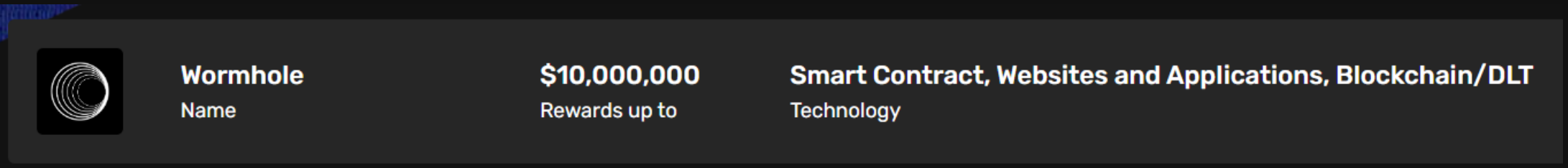
Up to $2,500,000									1.001 Android FCP Zero Click Android	1.002 iOS FCP Zero Click iOS
Up to $2,000,000									2.001 WhatsApp RCE+LPE Zero Click iOS/Android	2.002 iMessage RCE+LPE Zero Click iOS
Up to $1,500,000									2.003 WhatsApp RCE+LPE iOS/Android	2.004 SMS/MMS RCE+LPE iOS/Android
Up to $1,000,000										
Up to $500,000	3.001 Persistence iOS	2.005 WeChat RCE+LPE iOS/Android	2.006 iMessage RCE+LPE iOS	2.007 FB Messenger RCE+LPE iOS/Android	2.008 Signal RCE+LPE iOS/Android	2.009 Telegram RCE+LPE iOS/Android	2.010 Email App RCE+LPE iOS/Android	4.001 Chrome RCE+LPE Android	4.002 Safari RCE+LPE iOS	
Up to $200,000	5.001 Baseband RCE+LPE iOS/Android		6.001 LPE to Kernel/Root iOS/Android	2.011 Media Files RCE+LPE iOS/Android	2.012 Documents RCE+LPE iOS/Android	4.003 SBX for Chrome Android	4.004 Chrome RCE w/o SBX Android	4.005 SBX for Safari iOS	4.006 Safari RCE w/o SBX iOS	
Up to $100,000	7.001 Code Signing Bypass iOS/Android	5.002 WiFi RCE iOS/Android	5.003 RCE via MitM iOS/Android	6.002 LPE to System Android	8.001 Information Disclosure iOS/Android	8.002 [k]ASLR Bypass iOS/Android	9.001 PIN Bypass Android	9.002 Passcode Bypass iOS	9.003 Touch ID Bypass iOS	

** All payouts are subject to change or cancellation without notice. All trademarks are the property of their respective owners.*

2019/09 © zerodium.com

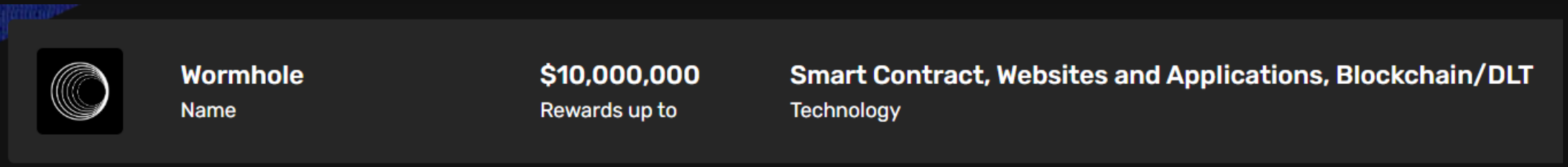
Block Chain

- 前面都開玩笑的，這個才是真正的一夜暴富
- Web3's leading bug bounty platform
  - https://immunefi.com/



Block Chain

- 前面都開玩笑的，這個才是真正的一夜暴富
- Web3's leading bug bounty platform
  - https://immunefi.com/



- 歷史紀錄: 發出 $10,000,000 的 Bounty (3 億新台幣)
  - Wormhole Uninitialized Proxy Bugfix Review

那些我領過的賞金

漏洞與牠們的產地

斂財手法

- 腳踏實地
  - Code Review / Reversing
- 挖礦致富
  - Fuzzing
- 搶頭香
  - 新出現的 Bounty Program / 目標
- 心誠則靈
  - 純運氣

腳踏實地

- Code Review / Reversing
- Samsung Fingerprint Trustlet Code Execution: $XX,XXX
  - Full Chain Exploit
  - Samsung Security Updates
- Trend Micro Apex One LPE: $XX,XXX
  - Multiple Patch Bypass
  - ZDI TIP Program
- IoTs: $XX,XXX
  - Pre-Auth RCEs
  - Router / NAS etc
  - 基本上就是一些軟柿子

挖礦致富

- Fuzzing
  - 挖 ETH 不如挖 BUG

挖礦致富

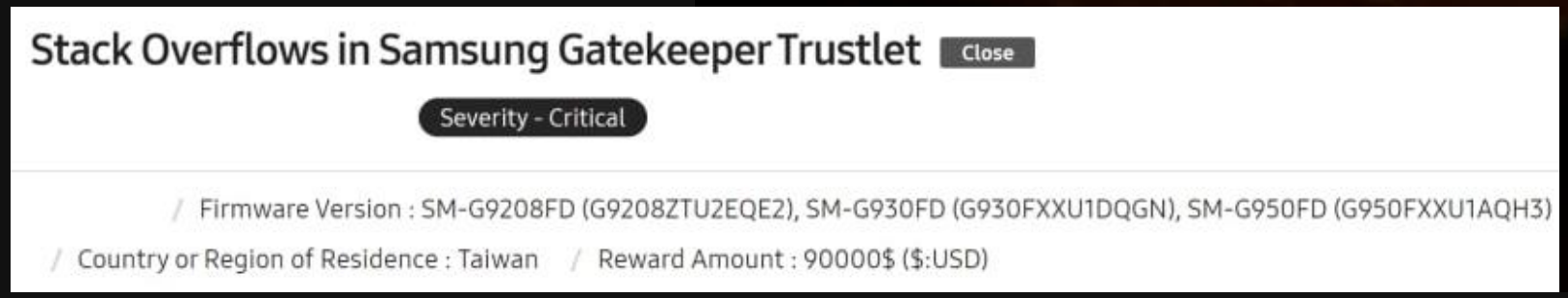
- Windows Parsers: $XXX,XXX
  - LNK, PoC Only: $30,000
  - 找 Attack Surface / 抄作業大賽
  - 可於每個 Patching Tuesday* 關注 MSRC 致謝頁面
- ZDI: $XX,XXX
  - PoC Only: $500 - $2500
  - 流行: Foxit Reader / Adobe / Advantech / Autodesk…
  - 可關注 ZDI Advisory

* Second Tuesday of every month

搶頭香

- Pwn2Own Tokyo 2020
  - NAS 目標首次登場，挑軟柿子打
  - 跟隊友花了一個下午找了兩個目標的洞
  - 「賭抽籤第一個抽到我」
  - 第三名 + $25,000
    - 抽籤大賽

- 當時 Samsung TrustZone 沒什麼人研究 (2017)
  - 隊友經驗: Gatekeeper Trustlet Stack Overflow Exploit: $90,000
  - ~~可能預算花不完~~



搶頭香

- 可以鎖定新出現在 Pwn2Own 上的目標
  - Pwn2Own Tokyo 2020: WD PR4100 NAS: $20,000
    - 6 Teams Targeted
  - Pwn2Own Vancouver 2021: Parallel Desktop $40,000
    - 6 Teams Targeted
    - 隔年就被從清單移除了
  - Pwn2Own Austin 2021: Printers $20,000
    - 11 Teams Targeted
  - Pwn2Own Miami for 2022落幕，研究人員找到26個位於工業控制系統的零時差漏洞
    - Keuper向《MIT Technology Review》表示，這是他們所參加過最簡單的競賽，因為工業控制系統中有太多唾手可得的成果，這是個安全性落後許多的領域
    - DOS 就有錢
- 挖漏洞就像買房子，永遠後悔沒早點下手

心誠則靈

- 漏洞研究員最高境界
  - 不用去找漏洞，漏洞會來找你
- Chromium Edge Immersive Reader UAF

  DEMO

PID: 2588 - WinDbg 1.2206.19001.0

File | Home | View | Breakpoints | Time Travel | Model | Scripting | Source | Memory | Command

Break | Go | Step Out | Step Into | Step Over | Step Out Back | Step Into Back | Step Over Back | Go Back | Restart | Stop Debugging | Detach | Settings | Source | Assembly | Local Help | Feedback Hub

Flow Control | Reverse Flow Control | End | Preferences | Help

Disassembly | Registers | Memory 0

Command

```
ModLoad: 00007ffc`552f0000 00007ffc`553b4000   C:\Windows\System32\ShellCommonCommonProxyStub.dll
ModLoad: 00007ffc`5c750000 00007ffc`5c7a1000   C:\Windows\System32\vaultcli.dll
ModLoad: 00007ffc`55e20000 00007ffc`55ee3000   C:\Windows\System32\Windows.Web.dll
ModLoad: 00007ffc`68bb0000 00007ffc`68bde000   C:\Windows\System32\aadWamExtension.dll
ModLoad: 00007ffc`69c70000 00007ffc`69c85000   C:\Windows\System32\Windows.System.UserProfile.DiagnosticsSettings.dll
ModLoad: 00007ffc`71670000 00007ffc`71688000   C:\Windows\System32\CRYPTSP.dll
ModLoad: 00007ffc`70e00000 00007ffc`70e34000   C:\Windows\system32\rsaenh.dll
ModLoad: 00007ffc`36130000 00007ffc`36258000   C:\Program Files (x86)\Microsoft\Edge\Application\89.0.774.50\learning
ModLoad: 00007ffc`735b0000 00007ffc`73a22000   C:\Windows\System32\SETUPAPI.dll
ModLoad: 00007ffc`68fa0000 00007ffc`69014000   C:\Windows\SYSTEM32\wlanapi.dll
ModLoad: 00007ffc`6c6c0000 00007ffc`6c76e000   C:\Windows\SYSTEM32\mscms.dll
ModLoad: 00007ffc`6cde0000 00007ffc`6cdf1000   C:\Windows\SYSTEM32\ColorAdapterClient.dll
ModLoad: 00007ffc`58ce0000 00007ffc`58f1c000   C:\Windows\System32\Windows.Devices.Bluetooth.dll
ModLoad: 00007ffc`58710000 00007ffc`58749000   C:\Windows\System32\Windows.Networking.HostName.dll
ModLoad: 00007ffc`58610000 00007ffc`58705000   C:\Windows\System32\Windows.Networking.dll
ModLoad: 00007ffc`585b0000 00007ffc`58607000   C:\Windows\System32\BiWinrt.dll
ModLoad: 00007ffc`5aa90000 00007ffc`5ab49000   C:\Windows\System32\Windows.Networking.Connectivity.dll
ModLoad: 00007ffc`63e90000 00007ffc`63f17000   C:\Windows\System32\Windows.Devices.Enumeration.dll
ModLoad: 00007ffc`5fd10000 00007ffc`5fd49000   C:\Windows\System32\Windows.Devices.Radios.dll
ModLoad: 00007ffc`63a10000 00007ffc`63a30000   C:\Windows\System32\DevDispItemProvider.dll
ModLoad: 00007ffc`6a8e0000 00007ffc`6a8ee000   C:\Windows\System32\DDORes.dll
ModLoad: 00007ffc`68590000 00007ffc`68598000   C:\Windows\System32\DefaultDeviceManager.dll
ModLoad: 00007ffc`58170000 00007ffc`581af000   C:\Windows\System32\CapabilityAccessManagerClient.dll
ModLoad: 00007ffc`62e20000 00007ffc`62e3f000   C:\Windows\system32\BthRadioMedia.dll
ModLoad: 00007ffc`62a10000 00007ffc`62a91000   C:\Windows\SYSTEM32\webauthn.dll
ModLoad: 00007ffc`6bc90000 00007ffc`6bd05000   C:\Windows\SYSTEM32\cryptngc.dll
(a1c.1a98): Break instruction exception - code 80000003 (first chance)
ntdll!DbgBreakPoint:
00007ffc`74730860 cc              int     3
0:048> g
onecore\com\combase\dcomrem\preventrundownbias.cpp(1310)\combase.dll!00007FFC72AFD82C: (caller: 00007FFC72AFD659) Log
```

BUSY Debuggee is running...

Locals

Name | Value

Locals | Watch

Threads

```
[0x860] = msedge_exe!wWinMainCRTStartup (00007ff6`8dceffe0)
[0x1be4] = ntdll!TppWorkerThread (00007ffc`746e2ad0)
[0x1128] = ntdll!TppWorkerThread (00007ffc`746e2ad0)
[0x10b0] = ntdll!TppWorkerThread (00007ffc`746e2ad0)
[0xa84] = msedge!base::`anonymous namespace'::ThreadFunc (00007ffc`1f26daa0)
[0x520] = msedge_exe!sandbox::BrokerServicesBase::TargetEventsThread (00007ff6`8
[0x16dc] = combase!CRpcThreadCache::RpcWorkerThreadEntry (00007ffc`72b3add0)
[0xbc4] = ntdll!TppWorkerThread (00007ffc`746e2ad0)
[0x494] = ntdll!TppWorkerThread (00007ffc`746e2ad0)
[0x1608] = msedge!base::`anonymous namespace'::ThreadFunc (00007ffc`1f26daa0)
```

Threads | Stack | Breakpoints

首頁 | HITCON PEACE 2022

https://hitcon.org/2022/

議程 | 活動 | 會場資訊 | 贊助 | 籌備團隊 | Login | ENG

HITCON PEACE 2022

SURVIVAL GUIDE FOR THE CYBER WAR

>> Login <<

08/19 | 08/20 南港展覽館二館 七樓 星光會議中心

取得門票

活動實際舉行將配合政府防疫政策，請關注官方公告，隨時了解最新訊息。

HITCON PEACE 2022

10:47 PM 8/17/2022

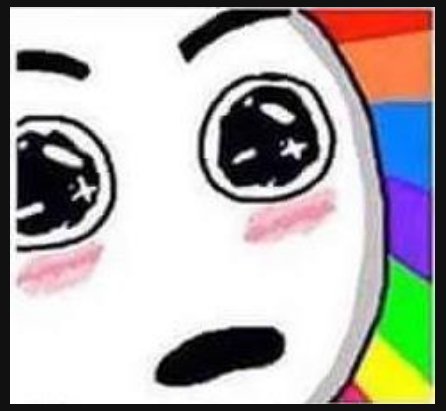
心誠則靈

- Chromium Edge Immersive Reader UAF: $30,000
  - Edge Bounty Program 項目最高金額

Microsoft Security Response Center <secure@microsoft.com>
寄給 我、 MSFT

Hello,

Thank you for taking the time to share your report. Based on the assessment from our engineering team, we have determined that your case 64466 is eligible for a US$30000.00 bounty award under the Edge on Chromium Bounty Program. Congratulations!



心誠則靈

心誠則靈

- Chromium Heap Overflow: $7,000
  - PoC Only
  - 寫 Edge Fuzzer 拿 Chromium PoC 測試時找到的…
  - 在 Edge 很容易觸發，沒人發現
- 講個祕密: 其實很多 Chromium 的漏洞都可以用手按出來…
  - Chromium Disclosed Security Bugs

心誠則靈

- 不要因為怕被拒絕而不敢回報
  - 先回報就對了
- 機會是留給準備好的人
  - 沒有 Background Knowledge，漏洞掉在你眼前你也不會發現
  - 講個祕訣: 從今天開始改用 Asan Chromium 上網
    - 拿到 Bounty 記得分我紅包
    - My ETH Wallet

回報技巧

為什麼你拿的比較多?

回報小技巧 1 – 作文比賽

- 報告撰寫
  1. 符合官方要求格式
  2. 盡可能詳細描述
  3. 附上 PoC，讓對方能快速重現，若重現方式較複雜可附上影片
  4. 以研究員角度提供可行的修補建議
  - 微軟報告撰寫範例: Example Report Submissions to the MSRC
  - ZDI 報告撰寫建議: GETTING INTO SUBMITTING: HOW TO MAXIMIZE YOUR RESEARCH
- 誠意很重要
  - PDF vs TXT / 就算 PoC 只有一行也包裝一下

回報小技巧 1 – 作文比賽

- 重要程度
  - 漏洞重現方式 / PoC >= 成因分析 > Exploit
    - 當然也有些廠商重視 Exploit
  - 研究員與工程師想的不一樣
    - 研究員: 我都彈小算盤了欸，報告應該滿分吧
    - 工程師: 今天下班前要修好…但窩看不懂 QQ
  - 通常把漏洞補好才是首要任務
- 規則就是一切
  - 贏的不是有 Exploit 的人，是符合規則的人
  - 莊家最大

回報小技巧 2 – 先上車後補票

- 若擔心回報拖太久被撞洞或修補，可以先送出初步的分析
  - 後續再補上詳細分析或是完整 Exploit

- 相反案例
  - 找到極佳 Attack Surface ，可能會被一次性修補
  - 囤積報告一次性送出
  - 隊友經驗
    - Samsung: Missing Param Type Check in Trustlet
      - 花一週趕工寫 Exploit
      - 10+ Critical CVEs
      - Samsung 怕了，說後面送的不算了 好險

回報小技巧 2 – 先上車後補票

14607	CVE-2019-20589	843	Exec Code	2020-03-24	2020-03-30	10.0	None	Remote	Low	Not required	Complete	Complete	Complete

An issue was discovered on Samsung mobile devices with O(8.x) and P(9.0) (with TEEGRIS) software. There is type confusion in the SKPM Trustlet, leading to arbitrary code execution. The Samsung ID is SVE-2019-14892 (August 2019).

14608	CVE-2019-20588	843	Exec Code	2020-03-24	2020-03-30	10.0	None	Remote	Low	Not required	Complete	Complete	Complete

An issue was discovered on Samsung mobile devices with O(8.x) and P(9.0) (with TEEGRIS) software. There is type confusion in the SEM Trustlet, leading to arbitrary code execution. The Samsung ID is SVE-2019-14891 (August 2019).

14609	CVE-2019-20587	843	Exec Code	2020-03-24	2020-03-27	10.0	None	Remote	Low	Not required	Complete	Complete	Complete

An issue was discovered on Samsung mobile devices with O(8.1) and P(9.0) (with TEEGRIS) software. There is type confusion in the MLDAP Trustlet, leading to arbitrary code execution. The Samsung ID is SVE-2019-14867 (August 2019).

14610	CVE-2019-20586	843	Exec Code	2020-03-24	2020-03-27	10.0	None	Remote	Low	Not required	Complete	Complete	Complete

An issue was discovered on Samsung mobile devices with O(8.1) and P(9.0) (with TEEGRIS) software. There is type confusion in the FINGERPRINT Trustlet, leading to arbitrary code execution. The Samsung ID is SVE-2019-14864 (August 2019).

14611	CVE-2019-20585	843	Exec Code	2020-03-24	2020-03-27	10.0	None	Remote	Low	Not required	Complete	Complete	Complete

An issue was discovered on Samsung mobile devices with O(8.x) and P(9.0) (with TEEGRIS) software. There is type confusion in the SEC_FR Trustlet, leading to arbitrary code execution. The Samsung ID is SVE-2019-14851 (August 2019).

14612	CVE-2019-20584	843	Exec Code	2020-03-24	2020-03-27	10.0	None	Remote	Low	Not required	Complete	Complete	Complete

An issue was discovered on Samsung mobile devices with O(8.x) and P(9.0) (with TEEGRIS) software. There is type confusion in the HDCP Trustlet, leading to arbitrary code execution. The Samsung ID is SVE-2019-14850 (August 2019).

14613	CVE-2019-20583	843	Exec Code	2020-03-24	2020-03-27	10.0	None	Remote	Low	Not required	Complete	Complete	Complete

An issue was discovered on Samsung mobile devices with O(8.x) and P(9.0) (with TEEGRIS) software. There is type confusion in the EXT_FR Trustlet, leading to arbitrary code execution. The Samsung ID is SVE-2019-14847 (August 2019).

回報小技巧 3 – 影分身之術

- 礙於 Policy ，單個報告能給的獎金可能有限
  - RCE -> Leak + Overflow / Multiple exploit chains ref to same leak bug
  - 比較遵循 Policy 的公司就適合把 Exploit Chain 拆開報
  - e.g. Microsoft, Samsung / 反例: Google
- 小八卦
  - 微軟很喜歡把多個 Case Merge 成單一個 CVE / Patch
  - 前幾年也出現過爭議，多個不同類型的洞被 Merge 成同一個 CVE
    - Bounty 也變一筆了…
  - ~~我懷疑他們內部會比賽誰可以用一個 Patch 修好最多 Bug~~

回報小技巧 4 – 據理力爭

- Vendor 不一定是對的
  - 錢太少、等太久都可以主動寫信溝通
    - 有時候是真的漏掉或發錯金額
  - 尊重 Vendor 最後決定，不要變成 Beg Bounty

- 慘痛經驗
  - 回報 Pre-auth RCE 給 Vendor 得到獎金 $500
  - 許久以後 CVE 發出來才發現被 Vendor 誤判成 XSS

回報小技巧 5 – 窮追不捨

- 追 Patch
  - 一出新版馬上打開來看怎麼修的
- 追 Commit
  - 研究員會專門盯著某些常寫出 bug 的開發者的 commit
  - Chromium
- 個人經驗
  - Vendor 發了 CVE 及 Patch，打開分析發現 完全沒修正
    - 再回報一次，並附上建議修正方式
  - 連續發了三次 CVE ，還是都沒修
    - 一份報告拿了三次獎金
  - 終於修好了之後...發現可以被繞過。
    - 此時已經過去了一年

給新手獵人的建議

- 從小目標找起，培養信心，相信高額獎金不只是都市傳說
- 累積足夠的背景知識，機會出現時才能把握
- 隨時關注各大漏洞修補資訊，跟上潮流
- 獎金不是最重要的，但可以是一個學習的動力與挑戰
  - ~~不要沉迷，不然會太有錢~~
- 「勿驕矜自滿，勿忘初衷」

Thank You

 @_L4ys