



그대들은 어떻게 살 것인가 (feat. V8 CTF)



Agenda



- 자기소개
- 제목으로 선택한 이유
- 나를 만든 경험들
- 그 이후
- Q&A

자기소개



박도영(adawn)

- Browser Security Researcher , Bug Bounty Hunter
- Sk Shieldus EQST Lab - V8
- ION - BreadHackers
- BoB VA - 14th
- WHS 2nd

자기소개



- CVE-2026-59754 , CVE-2026-62404 , CVE-2026-62408 ... +33 (assigned)
- V8CTF n-day submission (M147) , V8CTF n-day submission (M148)
- CVE-2026-43658 (WebKit)
- DEF CON CTF 2026 finals 9th
- Midnight Sun CTF 2026 Finals 3rd

자기소개



- 2nd Place, D^3CTF 2026, EQST, July 25-26, 2026
- 4th Place, Junior.Crypt.2026 CTF, adawn, July 11-12, 2026
- 2nd Place, R3CTF 2026, EQST, July 4-6, 2026
- 9th Place, HACKTHEON SEJONG 2026 Qualifier, Advanced Division, MeowMeow, Apr 25, 2026, advanced to finals
- 3rd Place, UMD CTF Open Division, EQST, Apr 24-26, 2026
- 4th Place, b01lers CTF, EQST, Apr 18-20, 2026
- 4th Place, Incognito CTF, EQST, Apr 14-15, 2026
- 8th Place, TAMU CTF, EQST, Mar 20-22, 2026
- 1st Place, Midnight CTF Quals Professional Division, EQST & Rubiya Team, Mar 13-15, 2026

제목으로 선택한 계기



© Hackingcamp. All Rights Reserved



POC SECURITY

제목으로 선택한 계기



나는 앞으로 어떻게 살아갈지에 대한 고민

나를 만든 경험들 - WHS



군대가기 이전



나를 만든 경험들 - WHS



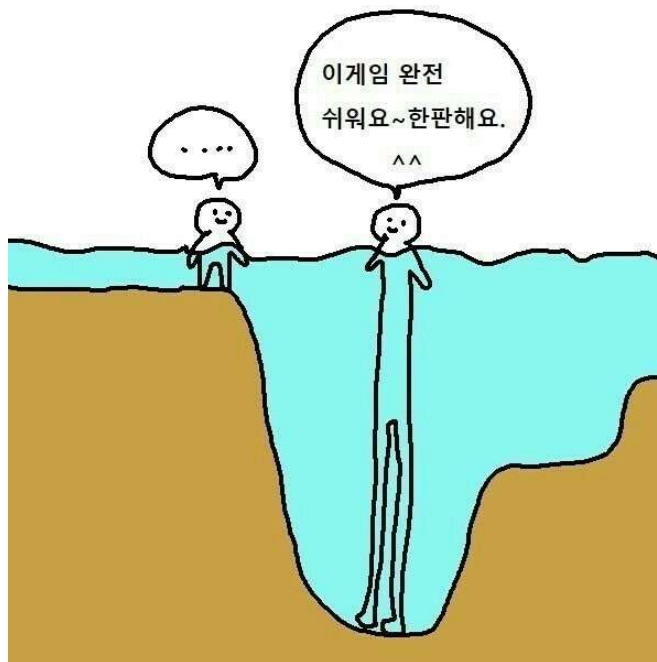
군대에서



나를 만든 경험들 - WHS



전역하고 나서



© Hackingcamp. All Rights Reserved

나를 만든 경험들 - WHS



화이트햇 스쿨
WhiteHat School



나를 만든 경험들 - WHS



프로젝트 선정

박도영 BACK 2024-04-29 오후 9:48

저는 SMB 프로토콜과 powershell을 선정하였습니다. SMB 프로토콜은 많은 취약점들이 존재하고 일상생활에 많이 사용되는 거 같아서 한 번 연구해보면 좋을 거 같아서 선정하게 되었고 powershell은 powershell 자체에 취약점이 존재한다면 위험할 거 같아서 선정하게 되었습니다. 타겟을 선정할때 고민했었던 건 NAS가 있었는데 회사와 같은 비즈니스 부터 가정에서 까지 사용한다고 하여 타겟으로 할까 고민하다가 앞에 두개를 고르게 되었습니다 해당 문서는 SMB 프로토콜과 powershell에 있던 취약점들에 대해 간략히 찾아본 결과입니다. (수정됨)

나를 만든 경험들 - WHS



프로젝트 선정



나를 만든 경험들 - WHS



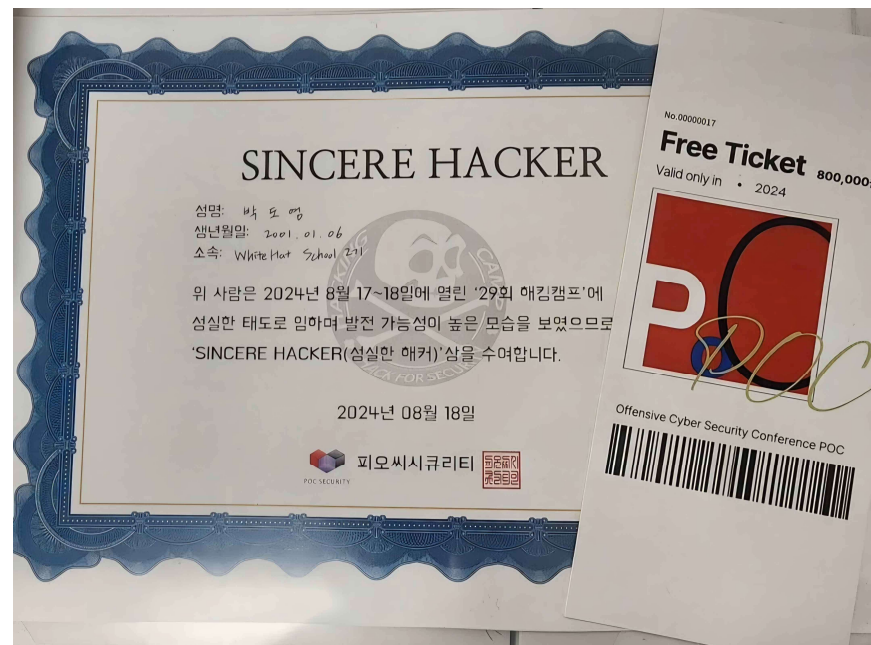
프로젝트

내용		5월					6월				7월	
		1	2	3	4	5	1	2	3	4	1	2
사전조사	자료 수집 및 개념 정리											
취약점 분석	환경설정											
	Root cause 분석											
	정적 분석 및 동적 분석											
익스플로잇 개발	exploit primitive 이해											
	mitigation 우회 및 exploit 작성											
문서화	격주 보고서											
	중간 보고서											
	최종 보고서											
발표	중간 발표											
	최종 발표											

나를 만든 경험들 - WHS



프로젝트 이후



29회 해킹캠프



과학교육정보통신부
Ministry of Science and ICT

KITRI 한국정보기술연구원
Korea Technology Research Institute

차세대 보안리더 양성 프로그램

BoB14기 모집

**2025. 4. 30.(수) 10:00
~ 5. 27.(화) 16:00**



모집대상

- 지원자 없음 마감일 기준 미취학 아동, 학생
- 2009년 12월 31일 이전 출생자
- 2024. 7월 ~ 2025. 3월 사이에 영어 가능할 자
- **무대사항**
 - 학교장, 교수 등 지도자의 인제 추천서 보유자
 - 일반 중학교 재학생이외의 자를 추천 가능한 입찰자
 - 워킹보트 스쿨 우수 수료자
- **지원제한사항**
 - 교육기관 중 재직자, 취업 학생자, 군복무(산입가능요령 포함)중인 자
 - * BoB 14명기(원부기)에 재직중인 경우 지원 가능
 - 차세대 보안리더 교육과정의 재직 및 출생지 불일치
 - 교육기관 중 장부 주권 위조인자 지원 프로그램 등 참여(예정)자
 - 차세대 보안리더 교육과정 수료생(제 1기~13기)

모집설명회

2025년 5월 17일(토) 14:00 / BoB 센터
* 세부 내용 추후 공지(홈페이지 참조)

교육기간

2025년 7월 1일 ~ 2026년 3월 31일

문의처

한국정보기술연구원 BoB센터
☎ 02-869-8301(내선) / bob@kitri.re.kr

접수방법

인터넷 접수 BoB 홈페이지(http://www.bob14.kr)
BoB 명함, 교육재 지원, 지원서 작성

제출 일정

1) 지원서 2) 자기소개서 3) 학교장/제시서
4) 개인정보수집·이용 동의서 5) 추천서(배정자)

지원사항

- ☐ 학업 지원
- ☐ 학원 지원
- ☐ 스포츠 교육
- ☐ A형 입양 지원
- ☐ 진로 지원
- ☐ 생활 지원
- ☐ 진로 지원
- ☐ 무주 교육원
- ☐ 생활 지원

교육특징

학교 보안 인문기에 대한 1개월 전도형 프로그램(현장 무교)
현장에서 요구하는 실무 중심 프로젝트 수행 및 교육

특전사항

- ☐ BoB 인재(BEST 10)
- ☐ 한국정보기술연구원
- ☐ BoB 인재(BEST 10)
- ☐ 한국정보기술연구원
- ☐ BoB 인재(BEST 10)
- ☐ 한국정보기술연구원
- ☐ BoB 인재(BEST 10)
- ☐ 한국정보기술연구원

선발절차

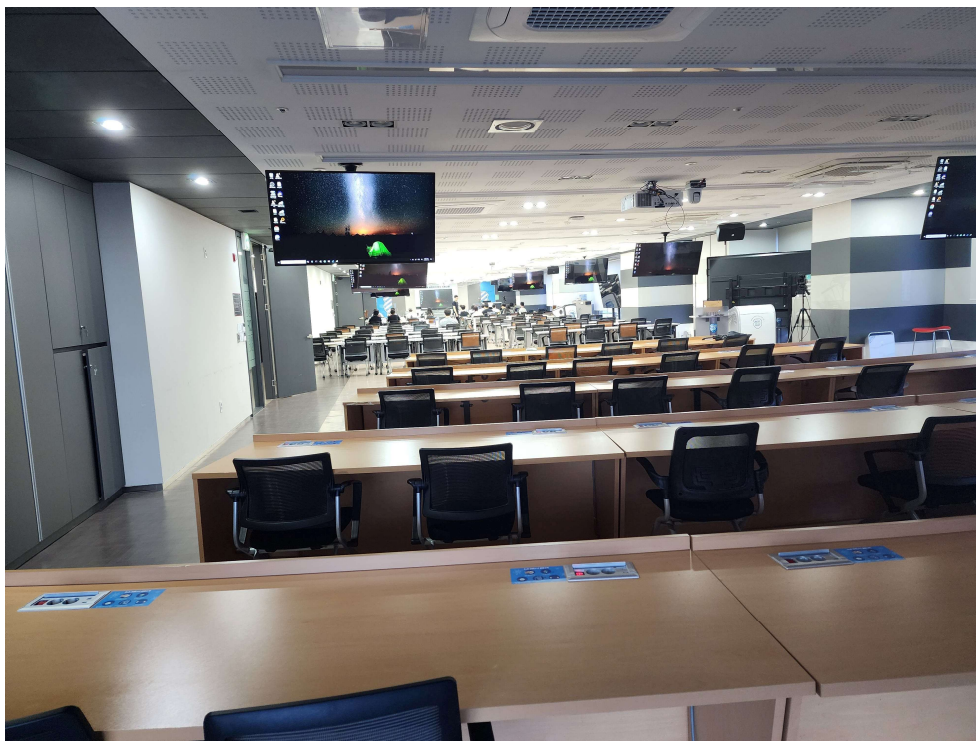
BoB 14기

서류 접수	서류 선별	면접 진행	면접 결과	합격자 발표
1. 지원서 학술계획서 등	2. 면접 평가사항	3. 심층 면접	4. 합격자 발표 6/18(수) 발표	

나를 만든 경험들 - BOB



공통 교육



© Hackingcamp. All Rights Reserved

나를 만든 경험들 - BOB



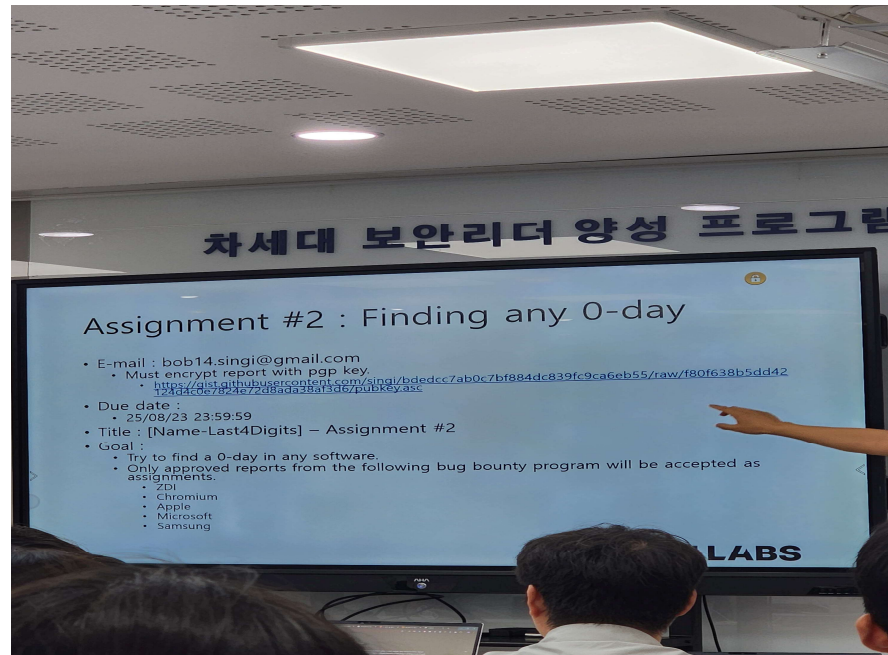
공통 교육



나를 만든 경험들 - BOB



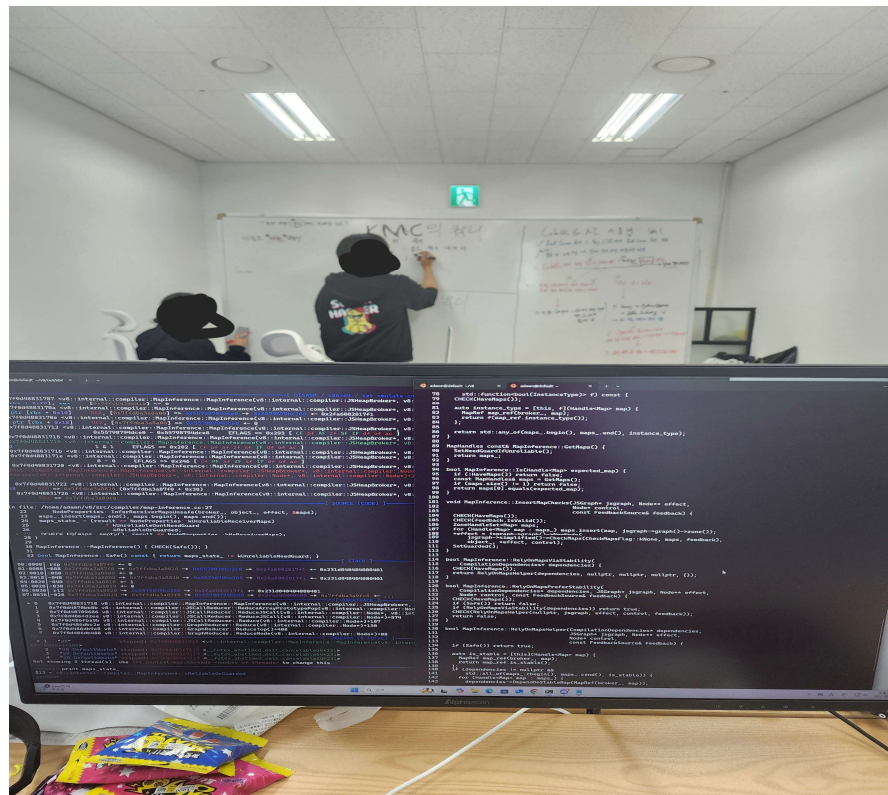
트랙 교육



나를 만든 경험들 - BOB



프로젝트



© Hackingcamp. All Rights Reserved



POC SECURITY

나를 만든 경험들 - BOB



프로젝트

(단위: transitions/exec)

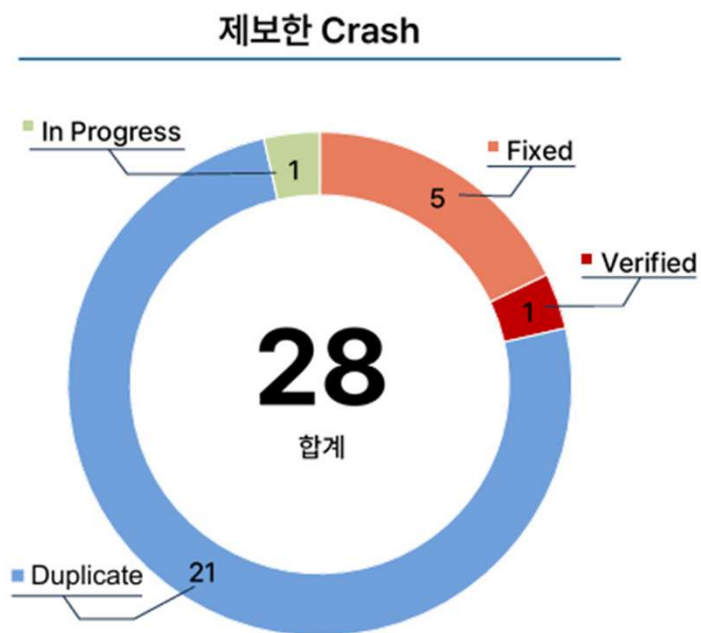
상태 전이 종류	기본 Fuzzilli		상태 전이 Fuzzilli		Mutator + 상태전이 Fuzzilli
Elements Transition	1.61	<	3.17	<	4.54
IC Transition	12.81	<	16.31	<	24.18
Normalization	25.54	<	27.72	<	29.16
Garbage Collection	1.73	<	2.98	>	2.61
Deopt	0.09	=	0.09	=	0.09
Generalization	2.00	<	4.42	>	4.11
Migrate	0.03	=	0.03	=	0.03

▶ 기본 Fuzzilli와 개선한 두 Fuzzilli에 대한 상태 전이 빈도 비교 검증

나를 만든 경험들 - BOB



프로젝트

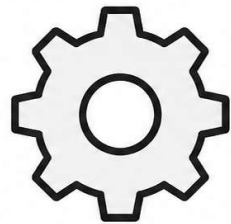


나를 만든 경험들



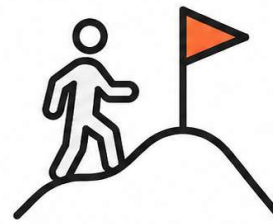
PM?

기술



VS

경험



그 이후



취직 그리고 새로운 시작

EQST

Experts, Qualified Security Team

대학 선배가 이별하고 프로그래밍 언어
5개 마스터 했어

화이팅

오늘 오후 11:04

ㅋㅋㅋㅋㅋㅋㅋㅋㅋㅋㅋㅋ

감사합니다..정말

저도 그래야겠어요



그 이후



Webkit CVE-2026-43658

googleprojectzero/**fuzzilli**

A JavaScript Engine Fuzzer



73
Contributors

62
Issues

2k
Stars

366
Forks



© Hackingcamp. All Rights Reserved



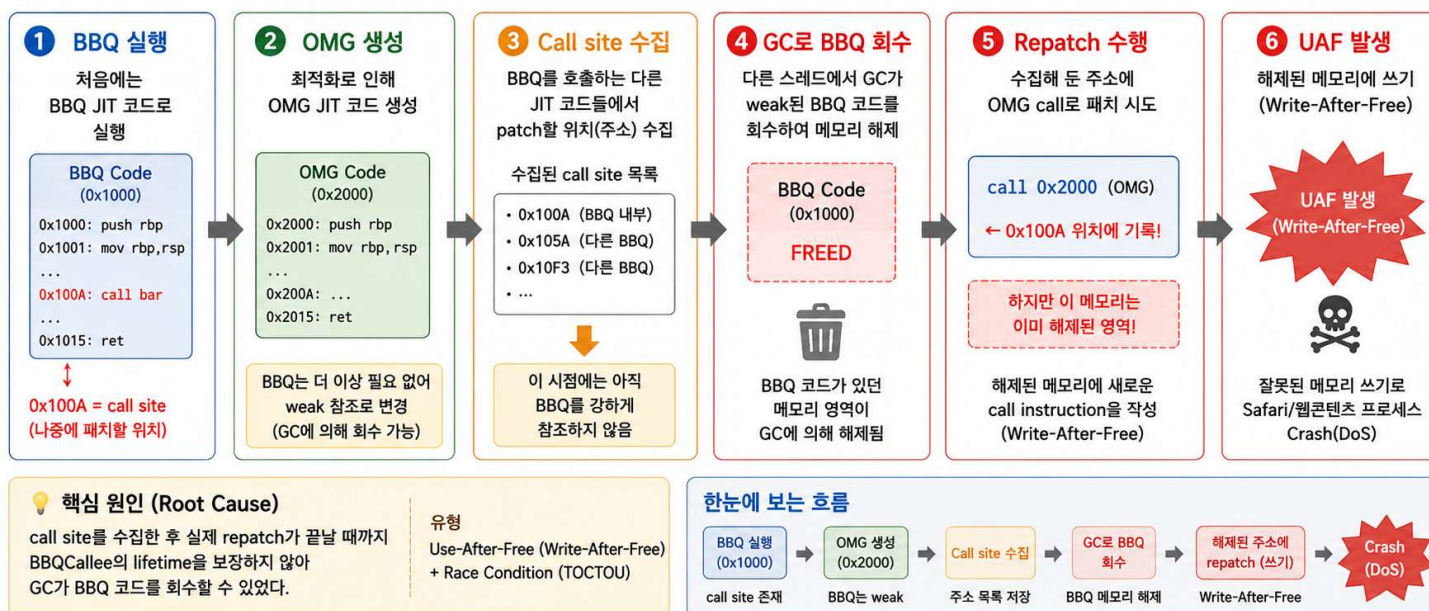
그 이후



Webkit CVE-2026-43658

CVE-2026-43658 (WebKit / JSC) — 흐름 요약

BBQ JIT 코드의 call site를 OMG로 패치하는 과정에서, 이미 GC에 의해 해제된 BBQ 코드 메모리에 쓰기(Write-After-Free)가 발생



그 이후



Webkit CVE-2026-43658

WebKit

Available for: macOS Sonoma and macOS Sequoia

Impact: Processing maliciously crafted web content may lead to an unexpected Safari crash

Description: The issue was addressed with improved memory handling.

WebKit Bugzilla: 307669

CVE-2026-43658: Do Young Park



그 이후



퀴즈

방금 설명했던 취약점(CVE-2026-43658 webkit)의 취약점 유형은 무엇일까요?

그 이후



퀴즈

정답 : UAF(use-after-free)

그 이후



V8 CTF?

v8CTF Rules

The v8CTF is a part of the [Google VRP](#) in which we reward successful exploitation attempts against a V8 version running on our infrastructure. This program is orthogonal to the [Chrome VRP](#), if you find a bug and exploit it, you can submit the bug to the Chrome VRP and use the exploit for the v8CTF.

In the following, we will differentiate between 0-day and n-day exploits. If the bug that led to the initial memory corruption was found by you, i.e. reported from the same email address as used in the v8CTF submission, we will consider the exploit a 0-day submission. All other exploits are considered n-day submissions.

Rules

The following rules apply to the eligibility of exploits:

- Your exploit needs to exfiltrate the flag from our v8CTF infrastructure.
- Only the first submission for a given bug that leads to the initial memory corruption is eligible.
- Only the first submission per deployed V8 version in v8CTF is eligible based on the timestamp of the form submission.
 - 0-day submissions are exempt from this limit.
- N-day submissions will only be accepted after the officially announced time, based on the timestamp embedded in the flag. Flags are updated automatically every hour on the hour.
- Exploits need to be reasonably fast and stable. We accept submissions with an average runtime of less than 5 minutes and at least 80% success rate.
- Valid submissions get a reward of \$10,000.

그 이후



V8 CTF?

Stable	151.0.7922.137	Beta	152.0.7977.42	Dev	153.0.8003.0	Canary	153.0.8006.0
151	151.0.7922.137 (100%) 1654411 @ Aug 12 2026 ⓘ	152	152.0.7977.42 (100%) 1669021 @ Aug 13 2026 ⓘ	153	153.0.8003.0 (100%) 1677660 @ Aug 14 2026 ⓘ	153	153.0.8006.0 (100%) 1678646 @ Aug 14 2026 ⓘ
151	151.0.7922.108 1654411 @ Aug 7 2026 ⓘ	152	152.0.7977.30 1669021 @ Aug 6 2026 ⓘ	153	153.0.7993.0 1674545 @ Aug 8 2026 ⓘ	153	153.0.8005.0 1678416 @ Aug 13 2026 ⓘ
151	151.0.7922.75 1654411 @ Aug 5 2026 ⓘ	152	152.0.7977.13 1669021 @ Aug 4 2026 ⓘ	153	153.0.7979.3 1670115 @ Aug 1 2026 ⓘ	153	153.0.8004.0 1677852 @ Aug 13 2026 ⓘ
151	151.0.7922.71 1654411 @ Jul 30 2026 ⓘ	152	152.0.7977.8 1669021 @ Jul 30 2026 ⓘ	152	152.0.7967.2 1666631 @ Jul 24 2026 ⓘ	153	153.0.8003.0 1677660 @ Aug 12 2026 ⓘ
150	150.0.7871.186 1639810 @ Jul 24 2026 ⓘ	151	151.0.7922.47 1654411 @ Jul 23 2026 ⓘ	152	152.0.7953.3 1662965 @ Jul 18 2026 ⓘ	153	153.0.8002.0 1677104 @ Aug 12 2026 ⓘ
150	150.0.7871.181 1639810 @ Jul 22 2026 ⓘ	151	151.0.7922.34 1654411 @ Jul 16 2026 ⓘ	152	152.0.7939.5 1658650 @ Jul 14 2026 ⓘ	153	153.0.8001.0 1676824 @ Aug 11 2026 ⓘ
Load more...		Load more...		Load more...		Load more...	

그 이후



V8 CTF rules

목표: V8 취약점을 이용해 실제 v8CTF 서버의 flag를 탈취

중복 제한: 같은 취약점은 가장 먼저 제출한 사람만 인정

버전당 1건: 각 V8 배포 버전에서는 기본적으로 첫 제출만 인정

단, 0-day는 예외

N-day 제한: 이미 공개된 취약점은 주최 측이 정한 공개 시점 이후에만 제출 가능

안정성: 평균 5분 이내, 성공률 80% 이상

보상: 유효한 제출 1건당 \$10,000

그 이후



V8 CTF 룰



tsuro 2026-07-01 오후 4:48

M150 is running. N-day submissions will be valid from Friday the 3rd at 14:00 GMT+0 (check the rules for details). We also took down M149 since it was already claimed.

2026년 8월 6일



tsuro 2026-08-06 오후 6:07

M151 is running. N-day submissions will be valid from Friday the 7th at 14:00 GMT+0 (check the rules for details). We also took down M150 since it was already claimed.



그 이후



퀴즈

V8 CTF에서 n-day를 이용한 submission은 버전(마일스톤)당 몇 번 인정될까요?

그 이후



퀴즈

정답 : 1회(최초)

그 이후



V8 CTF - M148

전체 공격 체인 한눈에 보기

앞 4단계는 취약점, 뒤 4단계는 익스플로잇 체인

① 취약점 (Root Cause)



② 익스플로잇 체인



그 이후



V8 CTF - M148

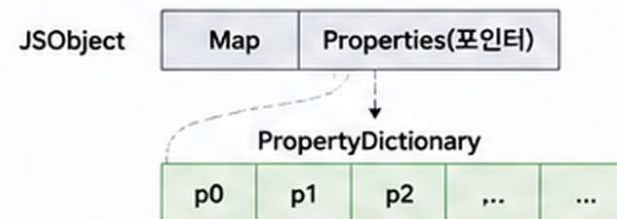
1 객체 저장 방식이 fast에서 slow로 변경

정상 동작

fast mode (in-object properties)



slow mode (properties in dictionary)



그 이후



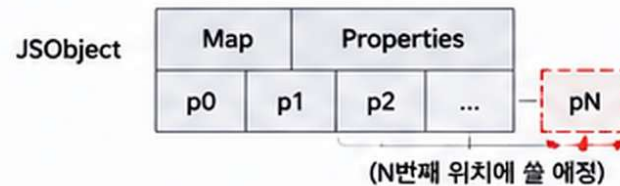
V8 CTF - M148

2 프로퍼티 추가 중에 위치를 미리 계산

```
obj.newProp = value; // 새 프로퍼티 추가
```

V8 내부 동작 (취약한 경로)

- 1) fast mode라고 가정하고
새 프로퍼티를 쓸 위치 계산



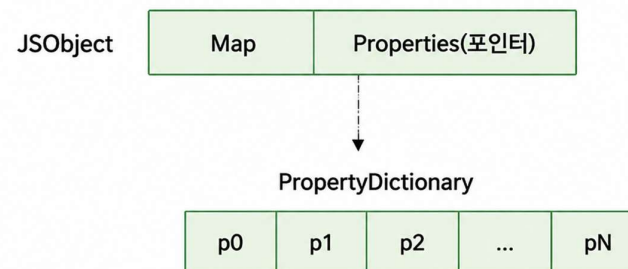
그 이후



V8 CTF - M148

3 중간에 객체가 slow mode로 전환되지만...

2) 프로퍼티 추가 과정에서
slow mode로 전환!



하지만 취약한 코드에서는
이미 계산해둔 위치(N번째)를 버리지 않음



그 이후



V8 CTF - M148

4 예전 위치에 그대로 쓰기 → OOB Write 발생

3) 예전에 계산한 N번째 위치에 그대로 Write!



그 이후



V8 CTF - M148

5 인접한 double array의 메타데이터 손상

메모리 배치 (예시)



double array 구조

elements (데이터 시작 주소)	0xAAAAAAAA0
length (배열 길이)	0x00000010 (16)

↓
OOB Write가 이 영역을 덮음!



그 이후



V8 CTF - M148

6 fake 배열을 이용해 V8 샌드박스 내부 메모리 Read/Write 획득

손상 후 double array

elements (데이터 시작 주소)	0x12345678 (임의 주소)
length (배열 길이)	0x7FFFFFFF (매우 큼)

↓

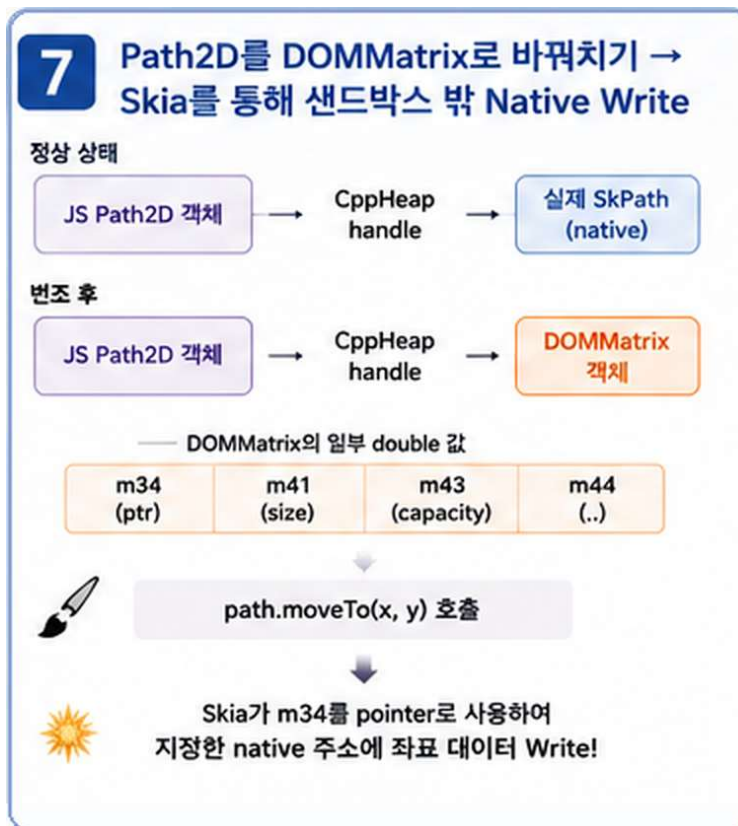
fake Uint8Array/double array로 사용

0	1	2	3	4	5	6	...
---	---	---	---	---	---	---	-----

그 이후



V8 CTF - M148



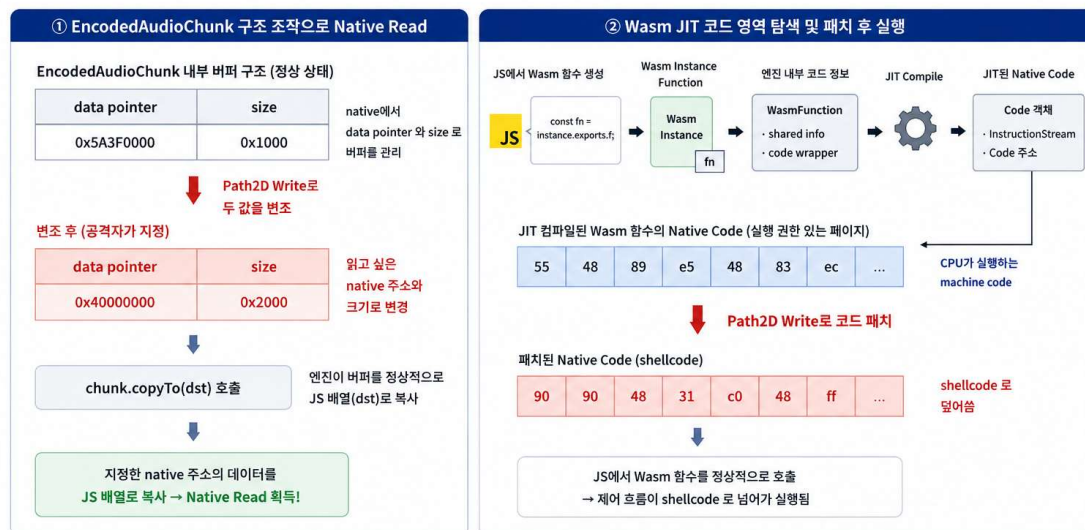
그 이후



V8 CTF - M148

8 EncodedAudioChunk로 Native Read, Wasm 코드 패치 후 셸코드 실행

읽기와 쓰기 원시를 조합해 Wasm 함수의 JIT 코드 영역을 찾아 덮어쓰고, 함수를 호출하여 셸코드를 실행합니다.



🎯 렌더러 프로세스 내 임의 코드 실행 (RCE) 성립

그 이후



V8 CTF - M148

sp...@google.com <sp...@google.com> #7

May 11, 2026 05:55PM

NOTE: This is an automatically generated email

Hello,

The v8CTF program panel has decided to issue a reward of **\$10000.00** for your report. Congratulations!

Important: This payment will be issued by Bugcrowd. You will receive an email from Bugcrowd in the next 24 hours which contains a submission you must claim to be rewarded.

If you do not receive an email from them, please check your spam folder and then reach out to us via a comment here. For issues related to Bugcrowd itself, please contact them via <https://bugcrowd.com/support>.

Regards,
Google Security Bot

P.S. Three other things we'd like to mention:

- Issuing a reward does not necessarily mean the issue is/will be fixed. Check this issue's status or reach out to us to understand if the issue has been fixed or not.
- If you'd like us to add your name to our Leaderboard at <https://bughunters.google.com/leaderboard>, please create a profile at <https://bughunters.google.com> if you haven't already done so.
- We encourage you to sign up for our Vulnerability Research Grants program at <https://www.google.com/about/appsecurity/research-grants/>, where we issue monetary payments to VRP researchers, even when no vulnerabilities are found.

How did we do? Please fill out a [short anonymous survey](#).

그 이후



Midnight Sun CTF Finals



© Hackingcamp. All Rights Reserved



그 이후



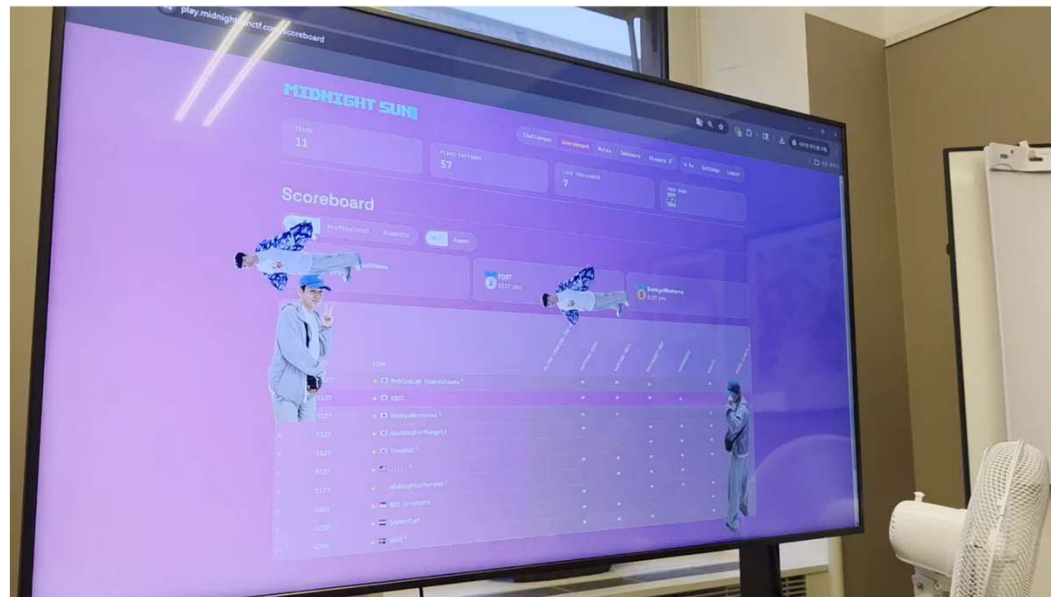
Midnight Sun CTF Finals



그 이후



Midnight Sun CTF Finals



© Hackingcamp. All Rights Reserved



POC SECURITY

그 이후



Midnight Sun CTF Finals



© Hackingcamp. All Rights Reserved

그 이후



Midnight Sun CTF Finals



그 이후



Midnight Sun CTF Finals

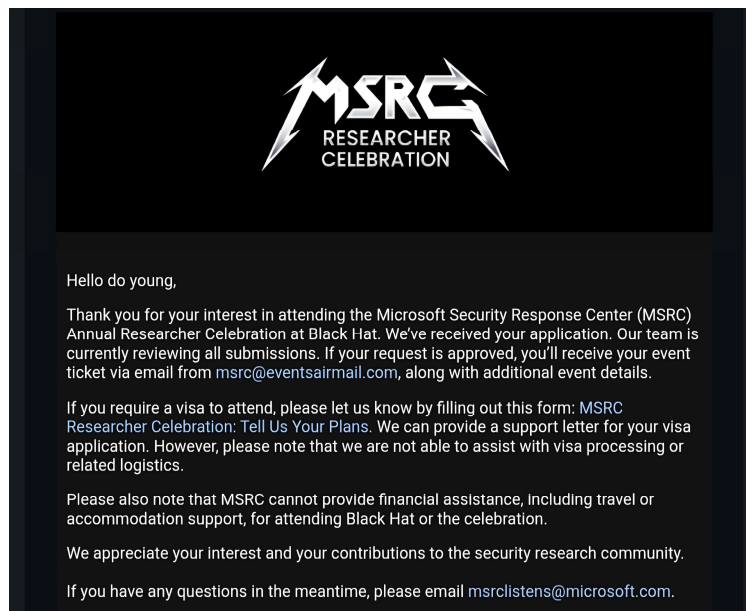


© Hackingcamp. All Rights Reserved

그 이후 - 현재



MSRC researcher celebration



그 이후 - 현재



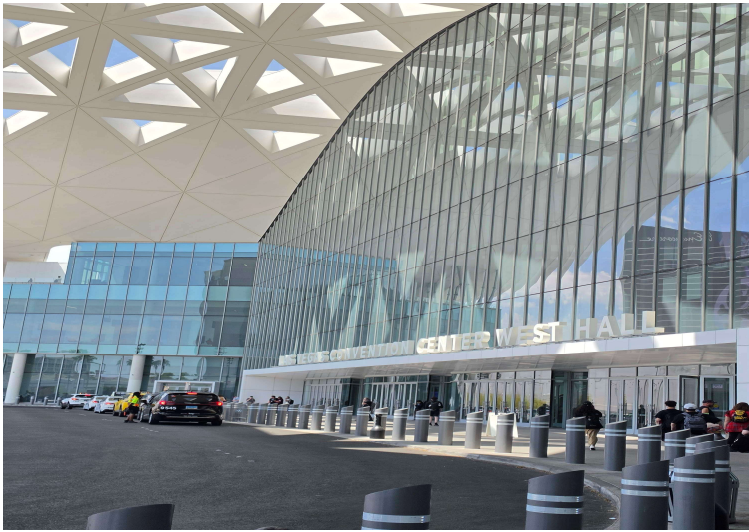
MSRC researcher celebration



그 이후 - 현재



Defcon CTF 2026



그 이후 - 현재



Defcon CTF 2026



© Hackingcamp. All Rights Reserved

그 이후



앞으로의 목표

1. AI 하네스를 통한 취약점 찾기 자동화 연구
2. 브라우저 및 모바일 공부
3. 경제적 자유 달성 후 카페 창업

감사합니다.

Discord : @a_dawn0106



LinkedIn

