

한글 안전하게 사용하는 방법

오지호

CONTENTS

목차

- 1 CVE란?
- 2 소개할 CVE
- 3 원리(어떻게 터지는지)
- 4 관련 문제 풀이
- 5 결론
- 6 소감



CVE란?

이미 공개된 소프트웨어·하드웨어 보안 취약점
에 번호 붙여서 관리하는 것



소개할 CVE



CVE-2017-8291





어떻게
터지나요?



어떻게
터지나요?



→ **EPS파일**
PostScript 코드

어떻게
터지나요?



→ **Ghostscript**
인터프린터

어떻게
터지나요?



검사



어떻게
터지나요?



검사중...(설정값 검사스킵)



검사



ghostscript®



MONTHLY REVIEW



어떻게
터지나요?



미아...



```
-sFONTPATH="/usr/share/fonts:/home/user/fonts"
```



MONTHLY REVIEW



어떻게
터지나요?



미안...



```
-sFONTPATH="/usr/share/fonts:/home/user/fonts"
```



```
-sFONTPATH="%pipe%<command>"
```

음 관참구만



어떻게
터지나요?



어떻게
터지나요?



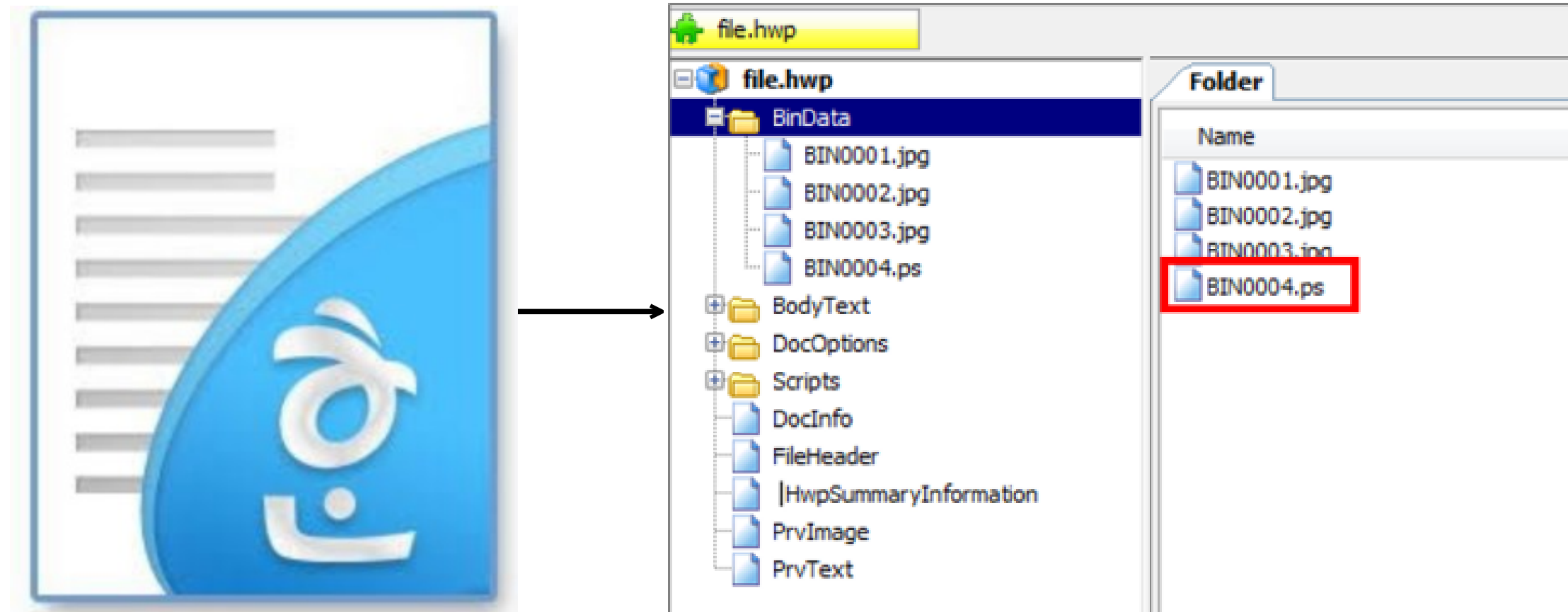


어떻게
터지나요?



어떻게 터지나요?

EPS 파일이 삽입되었을 때 파일 구조





관련 문제 풀이



관련 문제 풀이

5 LEVEL 5

DreamHWP1 

reversing

👁 703 📄 70 📅 2022.11.06. 23:01:48

📄 문제 파일 받기



관련 문제 풀이

85400945-0095-450c-ad19-a23153b8f72d (1).zip - 반디집 (스탠더드)					— □ ×	
파일(F) 편집(E) 찾기(I) 설정(S) 보기(V) 도구(T) 도움말(A)						
	▼		▼			
열기		풀기		새로 압축	파일 추가	파일 삭제
ZIP 85400945-0095-450c-ad19-a2						
					칼럼 설정	코드페이지
이름					압축 크기	원본 크기
Problem.hwp					53,543	58,880
						파일 종류
						한컴오피스 한글 문



관련 문제 풀이

 Problem.hwp	Folder	
 BinData		
 BIN0001.eps		
 BodyText		
 Section0		
 DocOptions		
 _LinkDoc		
 Scripts		
 DocInfo		
 FileHeader		
 HwpSummaryInformation		
 PrvImage		
 PrvText		
Name		Size [B]
 BIN0001.eps		

관련 문제 풀이

```
$ python3 solve.py Problem.hwp dump  
BinData stream: 1  
BIN0001.eps -> raw_deflate success, Signature: b'!PS-Adobe-3.0 EPSF-3.0\r\n%%Creat'  
$
```

관련 문제 풀이

✓ dump

≡ BIN0001.eps_decompressed.bin

≡ BIN0001.eps.bin

≡ Problem.hwp

🔗 solve.py

1



관련 문제 풀이

```
%AI6_EndPatternLayer
) &
(0 0 0 R 0 0 0 0 k
| 0 0 0 0 K
) @
(
%AI6_BeginPatternLayer
0 J 0 j 0.3 w 4 M []0 d
0 XR
16.9673 33.79 m
10.0083 40.749 L
10.0054 50.6084 L
16.9663 57.5693 L
26.8257 57.5703 L
33.7876 50.6113 L
33.7876 40.752 L
26.8296 33.791 L
16.9673 33.79 L
f
```

관련 문제 풀이

7083 f

7084 330.5332 385.7715 m

7085 313.0146 385.7715 L

7086 311.6318 385.7715 L

7087 307.1416 393.9707 L

7088 300.6216 409.1504 298.3398 386.7412 309.7139 387.9502 C

7089 292.9609 385.7715 L

7090 275.8154 385.7695 L

7091 274.2012 385.7695 L

7092 272.9121 439.0322 L

7093 300.2959 442.0273 L

7094 309.2617 442.0273 L

7095 321.9756 434.7212 313.5801 440.7285 317.4121 437.9683 C

7096 323.5244 419.6226 323.3613 430.3374 323.4434 425.7104 C

7097 315.9453 412.2354 319.7754 414.8325 314.4775 412.8032 C

7098 330.5332 385.7715 L

7099 F

7100 *U

7101 0.0196 0.8353 0.6902 0 k

7102 0 R

7103 0 0 0 0 K

7104 1.215 w 3.864 M

7105 0 XR

7106 253.4238 412.0024 m

7107 255.2646 410.7026 L

7108 254.3848 409.2495 254.123 407.9653 254.3633 406.8403 C

7109 255.7793 400.2036 275.1543 397.3335 299.8906 402.5703 C

7110 324.627 407.8076 341.1543 418.2783 339.7383 424.9155 C

7111 f

%AI6_EndPatternLayer

) &

(0 0 0 R 0 0 0 0 k

0 0 K

.ternLayer

w 4 M []0 d

3.79 m

40.749 L

4 50.6084 L

63 57.5693 L

257 57.5703 L

7876 50.6113 L

.7876 40.752 L

26.8296 33.791 L

16.9673 33.79 L

f



관련 문제 풀이

7083 f
7084 330.5332 385.7715 m
7085 313.0146 385.7715 L
7086 311.6318 385.7715 L
7087 307.1416 393.9707 L
7088 300.6216 409.1504 298.3398 386.7412 309.7139 387.9502 C
7089 292.9609 385.7715 L
7090 275.8154 385.7695 L
7091 274.2012 385.7715 L
7092 272.9121 439.0322 L
7093 300.2959 440.6855 274.2568 442.0234 387.1416 272.9141 388.7598 C
7094 309.2617 442.0273 L
7095 321.9756 434.7212 323.3613 430.3374 323.4434 425.7104 C
7096 323.5244 419.6226 319.7754 414.8325 314.4775 412.8032 C
7097 315.9453 412.2354 318.5527 411.1792 323.1172 401.5195 C
7098 330.5332 385.7715 L
7099 F
7100 *U
7101 0.0196 0.8353 0.6902 0 k
7102 0 R
7103 0 0 0 0 K
7104 1.215 w 3.864 M
7105 0 XR
7106 253.4238 412.0024 m
7107 255.2646 410.7026 L
7108 254.3848 409.2495 254.123 407.9653 254.3633 406.8403 C
7109 255.7793 400.2036 275.1543 397.3335 299.8906 402.5703 C
7110 324.627 407.8076 341.1543 418.2783 339.7383 424.9155 C
7111

```
%AI6_EndPatternLayer
) &
(0 0 0 R 0 0 0 0 k
0 0 0 K

ternLayer
w 4 M []0 d

3.79 m
40.749 L
4 50.6084 L
63 57.5693 L
257 57.5703 L
7876 50.6113 L
.7876 40.752 L
46.8296 33.791 L
16.9673 33.79 L
f
```

7004 298.71 347.6836 L
7005 f
7006 *u
7007 306.7617 349.5 m
7008 306.7617 346.6631 306.0684 345.4473 304.9678 345.4473 C
7009 304.5664 345.4473 303.9702 345.6875 303.5811 346.7529 C
7010 303.3438 347.4141 303.2524 348.2842 303.2402 349.3652 C
7011 303.2402 356.5107 L
7012 304.1709 349.5156 L
7013 304.1709 348.0146 L
7014 305.5757 347.3535 304.5239 347.3535 304.9497 347.3535 C
7015 305.8315 356.5107 L
7016 306.7617 356.5107 L
7017 306.7617 349.5 L
7018 f
7019 *u
7020 311.8867 345.7324 m
7021 310.9492 345.7324 L
7022 309.5918 354.6045 L
7023 309.5918 356.5107 L
7024 313.2432 356.5107 L
7025 313.2432 354.6045 L
7026 311.8867 345.7324 L
7027 311.8867 345.7324 L
7028 f
7029 *u
7030 311.8867 345.7324 m
7031 310.9492 345.7324 L



관련 문제 풀이

```
/Rrrr <
0632e7cb1d9f2067fda9197f289976cc0632e4cb75982340c99d3e266c98758a09448fd80c81734ed49d767f289976cc0632e2cb1d896253c98e267f289976cc0632e3cb1c896744ddcf70067adc21da0a5ae6db0ccd66479
| def%i1ohihfishihf7
0 1 Rrrr length 1 sub %
%i1ohihfishihf7
[ /Y20 %
exch
| def%i1ohihfishihf7
Rrrr dup Y20 get <296bd6eb2ca90321bbef5f5f4cfc10ec>%gggg
Y20 15 and get xor Y20 exch put%
] for %
Rrrr cvx %
%
%
exec
%%EOF
```

관련 문제 풀이

복호화

```
1  /flag <
2  9ae5bb9689fd9f9ba6ddacb1b7d99f9d88e89fecee9cf781e69ff9efff8cb
3  >%def
4  0 1 flag length 1 sub {
5    /key exch def
6    flag dup key get <deadcode>%ggggg
7    key 3 and get xor key exch put%
8  } for
9  flag cvx
10 print
```

관련 문제 풀이

```
xor_bytes = bytes.fromhex("dead0de")
flag_bytes = bytes.fromhex("9ae5bb9689fd9f9ba6ddacb1b7d99f9d88e89fecee9cf781e69ff9efff8cb")

res = bytes(b ^ xor_bytes[i & 3] for i, b in enumerate(flag_bytes))
print(res.decode("utf-8", errors="replace"))
```

DH{  }



관련 문제 풀이

축하합니다!

5 LEVEL 5 DreamHWP1
문제를 해결했습니다.

다른 사용자들을 위해 이 문제의 난이도를 평가해주세요.
적극적인 피드백은 드림핵에게 큰 도움이 됩니다.
자신의 위게임 점수에 따라 투표 불가능한 난이도가 있을 수 있습니다.



− 5 +

학습한 배경 지식을 기반으로 하는 응용 능력이 필요합니다.



괜찮아요

🗳 투표하기



결론

최신버전 사용하기
안전하게 eps파일 사용인지 확인



MONTHLY REVIEW



소감



MONTHLY REVIEW



Q&A

들어주셔서 감사합니다.

THANK YOU.