Waiting for Worm

(RPC 웜의 이해 및 파급효과) Ver.0.1

2003.8.12

작성자: 전 상훈(바다란)
(winsnort@hotmail.com)
(winsnort@securityindepth.net)

Waiting for Worm

1. Details

MS Windows 계열에서의 치명적인 취약점이 지난 7월 발견 되었다. 대상은 RPC Locator 서비스로서 Windows XP, 2000, NT 계열에 활성화 되어 있는 것으로서 간략히 설명하면 RPC Locator 서비스는 위치를 찾는 용도로 이용이 된다. MS 제품의 구성에서 핵심적인 구성요소는 OLE 로서 Object Linking & Embedding 을 기반으로 이루어 져있다. 이 내용은 간단하게 웹에서 워드 파일을 불러오고 익스플러러 내에서 Excel 파일을 보고 편집하고 또 워드 파일을 보고 편집하고 하는 기능을 말한다. 좁게 말하면 Copy & Paste 기능에서부터 파일의 호출과 수정 , 편집을 가능케 하는 기술이라고 할 수 있다. RPC Locator 서비스는 135번 Port를 이용하며 항상 Ready 상태로 대기하고 특정 요구가 올 때마다 그 요구 문자열을 파싱하여 해당하는 서비스와 연결시켜 주는 중개 역할을 하는데 이 요구 문자열을 파싱하여 스택에 쌓아 둘 때 문자열의 길이가 함수의 제한보다 크게 될 경우 스택 오버런을 일으키게 되고 이 오버런이 일어나 Return 되는 주소에 실행 코드를 넣음으로써 문제를 일으키게 된다.

```
HRESULT CoGetInstanceFromFile(
 COSERVERINFO * pServerInfo,
 CLSID * pclsid,
 IUnknown * punkOuter,
 DWORD dwClsCtx,
 DWORD grfMode,
 OLECHAR * szName,
 ULONG cmq,
 MULTI_QI * rgmqResults
);
```

함수에서 szName 인자를 처리 하는 것은 GetPathForServer와 GetMachineName 함수에서 처리를 하게 되는데 여기에서 문제가 발생하는 곳은 두 곳으로서 RPC Locator 서비스내에서의 GetPathForServer 함수에 할당된 영역공간 0x20 사이즈를 넘는 사이즈의 문자열을 쿼리함으로써 일어나는 버퍼 오버런과 CoGetInstanceFromFile 함수자체의 충족조건을 충족 시키지 못하는 것으로 인해 일어나는 오류 혹은 Com 구조의 붕괴가 일어날 수 있다.

Waiting for Worm

\\servername\c$\12345611111111111111111111111111.doc
CoGetInstanceFromFile 함수의 6번째 인자인 szName의 요구조건을 충족시켜서 CoGetInstanceFromFile 함수가 리턴값을 반드시 가져야 하나 (즉 Null 이 될 수 없슴) 가지지 못함으로 인해 문제가 발생하고 있다.

hr = CoGetInstanceFromFile(pServerInfo, NULL, 0, CLSCTX_REMOTE_SERVER, STGM_READWRITE, L"C:\\12345611111111111111111111111111.doc",1,&qi);
이와 같은 함수호출에서 존재하지 않는 파일을 호출할 경우 생성을 통해 IpersistFile::Load Interface에 연결점(Interface)를 돌려 주어야 하나 이 과정이 인자의 스트링 길이제한으로 비정상 종료 됨으로 인해 정상적인 Interface를 돌려 주지 못하고 있다.

이 부분이 RPC/DCOM 문제의 전체 개요이다. 즉 문제는 버퍼오버런에 의한 Remote Shell연결 혹은 시스템 권한 획득의 문제에 국한되지 않는 다는 것이다.

좀 더 부연하면 IpersistFile::Load 인터페이스 호출 루틴이 궁극적으로 실패함으로써 File의 각 연결지점(Interface)을 호출하는 루틴인 QueryInterface 인터페이스 함수 루틴 콜 자체가 실패하게 되었고 연결지점 저장정보를 가지고 있는 Imoniker 서비스 자체가 무너지게 되는 것으로 보인다.

간단하게 워드 파일내에 PowerPoint 슬라이드가 삽입되어 있는 경우 워드 파일내에서 슬라이드 화면을 클릭하면 Word Program 내에서 Power Point 슬라이드를 수정하고 변경할 수 있는 상태가 된다. 또 워드내에 포함되어 있는 Excel 파일의 경우도 마찬가지이다. 이런 경우 클릭을 하였을 경우에 각 부분이 어느 실행파일과 연결이 되고 또 어떤 기능들을 가지고 활성화가 되어야 되는지에 대한 구성을 가지고 있고 실행하는 것이 OLE 이고 여기서 더 나아가 COM 과 DCOM 이 된다. DCOM 은 원격개체에 대해 OLE와 비슷한 형태로 호출이 가능한 루틴이 된다. 웹상에서 워드 파일을 클릭하거나 아니면 원격 저장소에 위치한 문서의 링크를 클릭할 때 호출해주는 기능들을 가진 편리하고 뛰어난 기능이다. 그만큼 복잡하고 아는 사람이 적은 것이고....

이 부분은 상세하게 차후에 정리해 보도록 하자.

2. 파급효과

현단계의 웜이나 공격루틴은 초보적인 형태를 나타낼 수 밖에 없다. 즉 공격코드의 부분적인 수정과 변형을 통해 나타날 수 있는 바이러스와 간략한 해킹의 형태로 나타날 수 있는데 차후에 좀 더 복잡하고 잡기도 어렵고 막기도 어려운 형태의 웜으로 진화가 가능할 것이다. 아마 Microsoft가 가장 애먹을 분야는 COM 분야에서의 붕괴과정을 막는 것과 COM과 DCOM 에서 사용하는 Interface에 대한 직접적인 공격루틴이 발생할 경우일 것이다. 쉽게 해답을 찾기 힘들 것으로 예측한다.

현재 파급효과는 직접적인 135 포트에 대한 공격을 통해 권한 획득한 후 타 시스템으로의 공격을 위해 다른 공격코드를 다운 받거나 Remote Shell 을 특정 포트에 열어 주는 초기적인 단계의 변화로 볼 수 있다.

이 공격의 여파로 인해 시스템 권한을 빼앗기고 또한 원격에서 새로운 공격 도구가 침입 할 수 통로를 제공할 수 있다. 개인 사용자가 사용하는 PC나 서버군에서 이용하는 OLE와 DCOM을 활용하는 제품들(Office 와 그 외 OLE를 지원하는 모든 제품)에 지장을 받을 수 있다. 최소한 Copy & Paste 가 되지 않는 피해에서부터 정상적인 파일의 호출이 되지 않는 것과 기업 내부의 인트라넷에서는 인트라넷 상에서의 파일 호출루틴이 실패할 수 있을 것이다.

MS 측에서 DCOM을 사용하는 프로그램이 다음과 같다고 했다.

- Microsoft Access Workflow Designer
- FrontPage with Visual Source Safe on IIS
- BizTalk Server schedule client
- Excel uses DCOM if it includes an RTD statement
- SMS uses DCOM to get the hardware inventory off a client
- Win95 needs Client for Microsoft Networks or DCOM to work with MS SNA Server

그러나 본인은 위의 공격 영역은 DCOM (Remote) 영역이 아닌 이미

Waiting for Worm

Com (Local) 영역의 Interface 구현 부분을 파괴하고 있으므로 대다수 OLE와 COM을 이용하는 프로그램에 영향이 미칠 것으로 판단한다. 즉 RPCSS.EXE 파일에만 영향을 미치는 것이 아니라 부팅이 된 후에 Windows OS 위에서 이루어져 있는 Interface 구조가 통째로 흔들릴 수 있다는 것이다. 물론 리부팅하면 다시 구조는 복구된다.

거의 대부분의 Windows base 위에 올라가는 Editor 및 Office 프로그램이 크게는 파일 생성 오류 , 파일 호출 실패 , 비정상 종료를 경험할 수 있고 작게는 ClipBoard (Copy와 Paste를 위한 영역)를 이용하는 기능이 작동하지 않을 것이다. 이 말은 대부분의 프로그램이 영향을 받을 수 있다는 것이고 또한 Notes 혹은 타 Application 기반위에 이루어진 인트라넷 혹은 메일 시스템에서의 파일첨부 및 호출 루틴이 실패하고 원격 저장소에 저장된 파일을 호출하는 루틴이 연결되지 않을 것이다.

위험 OS:
직접적인 공격 대상: Windows NT 계열, 2000 , 2003 , XP 가 가능하리라 예상합니다.

간접적인 피해 대상: 인트라넷을 구성하고 OLE 기능을 구현한 메일 시스템 (주로 Notes로 많이 하더군요.) , DCOM 호출 기능을 가진 Application , MS Office (전 시리즈)… 그 외 다수.

피해여파:
1. RPC를 사용하는 루틴을 통한 시스템 권한 탈취 가능
2. MS Office 계열 사용 프로그램에 대한 문제 발생 가능성 높음
3. 일상적인 Copy & Paste 루틴의 비동작
4. 비정상 종료 가능성 존재
5. 시스템 권한 탈취에 따른 외부로 부터의 추가 공격 가능성

3. 앞으로 발전 방향 과 주의

분명히 말하지만 현재의 취약성을 이용한 공격은 이제 시작이다. 웜은 아직 나오지 않았다. 직접 공격을 통해 tftp 포트를 통한 공격파일 다운로드 혹은 특정 포트를 열어서 시스템 권한을 통한 제어가 가능하게 하는 것 이것이 끝은 아니란 이야기다. 그럼 앞으로의 발전 방향은 어떻게 될 것인가?

아직 회사나 ISP , 대형 통신회사, 기업체들에는 영향이 없을 것이다. 왜냐?.. 당연히 라우터와 방화벽에서 135 Port에 대한 것을 Blocking 하거나 Filtering 하기 때문에 당연히 공격이 들어 올 수 없다. 그러므로 상대적으로 안심하고 있을 것이다. 그럼 앞으로의 변화는 어떻게 될 것인가?. 본인의 예상으로는 복잡한 형태의 공격으로 변화 하리라 쉽게 예상한다.

Web(80) 포트에 대한 취약성 공격 -> Web Server 내에서 내부망 혹은 주위의 서버로 80번에 대한 공격과 135번에 대한 공격을 순차적 혹은 무차별 적으로 공격하는 루틴 실행 -> 135번으로 감염 시 80번과 135번에 대한 복합적인 공격루틴 실행.

즉 RPC 취약점외에 다른 공격루틴이 첨가 될 것이고 이 루틴은 80번 포트를 이용할 때 가장 큰 피해를 입힐 수 있을 것이다. 그렇다면 어느 운영체제를 택하여 80번 포트의 취약점을 공격할 것인가?.. 이번에도 MS 제품을 이용할 수도 있고 그렇지 않을 수도 있다. 그러나 공교롭게도 올해 들어 발견된 취약점과 공격 코드들의 발전방향을 보았을 때 유난히도 MS 계열에 공격이 집중된 경향을 개인적인 관찰로 느낄 수 있었다. 특히 Webdav 취약성과 Printer 확장자에 대한 공격, htw 확장자에 대한 공격이 새로이 업그레이드 되었을 가능성을 강하게 언급하고 싶다.

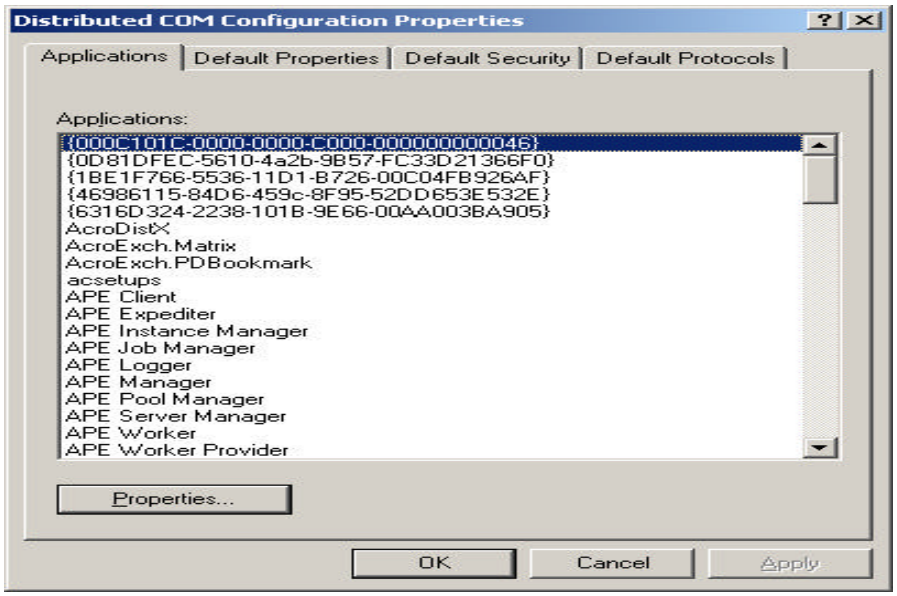
최근 zone-h.org 사이트의 deface 사이트 통계치를 보게되면 예전에 해킹을 당하지 않던 (즉 안전한 설정을 했으리라고 여기던) 사이트 들이 크래킹을 당하는 것을 자주 볼 수 있으며 그 발생 비율과 몇몇 사례를 조사해 보았을 때 WebDav 취약성 공격이 사용되었음을 알 수 있었다. 7월중에 일어난 일들이므로 한층 강화된 공격이 나왔음을 제시한다. 또 국내의 대다수 IIS 웹서버를 운영하는 웹사이트 들은 확장자에 대한 취약성 (ISAPI) 공격에 거의 대비가 없다고 본다.

Waiting for Worm

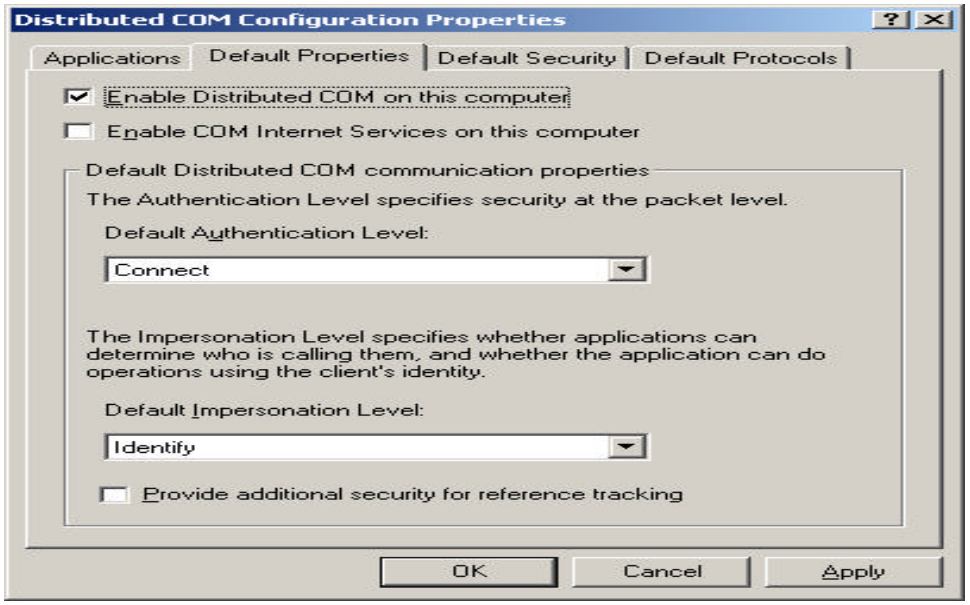
위험한 확장자로서는 idc ,.printer ,.htw ,.shtml 확장자가 있을 수 있으며 이 확장자에 대한 공격과 Webdav에 대한 공격이 가장 파괴력이 높은 웜이 될 수 있을 것으로 판단된다. 물론 다른 OS를 통해서 전파 될 수도 있으나 지속기간이나 MS 제품에 대한 보안인력이 부족한 것을 이유로 또 MS 제품에 대한 반감으로 강력하게 공격 코드가 출현할 것으로 예측한다.

4. 해결책

RPC 취약점의 해결책으로는 2000계열에서는 시작 -> 실행 -> Dcomcnfg.exe



Default Properties -> Enable DCOM On this computer의 체크를 해지하면 된다.



XP 사용자의 경우

Waiting for Worm

1. 시작 -> 실행 ->Dcomcnfg.exe
   A. 콘솔 루트 밑에 구성요소 서비스를 클릭한다.
   B. 구성요소 서비스 밑에 컴퓨터를 클릭한다.
   C. 컴퓨터 밑에 내 컴퓨터의 속성을 연다.
2. 기본 속성 탭을 선택한다.
3. 이 컴퓨터에서 DCOM사용을 uncheck한다.

패치의 경우는 다음과 같다.

Windows NT 4.0 Server
http://download.microsoft.com/download/e/0/0/e0068fdc-811d-48d8-9003-92f0efc40bb1/KORQ823980i.EXE

o Windows NT 4.0 Terminal Server Edition(영문버전)
http://download.microsoft.com/download/4/6/c/46c9c414-19ea-4268-a430-53722188d489/Q823980i.EXE

o Windows 2000
http://www.microsoft.com/downloads/details.aspx?FamilyId=C8B8A846-F541-4C15-8C9F-220354449117&displaylang=ko

o Windows XP 32 bit Edition
http://download.microsoft.com/download/e/3/1/e31b9d29-f650-4078-8a76-3e81eb4554f6/WindowsXP-KB823980-x86-KOR.exe

o Windows XP 64 bit Edition (영문버전)
http://download.microsoft.com/download/a/7/5/a75b3c8f-5df0-451b-b526-cfc7c5c67df5/WindowsXP-KB823980-ia64-ENU.exe

o Windows Server 2003 32 bit Edition
http://download.microsoft.com/download/1/3/a/13a09c68-443f-446a-b3a1-a35e545c582e/WindowsServer2003-KB823980-x86-KOR.exe

o Windows Server 2003 64 bit Edition(영문버전)
http://download.microsoft.com/download/4/0/3/403d6631-9430-4ff6-a061-9072a4c50425/WindowsServer2003-KB823980-ia64-ENU.exe

Waiting for Worm

아직 더 고려해야 될 사안이 많이 있고 현재의 패치는 인자의 버퍼오버런을 막은 형태이지만 Com까지 영향을 받는 것으로 보아 앞으로 많은 문제가 있으리라 예상 됩니다. 여러 가지 형태의 문제를 하나의 조치로 막기에는 역부족일 듯 싶네요.

ISP에서 135-139 ,445 포트를 막는다면 문제가 발생할 수 있는 소프트웨어로는 Exchange가 가장 클 수 있는데 Exchange 라는 제품 자체가 COM 기반위에 탄생하였고 이것을 확장하고 활용성을 높이기 위해 DCOM (Interface를 이용한 원격 연결)을 이용한 제품이 되었다. Exchange에서 호칭하는 CDO (Collaboration Data object) 자체가 OLE 베이스 위에 COM과 DCOM이 결합된 형태이므로 Interface를 통한 통합이 이루어 진다. 이 제품의 경우 정말 타격이 심할 수 있는데 Exchange를 사용하는 유저들은 다른 Exchange와 (특히 타 ISP 혹은 외부) 연결이 필요할 경우 장애가 발생할 수 있다. VPN이라도 연결하여 사용하고 방화벽과 라우터에서는 특정 IP외에는 접속하지 못하도록 하는 설정으로 극복하여야 할 것으로 보인다.!.. 아직 Exchange를 살펴 보지는 않았으나 문제가 발생한다면 Exchange 쪽에서 발생할 수 있는 장애가 더 많을 수도 있으리라 예측된다.

그리고 지금까지 나온 것은 껌입니다.

앞으로 나올 웜을 기다리며...

*/ 개인적으로 쓴 글입니다. 회사업무에 쫓기다 겨우 시간을 내어서 후다닥 쓰게 되었네요. 오늘 오전에 웜이 나왔다는 소리에 잠시 둘러 보았으나 아직은 아닙니다. 급히 쓰다 보니 중간중간 문맥에 맞지 않거나 오타가 있더라도 차후에 여유 있을 때 재차 보정하겠으니 양해 해주시길

*/. 현재 IIS의 Extension과 Webdav에 대한 취약성을 점검하는 스캐너는 개발완료 했습니다. 클래스 대역의 제한 없이 사용할 수 있으나 오용의 위험이.... !!.. 그리고 RPC/DCOM 스캐너도 개발은 됐으나 아직 디버깅을 더 해야 하는 상황입니다. 시간 여유가 없어서 못하고 있는데 틈나는 대로 완성되는 대로 공개하도록 하겠습니다.

질문은 winsnort@securityindepthe.net , winsnort@hotmail.com 으로..