WebDAV 취약점 분석

2003. 5. 16

전완근(wkjeon@certcc.or.kr)
류성철(ryusc@certcc.or.kr)

1. 개요

현재 해킹공격은 리눅스나 유닉스서버를 대상으로 하는 것보다 윈도우즈로 초점이 바뀌어 가고 있다. 이는 더욱 강화되어 가는 유닉스나 리눅스 서버에 비해 아직까지 많은 잠재적인 취약점을 지닌 윈도우즈 운영체제가 해킹에 많이 노출되어 있기 때문으로 보인다. 또한 www 이나 DNS는 항상 외부에 노출되어 있어 이에 대한 공격은 지속되고 있다.

최근에 윈도 2000서버에서 Web 폴더등으로 사용하고 있는 WebDAV에서 버퍼오버플로 취약점이 발견되었다. 이에 따라 본 문서에서는 WebDAV 에 대한 간략한 설명과 취약점에 관해 분석한 내용, 이에 대한 대응방법 등을 알아본다.

참고로, 이 문서는 IIS 서버를 사용하고 있는 Windows 2000 서버와 NT 4를 쓰는 기관의 시스템 관리자와 네트워크 관리자에게 필요한 내용을 담고 있으며, CERTCC-KR 에서는 추후 이 문서를 업데이트 할 예정이다.

2. WebDAV

2.1 WebDAV 개요

WebDAV는 HTTP 사양에 대한 확장 기능으로 "WebDAV"의 "DAV"는 "분산형 저술 및 버전 처리 (distributed authoring and versioning)"를 의미하며, 인가된 사용자는 원격지에서 웹 서버 상에 컨텐츠를 추가하고 관리할 수 있다.

2.2 WebDAV의 HTTP 기능보완

웹의 표준 데이터 전송 프로토콜인 HTTP 1.1(Hypertext Transfer Protocol)은 보기 용도로 작성된 정적 문서에는 잘 작동되지만, 클라이언트에게 풍부한 작성 기능을 제공할 수 있을 만큼 정교하게 문서를 처리하는 기능은 제공하지 못 한다.

이에 따라서 IETF WebDAV 작업 그룹은 표준 기반 포럼에서 현재 WebDAV 사양(IETF RFC 2518)은 공동 작성 도구의 다음 세 가지 문제를 중점적으로 다루고 있다.

① 덮어쓰기 방지

HTTP 1.1에는 클라이언트가 리소스를 보호하고 같은 시간에 동일한 리소스를 편집하고 있는 다른 클라이언트에 대한 걱정 없이 내용을 변경할 수 있는 메소드가 없다. WebDAV에서는 다양한 메소드 즉 (Lock, UnLock)등을 이용하여 리소스를 잠궈 본인이 문제의 리소스에 관심이 있음을 다른 클라이언트에게 알리거나 다른 클라이언트가 해당 리소스를 액세스하지 못하도록 한다.

② 리소스 관리

HTTP는 개별 리소스에 대한 직접 액세스만을 처리한다. 이와 달리 WebDAV는 데이터를 보다 효율적으로 구성하는 수단을 제공한다. WebDAV는 리소스를 담을 수 있는 컬렉션 개념(파일 시스템 폴더와 유사)을 도입한다. WebDAV를 통한 리소스 관리에는 컬렉션 내에 리소스나 파일 만들기, 이동, 복사, 삭제 기능 뿐만 아니라 컬렉션 자체를 만들기(Mkcol), 이동(Move), 복사(Copy), 삭제하는 기능도 포함된다.

③ 문서 속성

사람들이 사용하는 문서의 종류가 다양해짐에 따라 개별 문서의 속성을 기록한 목록도 점점 길어진다. 이에 따라 여러 속성을 관리하기 위해서 WebDAV에서 XML을 사용한다.(Propfind)
다른 종류의 데이터마다 해당 데이터를 설명하는데 도움이 되는 고유의 속성이 있다. 예를 들면, 전자 우편 메시지에는 보낸 사람의 이름과 수신 시간이 속성이 되며 통합 문서의 경우에는 원본 작성자 이름과 마지막 편집한 사람의 이름이 그 속성이 된다.

2.3 WebDAV에서 사용하는 메소드

HTTP 1.1은 클라이언트가 서버와의 통신에 사용할 수 있는 일련의 메소드를 제공하며 서버에서 요청을 한 클라이언트에게로 보내는 응답 형식을 지정한다. WebDAV는 HTTP 1.1의 메소드도 사용하고 있으며 일부 메소드는 더 확장하였고, 설명한 기능을 제공하는 다른 메소드도 추가했다. WebDAV에서 사용하는 메소드는 다음과 같다.

메소드	기능
Head, Trace	네트워크 행동을 찾고 추적하는 기능
Get	문서 검색
Put, Post	문서를 서버에 전달
Delete	리소스나 컬렉션을 삭제
Mkcol	컬렉션을 만듦
PropFind,PropPatch	리소스와 컬렉션의 속성을 검색하고 설정
Copy,Move	이름 공간 문맥 내에 있는 컬렉션과 리소스를 관리
Lock,Unlock	덮어 쓰기 방지 기능
Options	서버가 지원하는 메소드를 출력

(Get, Post , Head 는 HTTP/1.0 에 있는 메소드이다.)

2.4 WebDAV의 구조

WebDAV 요청의 일반적인 구조는 HTTP 형식을 따르며 아래의 세 구성 요소로 이루어진다.

1. 메소드. 클라이언트가 실행할 메소드(앞서 설명한 메소드)를 말한다.
2. 헤더. 작업 실행 방법을 설명한다.
3. 본문(옵션). 위 메소드를 실행하는 방법에 대한 설명이나 추가 설명에 사용되는 데이터를 정의한다.

```
PROPFIND / HTTP/1.1.....................................(메소드)
Content-Type: text/xml
Depth: 1
Host: 172.16.5.63
User-Agent: WebDrive/5.2 NT DAV
Accept-Language: en-us.................................(헤더)
Translate: f
Pragma: no-cache
Connection: close
Content-length: 277

<?xml version ="1.0" encoding= "utf-8" ?>
<propf ind xmlns="DAV:">
   <prop><creation date/>
      <getlastmodified/>
      <displayname/>
      <getcontentlength/>
      <href/>
      <owner/>
      <resourcetype/>.................................(본문)
      <locktoken/>
      <lockdiscovery/>
      <collection/>
      <activelock/>
      <isreadonly/>
      <ishidden/>
      <BSI_isreadonly/>
</prop>
</propfind>
```

※ 위에서 보는 것처럼 본문에는 XML 을 사용한다. WebDAV와 XML은 서로 밀접한 관계가 있다.

3. WebDAV 취약점 개요

WedDAV 취약점은 전 세계의 컴퓨터에서 서버로 많이 사용되고 있는 윈도우즈의 주요 시스템 파일중 하나인 ntdll.dll에서 버퍼 길이 검사를 하지 않아서 발생한 것으로, IIS 서버를 운영하고 있는 아래 시스템이 취약점을 지니고 있다.

주요 플랫폼
Windows NT Server 4.0
Windows NT Server 4.0 SP1
Windows NT Server 4.0 SP2
Windows NT Server 4.0 SP3
Windows NT Server 4.0 SP4
Windows NT Server 4.0 SP5
Windows NT Server 4.0 SP6
Windows NT Server 4.0 SP6a
Windows 2000 Server
Windows 2000 Server SP 1
Windows 2000 Server SP 2
Windows 2000 Server SP 3

이 문서를 쓰는 현재 알려진 5개의 Exploit 이 발표되었다. 초기 Exploit 툴은 간단하지만, 나중에 나온 툴일수록 자동화가 잘 되어 있다. 이것은 추후 모든 감염 및 전파가 자동화 될 웜의 가능성을 암시하고 있다.

참조사이트
-> http://www.securityfocus.com/bid/7116/exploit/

4. WebDAV 취약점 분석

4.1 WebDAV 취약점 공격 및 버퍼오버플로 디버깅

WebDAV 가 최근에 사용되기 시작하는 부분이고, XML의 사용이 광범위하게 퍼져 있지 않은 상태에서 분석이 어려운 점이 있었다.

WebDAV 가 설치된 IIS(Internet Information Service) 에 아래 형식의 패킷을 보내면

[공격코드 일부분]

```
SEARCH /AAAAAAAAAAAA... HTTP/1.1
Host: 172.16.5.63
Content-Type: text/xml
```

eip=00410041을 가리키는 다음과 같은 Buffer Overflow 가 일어난다. ntdll.dll 내부에 있는 RtlDosPathNameToNTPathName_U 함수 부분에 취약점이 존재한다.

[버퍼 오버플로가 일어나는 부분]

```
(3e0.46c): Access violation - code c0000005 (first chance)
First chance exceptions are reported before any exception
handling.
This exception may be expected and handled.
eax=00f5e908 ebx=00f5ef60 ecx=00410041 edx=77f8e639 esi=00f5e930
edi=00000001 eip=00410041 esp=00f5e870 ebp=00f5e890 iopl=0 nv up
ei pl zr na po nc
cs=001b  ss=0023  ds=0023  es=0023  fs=003b  gs=0000 efl=00010246
00410041 ??              ???
0:008> k
ChildEBP RetAddr
WARNING: Frame IP not in any known module. Following frames may be
wrong.
00f5e86c 77f8e440 0x410041
00f5e890 77f8e4db ntdll!RtlSetBits+0x330
00f5e918 77fa0316 ntdll!RtlSetBits+0x3cb
00f5ecc0 77f8b0c0 ntdll!KiUserExceptionDispatcher+0xe
00f5ef70 00410041 ntdll!RtlDosPathNameToNtPathName_U+0xc4
00410041 00000000 0x410041
```

앞에서 URL 부분에 입력된 수많은 AAAA는 메모리 상에서 Unicode 형태로 변형되어 실

제 메모리에는 'AAAA' 형식 인 41414141 이 아닌 41004100처럼 중간에 0 이 들어가 입력 된다. 많은 수의 'A' 입력값이 일정 크기의 Buffer 경계를 넘어, 결국 Return Address 를 덮어쓴 결과, 프로그램은 예상치 못한 곳으로 실행 위치가 변경된다.

```
0118ee00 41 00 41 00 41 00 41 00 41 00 41 00 41 00 41 00  A.A.A.A.A.A.A.A.
0118ee10 41 00 41 00 41 00 41 00 41 00 41 00 00 00 00 00  A.A.A.A.A.A.....
```

IIS 의 WebDAV 에서 SEARCH, PROPFIND, LOCK 나 Translate: f 헤더를 포함한 GET 호출을 할때 GetFileAttributesExW 함수가 호출되며, 이 함수는 취약한 RtlDosPathNameToNTPathName_U 함수를 호출해서 Buffer Overflow 가 발생한다. RtlDosPathNameToNTPathName_U 함수는 경계값 검사를 하지 않는다.

IIS 가 System 권한으로 돌고 있기 때문에 공격이 성공하면 공격자는 명령을 Local System 권한으로 실행할 수 있다.

4.2 WedDAV의 Stack과 Memory

4.2.1 WedDAV의 Stack 영역

실제 공격이 일어나는 RtlDosPathNameToNtPathName_U 함수가 불러지기까지의 Stack 영역을 보면 다음과 같다.

[RtlDosPathNameToNTPathName_U 가 실행되기까지 스택 내용]

```
0:008> k
ChildEBP RetAddr
WARNING: Stack unwind information not available. Following frames
may be wrong.
00f5ef70 77e67346 ntdll!RtlDosPathNameToNtPathName_U
00f5eff8 77628d27 KERNEL32!GetFileAttributesExW+0x30
00f5f03c 7762a99e httpext+0x8d27
00f5f2c4 776347cb httpext!DllUnregisterServer+0x11a4
00f5f2e0 77638b4b httpext!DllCanUnloadNow+0x6862
00f5f328 77629771 httpext!STR::operator=+0x2e16
00f5f444 657b7375 httpext!HttpExtensionProc+0x2d
00f5f48c 657b876f wam!SE_TABLE::ReleaseExtension+0x6d7
00f5f4d0 6596288f wam!SE_TABLE::ReleaseExtension+0x1ad1
00f5f518 65961136 w3svc!WamDictatorDumpInfo+0x4bd
00f5fd50 6594fe4d w3svc!PARAM_LIST::CanonList+0x242e
00f5fd74                                                6594fdd1
w3svc!HTTP_REQ_BASE::BuildURLMovedResponse+0x2639
00f5fd98                                                6595805b
w3svc!HTTP_REQ_BASE::BuildURLMovedResponse+0x25bd
00f5ff18 65949965 w3svc!HTTP_REQ_BASE::TestConnection+0xde5
00f5ff38 6594a7ac w3svc!ScanForTerminator+0x548
00f5ff80 6d528a25 w3svc!CLIENT_CONN::Free+0x126
77db5761 922868ff ISATQ!AtqGetCapTraceInfo+0x934
6aec8b55 00000000 0x922868ff
```

4.2.2 WedDAV의 Memory 영역

실제로 메모리 부분에는 아래 와 같은 명령 부분이 반복되면서 메모리 부분을 덮어 쓰게된다.

[메모리 부분을 덮는 코드 부분]

```
77f8ae68 894dcc          mov    [ebp-0x34],ecx    ss:0023:0118ec8c=0118ee18
77f8ae6b 015da0          add    [ebp-0x60],ebx    ss:0023:0118ec60=01bc5a58
77f8ae6e 8b55a0          mov    edx,[ebp-0x60]    ss:0023:0118ec60=01bc5a5a
77f8ae71 668b12          mov    dx,[edx]          ds:0023:01bc5a5a=0041
77f8ae74 6685d2          test   dx,dx
77f8ae77 74c9           jz ntdll!RtlNtStatusToDosError+0x962 (77f8ae42)
[br=0]
77f8ae79 663bd0          cmp    dx,ax
77f8ae7c 74c4           jz ntdll!RtlNtStatusToDosError+0x962 (77f8ae42)
[br=0]
77f8ae7e 6683fa2         cmp    dx,0x2f
77f8ae82 74be           jz ntdll!RtlNtStatusToDosError+0x962 (77f8ae42)
[br=0]
77f8ae84 6683fa2e        cmp    dx,0x2e
77f8ae88 75d9           jnz ntdll!RtlNtStatusToDosError+0x983 (77f8ae63)
[br=1]
77f8ae63 668911          mov    [ecx],dx            ds:0023:0118ee1a=0000
eax=0000005c ebx=00000002 ecx=0118ee1a edx=01bc0041 esi=00000000
edi=00000041
eip=77f8ae66 esp=0118ec18 ebp=0118ecc0 iopl=0         nv up ei pl nz ac pe nc
cs=001b  ss=0023  ds=0023  es=0023  fs=0038  gs=0000             efl=00000212
ntdll!RtlNtStatusToDosError+986:
77f8ae66 03cb            add    ecx,ebx
```

[스택영역이 파괴되는 부분]

```
0118ee00 41 00 41 00 41 00 41 00 41 00 41 00 41 00 41 00  A.A.A.A.A.A.A.A.
0118ee10 41 00 41 00 41 00 41 00 41 00 41 00 00 00 00 00  A.A.A.A.A.A.....
```

4.2.3 이외 취약한 관련 함수 및 라이브러리

아래의 왼쪽 함수들이 내부에서 RtlDosPathNameToNTPathName_U 함수를 호출하므로 잠재적인 취약점이 예상된다. 그리고 이 함수들을 내장하고 있는 라이브러리는 오른쪽에 있다. (물론 다른 라이브러리도 이 함수들을 호출할 수 있다.)

GetVolumneInformationW DeleteFileW GetDriveTypeW GetFileAttributesExW CreateDirectoryW FindFirstChangeNotificationW GetBinaryTypeW CreateNamedPipeW SetFileAttributesW MoveFileWithProgressW GetVolumeForVolumeMountPointW GetDistFreeSpaceW CreateDirectoryExW DefineDosDeviceW PrivMoveFileIdntityW GetCompressedFileSizeW SetVolumeLableW CreateHardLinkW RemoveDirectoryW	acledit.dll advapi32.dll cscdll.dll csrsrv.dll dskquoui.dll eventlog.dll gdi32.dll ifsutil.dll lsasrv.dll ntdll.dll ntmarta.dll ole32.dll perfproc.dll query.dll rshx32.dll scesrv.dll sdbapiu.dll setupdll.dll sfc.dll shell32.dll shim.dll srvsvc.dll svcpack.dll trkwks.dll ulib.dll wow32.dll

4.3 Weblog

공격이 성공하면 로그에는 아무것도 남지 않는다. 오직 공격을 했다는 흔적은 IIS 서버가 이유없이 재부팅 했을 경우에서 찾을 수 있다. 실제 공격 툴들은 공격 후 잠시 재부팅 하는 동안 응답이 없는 점을 이용해서 공격 성공 여부를 확인한다. (공격은 abcd.html 과 efgh.html 을 보는 사이에 이루어 졌다.)

[공격 성공 로그]

```
--------------------------------------------------------------------------------
#Software: Microsoft Internet Information Services 5.0
#Version: 1.0
#Date: 2003-04-09 06:42:13
#Fields: date time c-ip cs-username s-ip s-port cs-method cs-uri-stem
cs-uri-query sc-status cs(User-Agent)
2003-04-09 06:42:13 172.16.5.62 - 172.16.5.245 80 GET /index.html - 304
Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.0)
2003-04-09 06:42:25 172.16.5.62 - 172.16.5.245 80 GET /abcd.html - 404
Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.0)
#Software: Microsoft Internet Information Services 5.0
#Version: 1.0.....(재부팅 즉 공격성공부분)
```

```
#Date: 2003-04-09 06:43:31
#Fields: date time c-ip cs-username s-ip s-port cs-method cs-uri-stem cs-uri-query sc-status cs(User-Agent)
2003-04-09 06:43:31 172.16.5.62 - 172.16.5.245 80 GET /efgh.html - 404
------------------------------------------------------------------------
```

아래는 현재 공개되어 있는 공격 도구의 로그들이다. 버퍼 크기를 잘못 측정해서 버퍼 오버플로 공격이 실패 했을 때 로그가 남으며, 버퍼의 크기를 제대로 조사해 공격했다면 IIS Server가 Crash되고 재시작될 뿐 로그는 남지 않는다.

[공격 툴 Weblog]

----

webdavin tool

```
2003-04-09 07:04:05 172.16.5.62 - 172.16.5.245 80 SEARCH /金金金金金金金金金金金金金金金金金金金金金金金金金金金金金金金金金金金金金金金金金金金럱럱럱럱럱럱럱럱럱럱럱럱럱럱럱럱럱럱럱럱럱럱럱럱?- 500 -
2003-04-09 07:04:20 172.16.5.62 - 172.16.5.245 80 SEARCH /菉菉菉菉菉菉菉菉菉菉菉菉菉菉菉菉菉菉菉菉菉菉菉菉菉菉菉菉菉菉菉菉菉菉菉菉菉菉菉菉菉菉菉菉菉菉菉菉菉菉菉菉菉菉菉菉菉菉菉菉菉菉菉菉菉菉菉菉菉菉菉菉菉菉菉菉菉菉菉菉菉럱럱럱럱럱럱럱럱럱럱럱럱럱럱럱럱럱럱럱럱럱럱럱럱?- 500 -
```

KaHT tool

```
2003-04-09 07:13:46 172.16.5.62 - 172.16.5.245 80 PROPFIND / - 207 KaHT
2003-04-09 07:13:55 172.16.5.62 - 172.16.5.245 80 PROPFIND / - 207 KaHT
```

wd.pl

```
2003-04-09 07:20:36 172.16.5.62 - 172.16.5.245 80 GET /iisstart.asp - 200 -
2003-04-09 07:20:36 172.16.5.62 - 172.16.5.245 80 LOCK
/XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXびふぴ鉒皮참참참참참참참참참참참참참참참참참참쥩禱슦쮎쏀잉슉쥩遁遁쏀적nF갖る윗적´윕잊ら쥩α遁쮎遇黎탱뻽 δ쉹즅쮎즅HHDEvv440.,*abHH**,-¡?hi,, deXY+gg,*1.deXY~¡VV LMUUqq}}89LMLMLMLMbb++;9NNlmlmLM88_`LMLMLMddghxyrsDELMLLab33EF --``34ddgheexyVWDELMLL ,-vv11`a ``=>;8--+ lmlmLM+lmlmLMyzOP``891.333333TT'$ef ;8++-.))lmlmLMef33 ++--;9lmlmLMeede --33lmlmLMee33 lmlmLMTT'$ ef ;8++-.''lmlmLMef33 lmlmLM33LMccz{}}uv~~||vwLMccz{wwuvxxvw~~LMccz{}}z{{{uu~~LMggxx{|nnpq~~}}LMnnpqxxvwdeuv{{}}~~uuuuLM}}QRbcvw]Z~~pq~~LMLMLMLM{|~~vw^[vvuu~~uv^[zz| - 500 -
```

rs_iis.c

```
2003-04-09 07:51:07 172.16.5.62 - 172.16.5.245 80 SEARCH
/?H H H H H H H H H H H H H H H H H H H H H H H H H H H H 럱럱럱럱럱럱럱럱럱럱럱럱럱럱럱럱럱럱럱럱럱럱럱럱럱럱럱럱럱럱럱럱럱럱럱럱럱럱럱럱럱럱럱럱럱럱럱럱럱럱럱럱럱 - 500 -
```

2003-04-09 07:51:18 172.16.5.62 - 172.16.5.245 80 SEARCH
/?H H H H H H H H H H H H H H H H H H H H H H H H H H H H 릾릾릾릾릾릾릾릾릾릾릾릾릾릾릾
릾릾릾릾릾릾릾릾릾릾릾릾릾릾릾릾릾릾릾릾릾릾릾릾릾릾릾릾릾릾릾릾릾릾릾릾릾릾 - 500 -

wbr.c

2003-04-09 07:45:17 172.16.5.62 - 172.16.5.245 80 SEARCH
/↕↕↕↕↕↕↕↕↕↕↕↕↕↕↕↕↕↕↕↕↕↕↕↕↕↕↕↕ 릾 릾 릾 릾 릾 릾 릾 릾 릾 릾 릾 릾 릾 릾 릾 릾 릾 릾
릾릾릾릾릾릾릾릾릾릾릾릾릾릾릾릾릾릾릾릾릾릾릾릾릾릾릾릾릾릾릾릾릾릾릾?- 500

----

5. 대응방법

5.1 원격 확인 방법

아래의 Perl 프로그램을 사용해서 WebDAV가 작동되고 있는지 원격으로 확인 할 수 있다. 이 프로그램 출력 결과가 IIS WebDAV Patch needed라는 메시지가 나오는 서버들이 패치를 적용거나, WebDAV 사용을 중지시키는 것이 필요하다.
(주의: 이전에 WebDAV 보안 패치를 한 서버도 WebDAV를 사용하고 있으면, 마찬가지로 IIS WebDAV Patch needed 메시지를 출력하지만, 서버는 안전하다. - 패치 설치 여부는 [제어판]-[프로그램 추가/제거]-[현재 설치된 프로그램] 에서 Windows 2000 핫픽스(SP4) Q815021 이 설치되어 있는지 여부로 확인할 수 있다.)

check_webdav.pl

```
#!/usr/bin/perl
#created by oprix
#ryusc@certcc.or.kr

use IO::Socket;

$hostname = $ARGV[0];
$send_str    =    "OPTIONS    *    HTTP/1.1\r\nHost:    $hostname\r\nConnection:
Close\r\n\r\n";

if ( $#ARGV == 0 ) {
        print "Usage: perl check_webdav.pl [hostname]\n";
        exit;
}

$port = 80;

$socket = IO::Socket::INET->new( PeerAddr => $hostname ,
                                 PeerPort => $port,
                                 Proto    => "tcp",
                                 Type     => SOCK_STREAM) or die "Couldn't connect
$hostname : $@\n";

print $socket $send_str;

$answer = "";

while(<$socket>) {
        $answer = $answer . $_;
}

if ( $answer =~ /IIS/) {
        if ( $answer  =~ /DELETE/ ) {
```

```
                print "$hostname IIS WebDAV Patch needed\n";
        } else {
                print "OK, $hostname is Safe.\n";
        }
} else {
                print "OK, $hostname is Safe.\n";
}

close($socket);
```

5.2 대응 방법

대응 방법은 사용하는 서버가 어떤 용도로 쓰이는 지에 따라 다르다.

● IIS 를 사용하지 않을 경우

[시작]-[프로그램]-[관리 도구]-[컴퓨터 관리]-[서비스 및 응용 프로그램]-[서비스]에서 [World Wide Web Publishing Service]를 마우스 오른쪽 버튼으로 누르고, [일반]탭에서 서비스 상태에서 중지를 누른다음, 시작유형을 사용 안함으로 설정하면 된다.

● IIS를 사용하지만 WebDAV를 사용하지 않을 경우

아래의 용도로 쓰지 않으면 WebDAV 기능을 꺼 놓을 수 있다.
WebDAV 는 현재 다음과 같은 목적으로 이용되고 있다.
- Web Folders
- Office 2000 을 이용하는 (그러나 FrontPage Server 확장기능을 통하지 않는) 웹 사이트로의 출판
- Digital Dashboard 를 통한 IIS 5.0 서버의 모니터링

또한, 아래의 Microsoft 기술 자료 기사에 열거된 지시 사항대로 하면 WebDAV를 비활성화 할 수도 있다.

레지스트리 편집기(Regedt32.exe)를 시작한다.
레지스트리에서 다음 키를 찾아 누른다.
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\W3SVC\Parameters

편집 메뉴에서 값 추가를 누른 후 다음 레지스트리 값을 추가한다.
값 이름: DisableWebDAV
데이터 형식: DWORD
값 데이터: 1

● IIS를 사용하고, WebDAV도 필요한 경우
1) 시스템 패치
* 주의 사항 System Crash
MS 에 따르면, 2001년 12월부터 2002년 2월 사이에 발표된 Windows 2000 핫픽스

몇 가지가 이번 취약점 패치와 호환되지 않는다. Windows 2000 서비스 팩 2에, 이 취약점이 발표 되기 전에 나온 12개의 핫픽스를 실행했다면 이 패치 적용 후 재부팅시 Stop 오류 문제를 겪을 수 있다.

Windows 2000 서비스 팩 3을 실행중인 사용자나 이들 핫픽스를 설치한 적이 없는 사용자는 이런 문제를 겪지 않는다.

Windows 2000 SP2를 실행중이면, 이 패치를 설치하기 전에 시스템에 있는 ntoskrnl.exe의 버전을 점검하면 된다. 시스템의 ntoskrnl.exe 버전을 확인하려면, 다음과 같이 작업한다:
1. %windir%\system32 폴더를 연다.
2. ntoskrnl.exe 파일을 마우스 오른쪽 버튼으로 클릭한다.
3. 등록 정보를 선택한다.

'버전' 탭에 버전 정보가 표시된다.
ntoskrnl.exe의 버전이 5.0.2195.4797에서 5.0.2195.4928이면 이 패치와 호환되지 않는다.

※ Patch 사이트 주소:
http://www.microsoft.com/downloads/details.aspx?FamilyID=c9a38d45-5145-4844-b62e-c69d32ac929b&displaylang=ko

2) 버퍼를 제한하는 방법
IIS가 받아들이는 데 이용하는 버퍼를 제한할 수 있다. Microsoft는 URL Buffer Size Registry Tool을 제공하여 버퍼를 제한하는 레지스트리 키를 자동으로 설정할 수 있다. 이 도구는 Windows 2000을 운영하는 웹 서버에서 작동하여 이 취약점을 악용할 수 있는 침입으로부터 보호한다. 이 도구는 웹 서버 상에서 로컬로 작용하거나, 서버에 대해 관리 액세스를 가진 사용자에 의해 원격으로 다수의 웹 서버에 적용될 수도 있다.

URL Buffer Size Registry도구는 Windows 2000 Service Pack 2 또는 Service Pack 3를 운영하는 시스템에서 실행될 수 있다. 추가로 다음 기술 자료 기사에 있는 지시 사항대로 하면 수동으로 레지스트리 변경을 적용할 수 있다.

Hkey_Local_Machine\System\CurrentControlSet\Services\W3SVC\Parameters
값 이름: MaxClientRequestBuffer
데이터 형식: DWORD
값 데이터: 16000

반드시 버퍼가 64K 바이트 미만의 크기로 설정되어야 한다는 것에 주의해야 한다. 적당한 값으로 16K를 권장한다. 64K는 URL Buffer Size Registry 도구에 의해 자동으로 설정되는 한계이다.

6. Worm 으로의 생성 여부

가능성:

1) Windows 서버의 광범위 성:

전 세계의 컴퓨터의 많은 부분을 Windows가 점하고 있으며,
WebDAV 패치를 하지 않은 아래의 서버들이 취약하다.
Windows 2000 Server , SP1 , SP2 , SP3
Windows NT 4 SP1, SP2 , SP3 , SP4 , SP5 , SP6 , SP6a

2) Default 설치

Windows 2000에 IIS는 기본적으로 설치되며, IIS에 WebDAV 도 기본적으로 설치된다.

3) HTTP 프로토콜

대부분의 방화벽에서는 80(HTTP) 포트를 필터링 하지 않는다.

어려운 점:

1) IIS 내부 버퍼에서 공격 코드가 Unicode로 변환 되기 때문에, 각 나라마다 Unicode 가 다르므로, 전 세계 서버들을 대상으로 하는 공격 코드를 만들기가 힘들다. (실제로 Windows NT 계열은 내부에서 Unicode를 사용한다.)

7. 결론

WebDAV 취약점은 ntdll.dll 내부의 RtlDosPathTONTPathName_U 함수에서 경계 검사를 하지 않아서 생기는 문제이다. 이 취약점은 현재로서는 웜으로 만들기 어려운 점이 있지만, 영어를 사용하는 국가, 한글을 사용하는 국가, 이런 식으로 언어 코드가 같은 국가를 대상으로 공격 코드를 만드는 건 가능하다. 따라서 추후에 생길지도 모르는 한국을 대상으로 만들 어 질 수 있는 웜 관련 문제에 대비해, Windows 2000 서버 관리자들이 패치를 해서 사전에 이런 가능성을 차단하는게 좋다.

8. 참고자료

CERT-KR
Windows Web Component의 체크되지 않은 버퍼로 인한 코드 실행 취약점
김영직 http://www.certcc.or.kr/advisory/ka2003/ka2003-013.txt

Microsoft
Windows 구성요소 내에 있는 점검되지 않은 버퍼가 웹 서버를 손상시킬 수 있음
http://www.microsoft.com/korea/technet/security/bulletin/MS03-007.asp

Microsoft

기형의 WebDAV 요청으로 인해 IIS가 CPU 자원을 고갈시킴
http://www.microsoft.com/korea/technet/security/bulletin/MS01-016.asp

CERT
Buffer Overflow in Core Microsoft Windows DLL
http://www.cert.org/advisories/CA-2003-09.html

CIAC
Microsoft Unchecked Buffer in Windows Component Could Cause Web Server Compromise
http://www.ciac.org/ciac/bulletins/n-054.shtml

Next Generation Security Software
New Attack vectors and MS03-007
http://www.nextgenss.com/papers/ms03-007-ntdll.pdf

SecurityFocus
Microsoft Windows 2000 ntdll.dll Buffer Overflow Vulnerability
http://www.securityfocus.com/bid/7116

KLDP
아파치 WebDAV와 LDAP HOWTO
http://kldp.org/HOWTO/html/Apache-WebDAV-LDAP-HOWTO

WebDAV
DAV Frequently Asked Questions
http://www.webdav.org/other/faq.html

IETF
Hypertext Transfer Protocol -- HTTP/1.1
http://www.ietf.org/rfc/rfc2068.txt

IETF
HTTP Extensions for Distributed Authoring -- WEBDAV
http://www.ietf.org/rfc/rfc2518.txt

Microsoft
Web을 통해 WebDAV와 XML 데이터 통신
http://www.microsoft.com/korea/msdn/xml/articles/xmlandwebdav.asp