

Monthly Security News Letters



September. 2010

NETSOL
S Y S T E M

Table of Contents

SECTION 1. 보안뉴스 국/내외 동향..... 3

- 1.1 한컴오피스도 더블클릭 실행 악성코드 감염 위험3
- 1.2 GS칼텍스 개인정보유출 배상책임없다.....4
- 1.3 온라인 게임 계정 탈취 악성코드 주의5
- 1.4 1주일 5만7천 악성홍피 양산 (해외).....6
- 1.5 사이버보안 인식 제고 시급 (해외)7
- 1.6 블랙베리, 인도에 무류 `팍' 꿏다 (해외).....7

SECTION 2. 보안취약점 정보(VULNERABILITY) 9

- 2.1 ADOBE FLASH PLAYER 원격코드실행 취약점 주의9
- 2.2 HP DATA PROTECTOR EXPRESS LOCAL CODE EXECUTION VULNERABILITY.....9
- 2.3 2010년 9월 MS 월간 보안 업데이트 권고.....10
- 2.4 마이크로소프트 ASP.NET 신규 취약점 주의.....10
- 2.5 월간동향 및 허니넷/트래픽 분석11

SECTION 3. 보안 팁(TECHNOLOGY TIP & IT GOVERNANCE)..... 13

- 3.1 악의적인 파일 업로드 취약점의 점검 및 보호대책.....13
- 3.2 오라클 보안 강화를 위한 PARAMETER 설정 방법.....14
- 3.3 ARP SPOOFING 대책 수립 방법.....17

SECTION 1. 보안뉴스 국/내외 동향

1.1 한컴오피스도 더블클릭 실행 악성코드 감염 위험

'한컴오피스 2010' 17일 보안 패치 배포, 패치 서둘러야...

우리나라에서 가장 많이 사용되고 있는 토종 워드프로세서인 '아래아 한글'이 포함된 '한컴오피스'에서도 더블클릭시 악성코드에 감염될 수 있는 DLL 하이재킹 취약점이 존재하는 것으로 밝혀져 주의가 필요해 보인다.

특히 한컴오피스에 포함된 한글워드프로세서의 경우, 공공기관과 기업 및 일반사용자들 사이에서 가장 많이 이용되는 것으로 알려져 있어 문제의 심각성을 더하고 있다.

현재 이 취약점이 존재하는 것으로 확인된 한컴오피스 제품 버전은 '한컴오피스 2010' 과 '한컴오피스 2007'이다.

DLL 하이재킹은 마이크로소프트가 지난 8월 23일(미국 현지시간) 발표한 보안권고(2269637)와 관련된 것으로, 윈도우 프로그램에서 DLL파일을 로딩할 때 적절한 경로 검증을 하지 않아 발생하는 원격코드 실행 취약점이다. 이 취약점에 노출된 윈도우 프로그램은, 해커가 악성코드가 포함된 DLL파일을 실행시켜 개인 정보나 금융정보 노출 및 DDoS 공격에도 악용될 수 있다.

이 취약점은 악성공격자가 배포한 DLL파일이 존재할 경우, 더블클릭해서 파일을 열면 해킹 공격에 노출될 수 있다. 가령, 스팸메일이나 P2P 웹하드에서 다운받은 압축파일에 HWP파일과 공격용 DLL파일이 함께 존재할 경우, 압축을 해제하고 단순히 더블클릭으로

파일을 열기만 해도 해킹 공격을 받을 수 있다는 이야기다.

한컴오피스의 개발사인 한글과컴퓨터 측은 이 취약점의 위험성을 파악하고 서둘러 취약점 패치에 나선 것으로 확인되고 있다.

한글과컴퓨터의 한 관계자는 “현재 한컴오피스 2010 과 2007에 DLL 하이재킹 보안 취약점이 존재하는 것을 확인했다”면서 “한글과컴퓨터는 보안취약점에 대해서는 정규적인 업데이트와는 별도 최우선적으로 긴급히 업데이트를 배포할 방침”이라고 밝혔다.

한글과컴퓨터 측에 따르면, 한컴오피스 2010에 대한 보안 업데이트는 9월 17일 배포될 예정이며, 이후 한컴오피스 2007 패치도 배포할 예정이라고 전했다. 수정된 패치는 자동업데이트와 한글과컴퓨터 홈페이지 (<http://www.hancom.co.kr>) 자료실을 통해 업데이트를 받을 수 있다.

그러나 네티즌들은 이미 한컴오피스의 취약점이 어느 정도 예상된 상태에서 너무 느장 대응한 것이 아니냐는 비난의 목소리를 보내기도 했다.

ANOW라는 아이디의 블로거는 자신의 블로그에 ‘한글과컴퓨터 - DLL Hijacking 제로데이(0-day) 취약성 발생과 그 경과 — 아쉬운 한글과컴퓨터의 태도’라는 글에서 한컴오피스의 DLL 하이재킹에 대한 취약성과 이로 인해 나타날 수 있는 공격 시나리오를 올리고 한글과컴퓨터의 느장 대응을 지적했다.

그는 “만약, DLL 파일이 시스템 종료로 호출하게 하는 DLL 파일이었다고만 생각하면, 잘 모르는 사람들은 포맷까지 하는 웃지 못 할 상황도 연출 될 수 있을 것”이라고 지적했다.



▲한컴오피스 취약점 제보에 대한 답변

더불어 그는 “발견 된 취약성을 2010년 8월 29일 날짜로 한글과컴퓨터에 기술문의 센터에 제보했지만 답변이 없었고, 다시 9월 15일 재문의를 해서야 관련 내용을 확인하고 있다는 소극적인 모습을 보였다”고 비난했다.

보안업계의 한 전문가는 “윈도우기반 소프트웨어의 경우 MS윈도우의 제로데이 취약점으로 인한 공격이 대부분이기 때문에 소프트웨어 개발사들도 MS윈도우의 제로데이에 대한 관심을 가지고 이에 적극 대응해야 할 필요가 있다”고 조언했다.

[원문출처]

(보안뉴스 - 오병민기자)

<http://www.boannews.com/media/view.asp?page=1&gpage=1&idx=22902&search=&find=&kind=13>

1.2 GS칼텍스 개인정보유출 배상책임없다

서울중앙지법 민사합의31부(황적화 부장판사)는 16일 김모씨 등 2만8천 여명이 `GS칼텍스 회원정보 유출' 사건으로 피해를 봤다며 GS칼텍스와 자회사 GS넥스 테이션을 상대로 낸 손해배상 청구소송에서 원고 패

소로 판결했다.

재판부는 "GS칼텍스 등에게 사건의 책임을 지우려면 개인정보가 불특정 다수에게 공개돼 타인이 이를 열람하거나 수집·이용할 위험이 인정돼야 하는데 관련자 10여 명이 보관하다 수사 초기에 압수·반납되거나 폐기됐으므로 개인정보 자기결정권이 실질적으로 침해됐다고 인정하기 어렵다"고 밝혔다.

이어 "피해자로서는 정보가 유포될 수 있다는 불안감을 지닐 수 있다는 점은 충분히 이해되지만, 수사기관이 자료를 즉시 압수하는 등의 조치를 한 사건 경위에 비춰볼 때 위자료를 지급할 만큼의 정신적 손해가 발생했다고는 볼 수 없다"고 덧붙였다.

GS넥스 테이션의 직원이던 정모 씨는 고객 정보를 빼돌려 집단소송을 의뢰받은 변호사 등에게 판매하기로 마음먹고 2008년 7월 회사 서버에 접속해 보너스카드 회원 1천151만7천125명의 성명과 주민등록번호, 주소, 전화번호, 이메일 주소 등을 사무용 컴퓨터에 내려받은 뒤 DVD에 복사에 몇몇 지인에게 줬다.

이들 자료는 판매처 물색과정에서 `집단소송에 활용하려면 개인정보 유출 사실이 알려져 사회문제가 돼야 한다'는 모 변호사 사무실 사무장의 언급에 따라 `쓰레기 더미에서 고객정보가 담긴 DVD를 주웠다'는 거짓 설명과 함께 몇몇 기자와 PD에게 전달됐다.

이후 GS칼텍스의 고객정보가 유출됐다는 보도가 이어졌고 경찰은 즉시 수사에 착수, 정씨 등을 검거하고 고객정보가 담긴 DVD와 CD를 압수하거나 임의제출 받았으며 나머지는 폐기됐다.

정씨를 비롯해 유출에 관여한 5명은 정보통신망 이용촉진 및 정보보호 등에 관한 법률 위반 혐의로 기소돼 실형이나 집행유예가 확정됐으며, 종업원의 불법행

위 때문에 함께 기소된 GS백스태이션에는 업무의 일부로 이뤄진 범행이 아니라는 등의 이유로 무죄가 선고됐다.

당시 정보가 유출된 피해자들은 "GS칼텍스가 서버 내 개인정보를 이동저장장치에 내려받게 허용할 정도로 보안관리가 허술했다"며 1인당 100만원 안팎의 위자료를 청구하는 소송을 냈다.

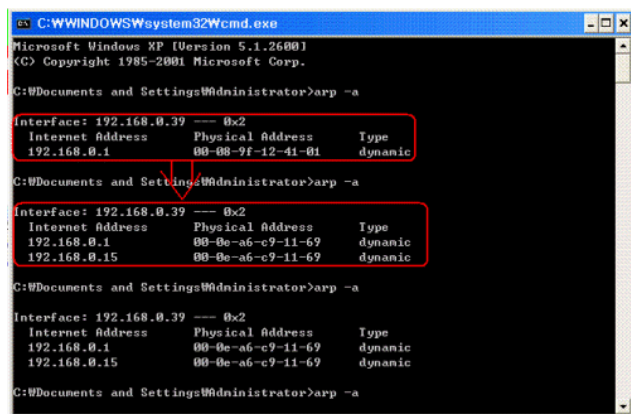
[원문출처]

(보안닷컴)

<http://www.boan.com/news/articleView.html?idxno=3037>

1.3 온라인 게임 계정 탈취 악성코드 주의

최근 온라인 게임 계정을 탈취하는 악성코드가 일부 웹사이트를 통해 확산 중인 것으로 파악돼 사용자들은 주의가 필요하겠다.



▲ARP 패킷을 유발하는 컴퓨터를 찾으려면 [시작] > [실행]을 실행 후 cmd 입력 후 [확인] 버튼을 누른다. 그리고 명령 프롬프트가 실행되면 'arp - a' 입력 후 위와 같이 동일한 물리적 주소(Physical Address)가 존재하는지 확인하면 된다.

안철수연구소(대표 김홍선)는 7일 최근 온라인 게임

계정을 탈취하는 악성코드가 일부 웹사이트를 통해 확산 중이라고 경고했다. 특히 이 악성코드는 ARP 스푸핑(ARP Spoofing)을 통해 감염된 컴퓨터와 동일 네트워크에 있는 다른 PC에 전염되므로 개인은 물론 기업에서도 각별히 주의해야 한다. 현재 안철수연구소 시큐리티대응센터에는 네트워크 장애를 겪는 기업, 인터넷 뱅킹 접속이 안 되는 개인의 사례가 접수되고 있다.

사용자가 보안에 취약한 웹사이트에 접속하면 악성코드인 yahoo.js 파일이 실행되고, 이어서 다른 악성코드가 다운로드 및 실행된다. yahoo.js 파일의 코드를 풀면 ad.htm, news.html, count.html 파일로 다시 접근한다. ad.htm 파일은 MS 인터넷 익스플로러의 MS10-018 취약점을, news.html 파일은 MS10-002 취약점을 이용해 s.exe 파일을 다운로드 및 실행한다.

s.exe 파일은 C:\ Windows\ System32 폴더에 xcvaver0.dll 파일을 생성하는데, 이 파일이 던전 앤 파이터, 아이온, 메이플 스토리 등의 온라인 게임 계정을 유출하는 기능을 한다. 또한 같은 네트워크에 있는 컴퓨터에서 웹 서핑을 할 경우 yahoo1.js (yahoo.js와 동일) 파일로 접근하게 한다. 사내 컴퓨터 중 한대라도 감염돼 있으면 다시 전파될 위험이 있는 것이다.

현재 이 악성코드는 안철수연구소를 비롯해 일부만 진단·치료하는 상태이다. 이 악성코드의 피해를 막으려면 사이트가드(기업은 사이트가드 프로)를 설치해 위험한 웹사이트 접속을 예방하고, 개인 및 사내 모든 컴퓨터를 V3 최신 버전으로 업데이트하고 윈도우 보안 패치를 해야 한다.

V3 제품군과 온라인 통합보안 서비스인 '안랩 온라인 시큐리티(AOS)', 유해 사이트 차단 서비스인 '사

이트가드 , 등은 JS/Exploit, JS/Psyme, Dropper/Malware.42496.GF, Win-Trojan/Downloader.4608.AOS 등으로 진단한다. 또한 안철수연구소는 ARP 스푸핑의 진원지 컴퓨터를 손쉽게 탐지/차단할 수 있는 전용 백신(www.ahnlab.com/kr/site/download/vacc/vaccView.do?webVaccBoardsVo.seq=73)을 별도 제공 중이다.

이에 전성학 안철수연구소 시큐리티대응센터장은 “개인은 물론 기업에도 피해를 주는 악성코드이므로 개인과 웹사이트 관리자, 기업 네트워크 관리자 모두 각별히 주의해야 한다”라고 당부했다.

한편 ARP 스푸핑(Address Resolution Protocol Spoofing)은 동일 네트워크에 존재하는 공격 대상 PC의 IP 주소를 공격자 자신의 랜카드 주소와 연결해 다른 PC에 전달돼야 하는 정보를 가로채는 공격을 말한다.

어떤 PC에 ARP 스푸핑 기능을 가진 악성코드가 설치되면 약간의 조작으로 동일 구역 내의 다른 PC에 쉽게 악성코드를 설치할 수 있다. ARP 스푸핑 공격을 이용한 악성코드 유포 기법은 2007년 상반기에 처음 나타났다. 과거에 해커는 유명한 웹 서버 자체를 공격해 악성코드 경유지로 활용했다.

그러나 웹 서버 보안이 강화하자, 네트워크의 서브넷(subnetwork) 내에 침투해 ARP 위장으로 해당 서브넷 내의 PC들을 감염시키는 기법을 쓰게 된 것이다. 어떤 컴퓨터에 ARP 위장 기능을 가진 악성코드가 설치되면 약간의 조작으로 동일 구역 내의 다른 컴퓨터에 쉽게 악성코드가 설치될 수 있다. 이는 종전과 달리 사용자가 해킹된 웹사이트를 방문하지 않더라도 악성코드에 감염될 수 있다는 것을 의미한다.

[원문출처]

(보안뉴스 - 김정완기자)

<http://www.boannews.com/media/view.asp?page=3&gpage=1&idx=22734&search=&find=&kind=0>

1.4 1주일 5만7천 악성츄피 양산 (해외)

해커들이 주당 5만7000개의 악성페이지를 만들어 내고 있는 것으로 조사됐다.

네트워크월드는 8일 보안전문회사 팬더시큐리티의 조사를 인용해 해커들이 악성코드 등에 감염된 새로운 웹페이지를 매주 5만7000여개를 양산해내고 있다고 밝혔다.

팬더시큐리티 리서치센터는 또한 이런 악성 웹사이트의 65%가 은행으로 보이도록 설계됐으며 27%는 이베이와 같은 온라인 경매사이트라고 생각하도록 설계됐다고 조사했다.

1.9%의 가짜 웹사이트는 정부기관처럼 보이도록 만들어놓았으며 2.3%는 펀드 및 브로커 등 금융기관을 사칭하는 사이트로 구성해놓았다.

나머지 악의적인 사이트들은 ISP와 게임사이트에 접속하고 있는 것으로 인터넷이용자들을 속이고 있으며 페이팔 같은 가짜 지불사이트로 위장한 사이트도 발견됐다.

팬더시큐리티는 “검색엔진에서 웹사이트 방문시 해당 사이트가 진짜인지 가짜인지 위험성이 있는지 등을 인터넷사용자에게 알려줘야한다”며 “검색엔진에서 이러한 기술을 제공한다면 입력시 검색엔진을 사용하는 것이 더 정확할 수 있다”고 말했다.

[원문출처]

(보안닷컴 – 장윤정기자)

<http://www.boan.com/news/articleView.html?idxno=2986>

1.5 사이버보안 인식 제고 시급 (해외)

미국이 사이버보안 인식 제고를 위해 다양한 노력을 기울이고 있어 우리나라도 이와 관련한 대책이 필요하다는 지적이다.

미국은 최근 국가 기반시설 보호와 사이버 보안에 대한 인식 제고를 위해 웹사이트를 개설했다. 미국은 이 사이트를 통해 개인 PC 보안지침을 비롯해 오바마 정부의 사이버 보안 정책 등을 자세히 알릴 계획이다.

미국이 이처럼 사이버보안 인식 제고를 추진하는 것은 최근 미국에서 인터넷 침해사건이 늘어났기 때문이다. 미국 사이버보안 간부회의에 따르면, 지난해 상반기에만 미국 국방부를 대상으로 약 4만건 이상의 해킹시도가 있었다. 미국은 이를 해결하기 위해 1억 달러(약 1160억원)이상을 사용했으며, 올 들어 미국 은행의 사이버 범죄로 인한 피해액만 1억달러에 달한다.

이에 따라 미국은 대통령실에 사이버공간보호국(NOC)을 설치하고, '연방정보보안관리법 개정안'을 과반수 찬성으로 통과시키는 등 사이버보안 인식 제고를 위해 노력하고 있다.

그러나 우리는 관련법 정비는 물론 홍보조차 제대로 이뤄지지 못하고 있는 실정이다. 방송통신위원회가 지난달부터 지상파 방송 3사와 케이블TV 등을 통해 사이버보안 인식 제고를 위한 방송을 시작했다. 방통위는 하반기에 매 달 주제를 달리해 사이버 보안과 관련한 프로그램을 방송하고 이 달 1일부터 좀비PC를

주제로 한 사이버 보안 캠페인을 방송을 통해 홍보할 계획이다.

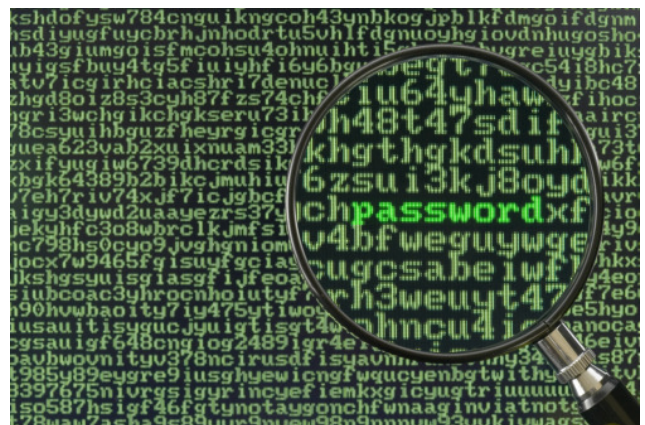
그러나 전문가들은 단순히 방송만을 통한 홍보에는 한계가 있고, 조직정비와 다각적인 홍보전략을 마련해야 한다고 지적하고 있다.

[원문출처]

(디지털타임스 – 감지선기자)

http://www.dt.co.kr/contents.html?article_no=2010090102010251746002

1.6 블랙베리, 인도에 무류 '팍' 꿰다 (해외)



▲ 통신서비스업체들은 고객 메시지가 정부 감시의 눈길에서 벗어나길 원한다. 반면 정부는 범죄나 드러나지 않은 테러 계획 등을 추적하기 위해 이메일 등 통신 내용에 접근하기를 고집하고 있다.

'블랙베리'의 리서치인모션(RIM)이 인도 정부에 고객 데이터 접근을 허용하기로 했다.

로이터와 AFP등 외신은 RIM이 최근 인도 정부에 암호화 코드 해독을 통한 고객의 이메일과 문자메시지 검열방안을 제안했으며, 인도 정부 또한 검토중이라고 31일 보도했다.

인도 정부는 그동안 사우디아라비아, 아랍에미리트 (UAE), 쿠웨이트 등과 같이 ‘블랙베리’의 암호화된 이메일과 문자메시지가 국가 보안에 위협이 된다고 주장해 왔다.

이번 RIM의 데이터 검열 협조 방침은 인도 정부에 의해 먼저 알려졌다. 인도 정부는 지난 30일(현지 시각) 성명을 내고 RIM의 제안에 대해 밝혔다.

인도 내무부는 RIM의 보안 협조 범위 및 시기 등 구체적인 내용을 밝히지는 않았지만 RIM에게 60일 간의 유예기간을 준다고 밝혔다. 인도 정부는 이 기간 동안 RIM이 제시한 데이터 접근 솔루션을 검증할 계획이다.

인도 정부는 “RIM이 이해할만한 제안을 했다”며 “통신국이 관련 보고서를 제출할 때까지 내무부는 블랙베리의 안보 관련 문제를 재고할 것”이라고 설명했다.

RIM은 관련 사항에 대해 즉답을 피했다. 하지만 인도 정부 관계자에 따르면 “1일부터 실행되며 인도를 통하는 모든 통신 행위를 검열할 수 있는 방안을 제시해야 한다”며 “인도에 서버를 설치해야 한다”고 말했다.

[원문출처]

(보안닷컴 - 이성현기자)

<http://www.boan.com/news/articleView.html?idxno=2894>

SECTION 2. 보안취약점 정보(Vulnerability)

2.1 Adobe Flash Player 원격코드실행 취약점 주의

□ 개요

- o Adobe Flash Player에 대한 임의의 코드 실행이 가능한 취약점[1, 2]
- o Adobe Reader와 Adobe Acrobat에도 영향을 미칠 수 있고, 최근 보급률이 증가된 안드로이드 기반 스마트폰의 Adobe Flash Player도 해당되므로 사용자 주의가 요구됨

□ 해당시스템

- o Adobe Flash Player 10.1.82.76 및 이전버전 (윈도우, 매킨토시, 리눅스, 솔라리스)
- o Adobe Flash Player 10.1.92.10 (안드로이드)
- o Adobe Reader 9.3.4 및 이전버전 (윈도우, 매킨토시, 유닉스)
- o Adobe Acrobat 9.3.4 및 이전버전 (윈도우, 매킨토시)

□ 임시 조치

- o 취약점에 의한 피해를 줄이기 위하여 사용자는 다음과 같은 사항을 준수해야함
 - 파일공유 기능 등을 사용하지 않으면 비활성화하고 개인방화벽을 반드시 사용
 - 사용하고 있는 백신프로그램의 최신 업데이트를 유지하고, 실시간 감시기능을 활성화
 - 신뢰되지 않는 웹 사이트의 방문 자제
 - 출처가 불분명한 이메일의 링크 클릭하거나 첨부 파일 열어보기 자제

□ 용어 정리

- o Adobe Flash Player : Adobe Flash 등에서 생성한 SWF 파일을 구동하는 프로그램
- o SWF(Shockwave Flash): Macromedia社가 개발한

멀티미디어 및 벡터 그래픽 파일 형식으로 주로 웹에서 사용됨

- o Adobe Acrobat : PDF 문서 편집/제작을 지원하는 상용 프로그램
- o Adobe Reader : PDF 문서의 편집 기능은 없이 보기/인쇄만 할 수 있는 무료 프로그램
- o PDF(Portable Document Format) : Adobe社가 개발한 다양한 플랫폼을 지원하는 전자문서 파일 형식

□ 참고 사이트

- [1] <http://www.adobe.com/support/security/advisories/apsa10-03.html>
- [2] <http://news.cnet.com/security/>

2.2 HP Data Protector Express Local Code Execution Vulnerability

□ 개요

- o HP Data Protector Express와 HP Data Protector Express Single Server Edition(SSE)에서 원격 공격자에 의해 서비스 분산 공격을 일으킬 수 있는 취약점이 발견됨. 이는 지정되지 않은 오류에 의해 발생하며 이로 인해 공격자는 취약한 시스템의 어플리케이션에 충돌을 일으키게 하거나 악성 코드를 실행 시킬 수 있음

□ 해당 시스템

- o 영향 받는 소프트웨어
 - HP Data Protector Express versions 3.x
 - HP Data Protector Express versions 4.x
 - HP Data Protector Express SSE versions 3.x
 - HP Data Protector Express SSE versions 4.x

□ 해결 방안

o version 4.0 SP1 build 56906 및 version 3.5 SP2 build 56936 설치

[참조사이트]

[1] <http://www.vupen.com/english/advisories/2010/2334>

[2] <http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=c02498535>

2.3 2010년 9월 MS 월간 보안 업데이트 권고

2010년 MS社에서 MS10- 061~ 069 9월간 보안패치 내용입니다. [9/01~ 9/21 기준]

[MS10- 061] 프린트 스피러 서비스(Print Spooler Service) 취약점으로 인한 원격코드실행 문제

[MS10- 062] MPEC- 4 코덱 취약점으로 인한 원격코드실행 문제

[MS10- 063] 유니코드 스크립트 프로세서(Unicode Scripts Processor) 취약점으로 인한 원격코드실행 문제

[MS10- 064] MS Outlook 취약점으로 인한 원격코드실행 문제

[MS10- 065] Microsoft Internet Information Services(IIS) 취약점으로 인한 원격코드실행 문제

[MS10- 066] Remote Procedure Call(RPC) 취약점으로 인한 원격코드실행 문제

[MS10- 067] WordPad Text Converters 취약점으로 인한 원격코드실행 문제

[MS10- 068] Local Security Authority Subsystem Service 취약점으로 인한 권한상승 문제

[MS10- 069] Windows Client/Server Runtime Subsystem 취약점으로 인한 권한상승 문제

[참조사이트]

<http://www.microsoft.com/technet/security/Bulletin/MS10-061~069.mspx>

2.4 마이크로소프트 ASP.NET 신규 취약점 주의

□ 개요

o MS ASP.NET에서 악의적으로 조작된 데이터를 처리하는 과정에서 ViewState 필드와 같이 암호화된 데이터나 Web.config와 같은 설정 파일의 내용이 노출되는 취약점[1][2]

o 공격자는 해당 취약점을 이용하여 취약한 웹서버의 시스템 정보 획득이 가능함

o 해당 취약점에 대한 정보가 공개되었으므로, ASP.NET이 운영 중인 웹서버에 대한 관리자의 주의가 요구됨

□ 해당 시스템

o 영향 받는 소프트웨어 [1]

- .NET Framework 1.0 SP3 on Windows XP Media Center and Tablet PC 2005

- .NET Framework 1.1 SP1 on Windows XP SP3, Professional x64 Edition SP2, Windows Server 2003 SP2, x64 Edition SP2, Windows Server 2003 SP2 for Itanium Systems, Windows Vista SP1, SP2, Windows Server 2008 SP0, SP2 for 32-bit, x64 Systems, Windows Server 2008 SP0, SP2 for Itanium Systems

- .NET Framework 2.0 SP2 on Windows XP SP3, Professional x64 Edition SP2, Windows Server 2003 SP2, x64 Edition SP2, Windows Server 2003 with SP2 for Itanium-based Systems

- .NET Framework 3.5 on Windows XP SP3, Professional x64 Edition SP2, Windows Server 2003 SP2, x64 Edition SP2, Windows Server 2003 with SP2 for Itanium Systems, Windows Vista SP1, SP2,

Windows Server 2008 for 32-bit Systems SP0, SP2, Windows Server 2008 for x64 Systems SP0, SP2, Windows Server 2008 for Itanium Systems, SP0, SP2 - .NET Framework 3.5 SP1 on Windows XP SP3, Professional x64 Edition SP2, Windows Server 2003 SP2, x64 Edition SP2, Windows Server 2003 with SP2 for Itanium Systems, Windows Vista SP1- SP2, Windows Server 2008 SP0, SP2 for for 32-bit, 64-bit Systems, Windows Server 2008 for Itanium Systems SP0, SP2

- .NET Framework 3.5.1 on Windows 7 for 32-bit Systems, x64-based Systems, Windows Server 2008 R2 for x64 Systems, Windows Server 2008 R2 for Itanium systems

- .NET Framework 4.0 on Windows XP SP3, Professional x64 Edition SP2, Windows Server 2003 SP2, x64 Edition SP2, Windows Server 2003 with SP2 for Itanium Systems, Windows Vista SP1, SP2, Windows Server 2008 Systems SP0, SP2, for 32-bit, 64-bit, Windows Server 2008 for Itanium Systems SP0, SP2, Windows 7 for 32-bit Systems, x64 Systems, Windows Server 2008 R2 for x64 Systems, Windows Server 2008 R2 for Itanium-based systems

□ 임시 해결 방안

o 현재 해당 취약점에 대한 보안업데이트는 발표되지 않았음

o 보안업데이트가 발표되기 전까지, 해당 운영체제 및 .NET프레임 워크 버전에 따라 MS 홈페이지에서 제공하는 임시 해결 방안을 적용하여 취약점으로 인한 피해를 예방함

※ <http://www.microsoft.com/technet/security/advisory/2416728.msp>

o KrCERT/CC 홈페이지 및 윈도우 보안 업데이트를 주기적으로 확인하여, 해당 취약점에 대한 보안 업데이트 발표 시 신속히 업데이트를 적용하도록 함

□ 참고 사이트

[1] <http://www.microsoft.com/technet/security/advisory/2416728.msp>

[2] <http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-3332>

2.5 월간동향 및 허니넷/트래픽 분석

□ 핫 이슈

MS 윈도우의 일부 응용프로그램이 동적 라이브러리 파일의 경로를 적절하게 검증하지 않아 원격 악성코드실행을 통한 개인정보 유출 및 DDoS 공격에 악용될 위험 증가, 인터넷 이용자는 자신의 PC가 사이버 공격에 악용되지 않도록 출처가 불분명한 이메일 열람, 네트워크 공유폴더 및 USB 등 사용에 주의가 필요함.

※ 주요 취약점, 웜·바이러스

제 목	영향받은 제품 / 사용자	영향력 / 예방 및 대책
예를 쉼타임 플레이어 플러그인 실행 취약점 주의	Windows IE 6 이상의 쉼타임 플레이어 버전 7.x, 6.x	<ul style="list-style-type: none"> ○ 인터넷 사용자가 공격자가 악의적으로 개설한 사이트에 접속한 일 경우 예를 쉼타임 플레이어에 대한 임의의 코드 실행이 가능한 취약점 <ul style="list-style-type: none"> ● 애플리케이션의 정식 보안업데이트는 발표되지 않음 ○ 쉼타임 플레이어 ActiveX 컨트롤 실행 중지를 위한 KB Bit 설정 등 임시조치
DLL 하이재킹 취약점으로 인한 악성코드 감염 주의	DLL을 안전하지 않은 방식으로 로드하는 MS Windows의 모든 응용프로그램 (KrCERT/CC 보안공지 참조)	<ul style="list-style-type: none"> ○ 일부 응용프로그램에서 로드하는 라이브러리 파일의 경로 불충분하게 검증함으로써 악성코드 실행 취약점이 발생 ○ WebDAV와 원격 네트워크 공유로부터 라이브러리가 로딩되지 않도록 설정, WebClient 서비스 비활성화
(MS 보안업데이트) 2010년 8월 MS 정기 보안업데이트 권고	Windows XP, Vista, 7 등 (KrCERT/CC 보안공지 참조)	<ul style="list-style-type: none"> ○ 최신 MS 보안업데이트 설치 (MS10-047) Windows Kernel 취약점으로 인한 권한 상승 문제 (MS10-048) Windows 커널 모드 드라이버 취약점으로 인한 권한상승 문제 (MS10-050) Windows Movie Maker 취약점으로 인한 플러그인 실행 문제 (MS10-053) Internet Explorer 누락 업데이트 등

※ 통계 분석

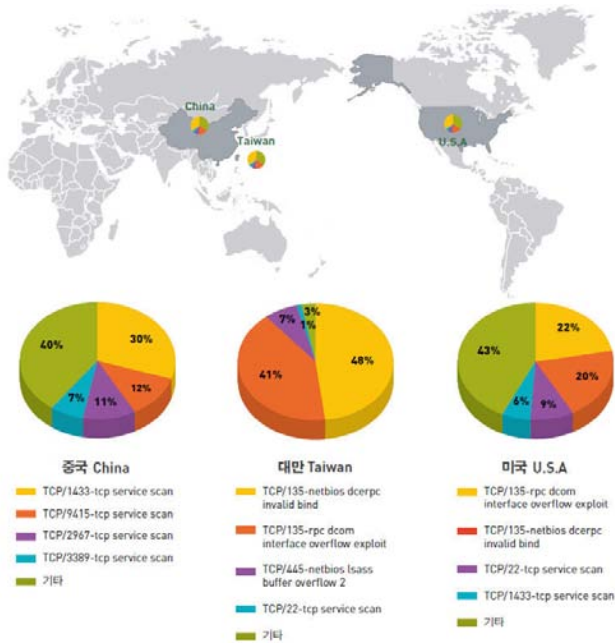
● 웜·바이러스 피해신고는 전월에 비하여 12.7% 감소

● 해킹신고 처리는 전월대비 26.5% 증가 (스팸 릴레이, 단순침입시도, 기타해킹, 홈페이지 변조는 각각 19.8%, 4.7%, 108.4%, 52.9% 증가, 피싱경유지는 24.2% 감소)

● 전 세계 악성 Bot 감염 추정 PC 대비 국내 감염률은 0.4%로 전월(0.5%) 대비 0.1% 감소

□ TOP 3 국가별 공격 유형

해외로부터 KISC 허니넷에 유입된 트래픽을 근원지 IP소재 국가별로 분석한 결과 중국으로부터 유입된 트래픽이 69.3%로 가장 많았으며 다음으로 대만(9.9%), 미국(7.1%) 순이었다. 중국으로부터의 트래픽은 TCP/1433 포트에 대한 서비스 스캔이 가장 많은 비중을 차지하였으며, 대만, 미국은 TCP/135 취약점 스캔이 가장 많았던 것으로 나타났다.



[원문출처]

(인터넷침해사고 동향 및 분석 월보 8월 中)

SECTION 3. 보안 팁(TECHNOLOGY TIP & IT GOVERNANCE)

3.1 악의적인 파일 업로드 취약점의 점검 및 보호대책

1. 취약성

대부분의 홈페이지는 사용자들을 위하여 여러 가지 종류의 게시판을 사용하고 게시판들은 파일을 첨부하는 기능 등 다양한 기능을 가지고 있는데 이런 게시판의 첨부파일 업로드를 기능을 악용하여 웹 서버의 권한이 노출될 수 있음.

2. 점검방법

- 먼저 사용자 게시판에 파일첨부 기능이 있는지 조사한다.
예) 게시판, 공개 자료실, 관리자 자료실, 이미지 자료실 등
- 첨부기능이 존재하는 경우, 확장자가 **jsp, php, asp, cgi** 등 **Server SideScript** 프로그램을 업로드하여 업로드가 가능한지 조사한다. 이 때 클라이언트 프로그램에서 **JavaScript, VBScript** 등의 스크립트로 파일첨부를 차단하는 경우 차단기능을 수정하여 파일을 첨부한다.
- 홈페이지에 있는 디렉터리 정보를 이용하여 첨부한 **Server Side Script**프로그램의 위치를 조사한 후 브라우저 주소 창에서 해당 프로그램을 실행한다.
- 실행 창에서 프로그램 소유자를 조사하거나 중요 정보가 존재하는지 조사한다.

3. 보호대책

- 일반대책

A. 파일 업로드 기능 제한

게시판 첨부 파일 업로드, 사진 업로드 모듈 등을 이용하여 악성 스크립트를 서버에 업로드 할 위험이 있습니다. 이를 실행시킬 수 있다면 해당 서버

는 물론 해당Application Server와 신뢰관계를 맺고 있는 서버들(예, Web DB서버, 내부 연동서버 등)들이 공격 당할 수 있는 가능성 있다.

B. Upload 파일을 위한 디렉터리에는 실행설정을 제거 (웹 서버)

Upload 파일을 위한 적용 디렉터리를 별도 생성하여 **httpd.conf**와 같은 웹 서버 데몬 설정파일에서 실행설정을 제거함으로써, **Server SideScript**가 Upload되더라도 웹 엔진이 실행하지 않게 환경을 설정함

C. 첨부파일의 확장자 필터링 처리

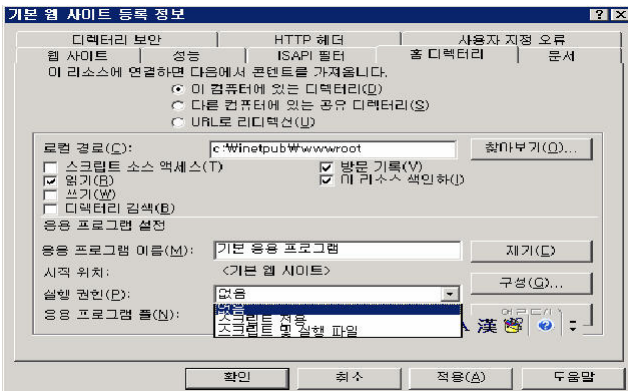
사용자가 첨부파일의 Upload 시도 시, Upload되는 파일의 확장자를 검토하여 적합한 파일인지를 검사하는 루틴을 삽입하여, 적합한 파일의 확장자 이외의 파일에 대해서는 업로드 되지 않도록 하며, 이런 필터링 규칙은 서버에서 구현해야 한다.

- 시스템 보안

웹 서버 구동은 반드시 관리자 권한이 아닌 일반 사용자 권한으로 구동하도록 한다. 외부사용자가 첨부파일을 이용하여 권한을 획득할지라도 최소한의 권한만을 사용할 수 있도록 한다.

A. IIS 보안 설정

설정→제어판→관리도구→인터넷 서비스 관리자 선택
해당 업로드 폴더에 오른쪽 클릭을 하고 등록정보→디렉터리→실행권한을 "없음"으로 설정



B. Apache 설정 (httpd.conf 설정 파일 수정)

디렉토리에 대한 문서 타입을 컨트롤하기 위해 Directory 섹션의 AllowOverride 지시자에서 FileInfo 또는 All추가

```
<Directory "/usr/local/apache">
AllowOverride FileInfo (또는 All) .....
.....
</Directory>
```

파일 업로드 디렉토리에 .htaccess 파일을 만들고 다음과 같이 AddType 지시자를 이용하여 업로드된 스크립트가 실행되지 않도록 설정한다. 또는 FileMatch 지시자를 이용하여 *.ph, *.inc, *lib Server Side Script 파일에 대해서 호출을 금지 시킨다.

```
<.htaccess>
<FilesMatch ".*(ph|inc|lib)">
Order allow, deny
Deny from all
</FilesMatch>
AddType text/html .html .htm .php .php3 .php4 .phtml .phps .in .cgi .pl .shtml .jsp
```

※ 주의사항

1. Apache 서버의 경우 AllowOverride 지시자를 변경 시 apache restart가 필요하다.
2. 파일 업로드 되는 디렉토리에 운영에 필요한 Server Side Script가 존재하는지 확인한다. 파일 다운로드 프로그램이 아닌 직접 URL 호출을 통해 파일을 다운받는 경우 FileMatch 지시자를 사용하면

차단 설정한 확장자의 파일 다운로드는 거부된다.

- 개발 언어별 대책

- 첨부 파일에 대한 검사는 반드시 Server Side Script에서 구현해야 한다.
- 첨부파일을 체크하여 특정 종류의 파일들만 첨부 가능하도록 하고 에러코드를 삽입하거나 첨부 파일을 처리하는 파일 업로드 프로그램(PHP, PHP3, CGI, HTML, JSP 등)에서 모든 실행 가능한 파일은 첨부할 수 없도록 한다.
- 프로그램에서 필터링을 할 경우 단순히 파일이름 기준으로 점검하지 말고 확장자 명에 대하여 검사 하되 대소문자를 모두 검사하도록 한다.
- 너무 작거나 큰 파일을 처리하는 로직을 포함해야 하고, 임시 디렉토리에서 업로드 된 파일을 지우거나 다른 곳으로 이동시켜야 한다. 또한 폰에서 어떠한 파일도 선택되지 않았다면, 파일 업로드에 사용되는 변수를 초기화 시켜주어야 한다.
- 웹 서버 엔진 설정 시 업로드 된 디렉토리의 Server Side Script 언어의 실행 권한을 제거하고 업로드 된 파일이름을 임의로 변경하여 저장하는 것도 안전한 방법이다.

3.2 오라클 보안 강화를 위한 Parameter 설정 방법

1. Data Dictionary 보호

Data Dictionary는 데이터베이스의 핵심 정보가 기록되는 곳으로 데이터 베이스의 구조, 객체에 대한 정의 및 공간 할당, 사용자, 롤(role), 권한, 감사와 같은 정보들을 제공한다. Data Dictionary는 테이블의 형태로 제공되며 데이터베이스 엔진에서 관리하여 사용자가 직접 변경할 수 없도록 되어있다. 또한 Data Dictionary는 대부분 DBA_, ALL_, USER_ 로 시작하는 접두어를 가지고 있어 구분하기 쉽다.

이러한 Data Dictionary는 'DROP ANY TABLE' 시스템 권한 가진 사용자가 악의적으로 Data Dictionary 테이블의 삭제가 가능하므로 오라클에서 제공하는 파라미터를 변경하여 DBA 권한으로 접속한 사용자가 Data Dictionary의 ANY 시스템권한을 사용할 수 있도록 해야 한다.

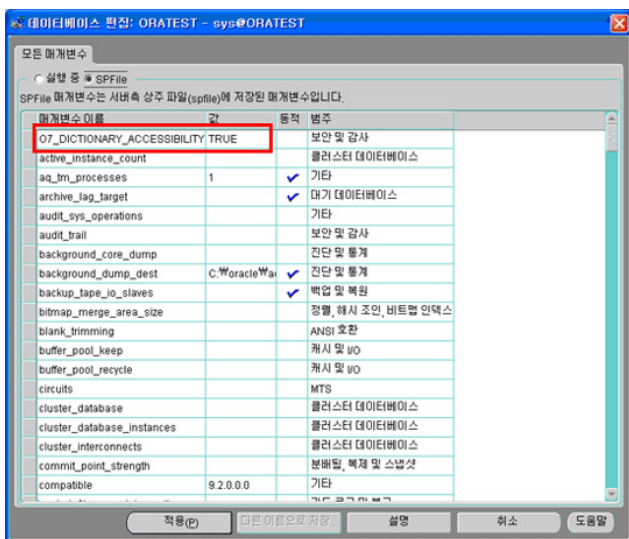
**** 파라미터 파일**
 오라클 데이터베이스 인스턴스의 초기화 설정에 사용되며 텍스트 형식의 PFILE과 바이너리 형태인 SPFILE이 존재한다. PFILE은 init<sid>.ora와 같은 이름으로 SPFILE은 spfile<sid>.ora 같은 이름으로 각각 생성되며 PFILE과 SPFILE파일이 모두 존재할 경우 SPFILE파일이 우선순위를 가진다. Oracle 9i에서는 디플트 설치 시 기본적으로 SPFILE을 이용하게 된다. OS별 파라미터 파일의 경로는 다음과 같다.

OS	경로
Windows	\$ora_home/database/spfile<sid>.ora
Unix/Linux	\$ora_home/dbs/spfile<sid>.ora

OEM(Oracle Enterprise Manager)을 이용하여 파라미터 파일을 확인하고 설정하기 위해서는 다음과 같은 방법을 이용한다.

- ① OEM에서 [데이터베이스] -> [세부정보보기/편집] -> [데이터베이스 편집] -> [모든 초기화 매개변수.] 창을 열어 [모든 매개변수] 탭을 확인하면 다음과 같이 현재 적용된 모든 파라미터의 값을 확인할 수 있다.

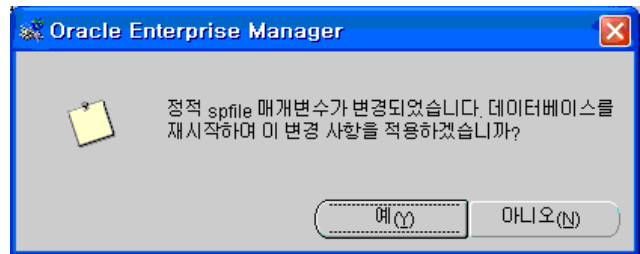
Data Dictionary와 관련된 파라미터는 **7_DICTIONARY_ACCESSIBILITY**으로 해당 값을 **FALSE**로 설정하여 Data Dictionary를 보호해야 한다.



- ② [모든 매개변수] 탭에서 [SPFILE]을 선택하여 현재 구성파일(SPFILE)에 있는 O7_DICTIONARY_ACCESSIBILITY 파라미터의 값이 TRUE로 되어 있을 경우 이를 변경하여야 한다.

Oracle 9i 및 10g에서는 O7_DICTIONARY_ACCESSIBILITY 파라미터의 값이 기본적으로 FALSE로 설정되어 있으나 Oracle8i는 TRUE로 설정되어 있으므로 반드시 변경하여야 한다.

- ③ O7_DICTIONARY_ACCESSIBILITY 파라미터의 값을 변경한 후 [적용]을 누르면 다음과 같이 데이터베이스를 재 시작하라는 메시지가 뜬다. 이때 데이터베이스를 재 시작해야만 변경된 파라미터의 값이 적용된다.



참고로 SPFILE에서 동적 매개변수를 변경할 경우 현재 실행중인 메모리에 즉시 반영이 되고 동시에 SPFILE에 저장되나 O7_DICTIONARY_ACCESSIBILITY와 같은 정적 매개변수의 값이 변경된 경우 변경된 값은 SPFILE파일에만 저장되므로 데이터베이스를 재 시작하여 변경된 값을 적용해야 한다.

2. 원격 인증기능 설정

오라클에서 지원하는 원격인증 기능이 활성화되면, 원격의 클라이언트는 오라클 데이터베이스에 접속할 수 있도록 허용된다. 즉, 데이터베이스는 적절하게 인증된 (클라이언트 자체OS의 인증) 모든 클라이언트들을 신뢰한다. 그러나 PC와 같은 클라이언트의 경우 Virus, Worm, Backdoor 등이 설치되어 있을 수 있어 데이터베이스에 접속할 경우 적절한

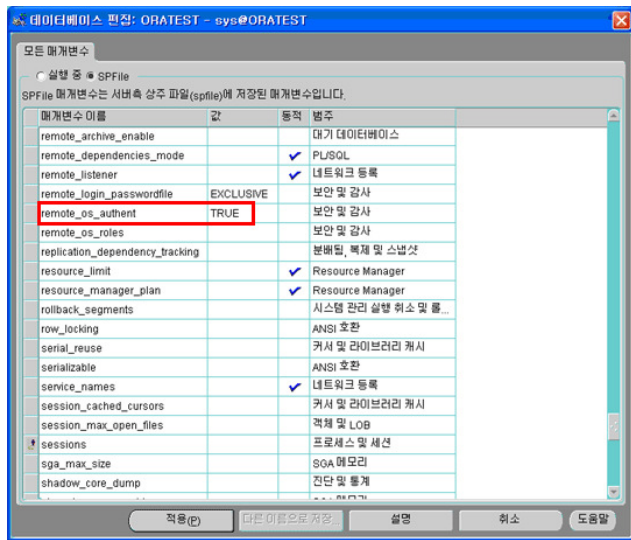
인증여부를 보장할 수 없어 보안이 대단히 취약해진다.

이러한 원격 인증기능을 비활성화시켜 오라클 데이터베이스에 접속하는 클라이언트는 Server- Based 인증(데이터베이스 어플리케이션의 인증)을 하도록 파라미터를 변경하여 보안을 강화하여야 한다.

OEM(Oracle Enterprise Manager)을 이용하여 파라미터 파일을 확인하고 설정하기 위해서는 다음과 같은 방법을 이용한다.

① OEM에서 [데이터베이스] -> [세부정보보기/편집] -> [데이터베이스 편집] -> [모든 초기화 매개변수...] 창을 열어 [모든 매개변수] 탭의 구성파일(SPFIL)을 선택한 후 파라미터 값을 확인한다.

원격 인증기능과 관련된 파라미터는 **REMOTE_OS_AUTHENT**으로 해당 값을 **FALSE**로 설정하여 OS인증이 아닌 오라클 어플리케이션의 인증을 받도록 설정한다.



Oracle 9i 및 10g 에서는 O7_DICTIONARY_ACCESSIBILITY 파라미터와 같이 REMOTE_OS_AUTHENT 파라미터의 값이 기본적으로 FALSE로 설정되어 있으나 Oracle8i는 TRUE로 설정되어 있으므로 반드시 변경하여야 한다.

② REMOTE_OS_AUTHENT 파라미터의 값을 변경

한 후에는 Data Dictionary 를 위한 파라미터 변경과 마찬가지로 데이터베이스를 재시작하여 변경된 파라미터값을 적용하면 된다.

3. Listener 의 설정 제한

Listener는 오라클 데이터베이스에 원격의 클라이언트가 접속할 수 있도록 실행되는 프로세스이며 클라이언트측의 요청을 받아 실제 쿼리문을 수행하는 서버프로세스를 생성하게 된다.

그러나 Listener의 패스워드는 디폴트로 설정되어 있지 않아 오라클의 Service Name을 알 경우 공격자에 의하여 Listener프로세스가 시작/정지 또는 재설정될 수 있다.

**** Service Name**
하나의 오라클 서버에 여러 DBMS프로세스(인스턴스)가 동작할 경우 이를 구별하기 위해 하나의 인스턴스를 Service Name으로 나타내게 된다. 이러한 Service Name은 sid, 서버IP, 접속 프로토콜 등의 정보로 구성이 되며 TNSNAME.ORA 파일에 의해서 정의되게 된다.

이러한 Listener에 패스워드를 설정하여 임의의 공격자가 Listener를 정지시켜 원격의 사용자가 오라클에 접속하지 못하게 하는 것을 방지하여야 한다. Listener에 패스워드는 LSNRCTL 유틸리티의 change_password 명령어를 이용하여 설정이 가능하며 설정된 패스워드는 LISTENER.ORA파일에 암호화되어 저장되게 된다.

Listener에 패스워드를 설정하기 위해서는 LSNCTL 유틸리티를 사용하며 다음과 순서로 진행된다.

```
OS> lsnrctl LSNRCTL> set current_listener LISTENER
LSNRCTL> set save_config_on_stop on
LSNRCTL> change_password
Old password: 처음의 경우 enter
New password: *****
Reenter new password: *****
```

위와 같이 설정한 후 Listener에 설정된 내용을 확인하기 위해서는 \$ORACLE_HOME/network/admin/listener.ora 경로에 존재하는 LISTENER.ORA파일을 텍스트에디터를 이용하여 확인해 보면 된다.

LISTENER.ORA파일에 다음과 같이 설정되어 있을

경우 Listener의 시작 및 정지 시에 패스워드를 물어보게 된다.

```
SAVE_CONFIG_ON_STOP_LISTENER = ON
PASSWORDS_LISTENER = 2D6C48144CF753AC
```

또한 Listener의 설정파일인 LISTENER.ORA은 LSNRCTL 유틸리티의 SET 명령어를 사용하여 수정이 가능하므로 다음과 같은 파라미터를 수정하여 원격에서 LSNRCTL 유틸리티를 사용한 Listener의 설정을 변경할 수 없도록 해야 한다.

Listener의 설정을 변경하기 위해서는 OS상에서 LISTENER.ORA파일을 텍스트 에디터로 열어 수정해야 한다.

```
ADMIN_RESTRICTIONS_listener_name=ON
```

4. 접근 IP 대역 제한

오라클에서 임의의 사용자에게 의한 원격 접속을 차단하기 위해 Listener의 IP 접근제한을 설정할 수 있다. 특정 클라이언트에서의 접근만 가능하도록 접근 가능 IP를 설정하여 불필요한 외부의 사용자가 접근하는 것을 차단한다.

환경설정 파일에서 접근 가능한 IP 대역과 접근 불가능한 IP대역을 설정하여 네트워크 접근통제를 할 수 있으며 Oracle 8i 는 **\$ORACLE_HOME/network/admin/protocol.ora** 파일에서, Oracle9i 에서는 **\$ORACLE_HOME/network/admin/sqlnet.ora** 파일에서 설정을 한다.

SQLNET.ORA 및 PROTOCOL.ORA파일을 OS상에서 텍스트 에디터로 열어 다음과 같이 편집하여 설정을 한다.

```
TCP.VALIDNODE_CHECKING = YES
TCP.INVITED_NODES=(접속을 허용할 ip)
TCP.EXCLUDED_NODES =(접속을 차단할 ip)
```

tcp.validnode_checking를 YES 로 설정한 후 접속을 허용·차단할 IP 또는 호스트 이름을 ','를 구분자로 하여 넣어주면 된다.

다음 예제와 같이 접근통제를 할 IP, 및 네트워크 대역을 넣어 설정할 수 있다.

```
TCP.VALIDNODE_CHECKING = YES
TCP.INVITED_NODES =(192.168.100.12, 192.168.100.13, dbms.com)
TCP.EXCLUDED_NODES =(192.168.200.0)
```

tcp.invited_nodes 만을 사용할 경우 허용된 IP에서만 접근이 되며 그 외의 IP에 대해서는 접근이 불가능하다. 이때 주의해야 할 것은 반드시 자기 자신의 IP를 추가해줘야 한다는 것이며 tcp.excluded_nodes를 같이 사용하여 차단할 IP를 추가하여도 된다.

SQLNET.ORA 및 PROTOCOL.ORA파일을 수정한 후에는 Listener를 재시작해야 해당 설정이 적용된다.

[자료출처]

(AhnLab Cocount 자료 中)

3.3 ARP Spoofing 대책 수립 방법

1. 취약성

ARP Spoofing 공격은 로컬 네트워크(LAN)에서 사용하는 ARP 프로토콜의 허점을 이용하여 자신의 MAC(Media Access Control) 주소를 다른 컴퓨터의 MAC 인 것처럼 속이는 공격이며, ARP Cashe 정보를 임의로 바꾼다고 하여 “ARP Cache Poisoning Attack” 이라고도 한다.

과거의 더미 허브 환경에서는 쉽게 Sniffing 이 가능하였지만, 최근에는 대부분 스위치 환경으로 네트워크를 구성하며, 이러한 스위치 환경에서는 해당 MAC 을 가진 컴퓨터에게만 패킷이 전달되므로, 더미 허브 환경에 비해 Sniffing 이 쉽지 않다. 하지만 공격자들은 자신의 MAC 주소를 라우터 또는 Sniffing 하고자 하는 대상 서버의 MAC 주소로 위장(ARP Spoofing) 하여 스위치 환경에서도 패킷을

Sniffing 할 수 있다. 그리고 이러한 Sniffing 수법은 이미 널리 알려져 있는 수법이다.

2. ARP Spoofing 공격 방지 대책

가. 시스템에서의 방지 대책

1) 정적인 ARP Table 관리

윈도우 계열에서 사용하는 시작/종료 스크립트에 정적으로 관리하고자 하는 시스템의 IP 와 MAC 주소를 입력하는 스크립트를 지정하거나, 리눅스 계열에서의 rc3.d 와 같이 시작 스크립트를 기동하는 곳에서 스크립트를 실행하도록 하여 재부팅 시에도 항상 정적인 ARP Table 이 관리 될 수 있도록 한다. 아래는 윈도우 계열의 경우에 ARP Table 을 정적으로 관리하는 명령이다. 특히, Gateway 의 IP 와 MAC 주소를 정적으로 고정시킴으로써 잘못된 ARP Reply 정보가 오더라도 이를 ARP Table 에 반영하지 못하도록 한다.

```
Example:
> arp -s 157.55.85.212 00-aa-00-62-c6-09 .... Adds a static entry.
> arp -a ..... Displays the arp table.
```

2) ARP Spoofing 서버로 악용되지 않도록 보안수준 강화

지금까지 신이교/접수되어 분석된 대부분의 ARP Spoofing 서버들은 본래의 용도 외에 침입자가 설치한 프로그램으로 인해 네트워크 트래픽 변조 서버로 악용된 것이었다. 그러므로 전체적인 보안수준을 강화하여, 공격자에게 악용되지 않도록 관리하여야 한다.

3) 중요 패킷 암호화

자신의 서버를 안전하게 구축하였다고 하더라도 공격자는 동일 서브네트워크내의 취약한 서버를 해킹하여 트래픽의 도청 및 변조가 가능하다. 따라서 네트워크를 통해 ID , Password, 주민번호, 금융정보 등 중요 데이터가 송수신 될 경우 이 정보 또한 공격자에 의해 유출되거나 변조 될 수 있으므로 이

러한 데이터에 대한 암호화가 바람직하다.

국내에서는 정보통신망 이용촉진 및 정보보호에 관한 법률에 의해 인터넷상에서 개인정보가 송수신되는 웹서버의 경우 보안서버를 구축하도록 규정하고 있음으로, 개인정보나 금융 정보가 네트워크를 통해 송수신되는 서버의 경우 SSL(Secure Socket Layer)방식 등을 이용하여 웹트래픽을 암호화 할 필요가 있다.

나. 네트워크 장비에서의 방지 대책

1) Mac Flooding 제어 및 정적인 MAC 주소 관리

이더넷 스위치 환경의 경우, 허브 환경과는 다르게 단순히 자신의 시스템만 Promiscuous Mode로 동작 시킨다고 해서 Sniffing 할 수 없기 때문에 다양한 방법들을 동원하여 Sniffing하게 된다. 그중에서 MAC Flooding (또는 Switch Addressable Memory)을 관리하는 자원을 고갈 시킴으로써 이더넷 프레임들을 모든 포트에 전송도록 하는 공격을 일컫는데, 시스코 장비의 예를 들면, 이 공격을 차단하기 위해서 아래의 그림과 같이 Port Security 라는 기능을 사용하는 것이 효과적이다.

```
Switch(config)# interface fastethernet 5/12
Switch(config-if)# switchport mode access
Switch(config-if)# switchport port-security
Switch(config-if)# switchport port-security maximum 5 → 최대 허용 MAC Address
Switch(config-if)# switchport port-security mac-address 1000.2000.3000 → 허용 MAC address
Switch(config-if)# switchport port-security violation [protect/restrict/shutdown] → 공격 위반시 Action
```

이 기능에는 물리적인 포트가 수용할 수 있는 MAC 주소의 개수를 지정하거나 사용 가능한 MAC 주소를 지정할 수 있으므로, 수 많은 MAC 주소가 발생해도 MAC의 관리에 어려움이 없게 된다.

IDC와 같이 시스템의 변경이 빈번하지 않은 환경이라면 충분히 효과적으로 활용 할 수가 있다.

참고로 MAC 주소의 정적인 관리는 양쪽의 시스템 모두에서 이루어 져야 한다. 만약 서버측에서만 정적인 ARP table을 관리한다면, ARP Spoofing 발

생 시 네트워크 트래픽의 흐름이 Client -> G/W -> S/W -> ARP Spoofing Server -> 피해서버 -> S/W -> G/W -> Client 순서로 이동하기 때문에, Sniffing 에 의한 정보유출이나 조작된 정보 입력 등의 피해가 발생할 수 있으므로, 반드시 네트워크 장비와 Host 시스템 양측 모두 정적인 ARP 관리가 되어야 효과적인 차단이 가능하다.

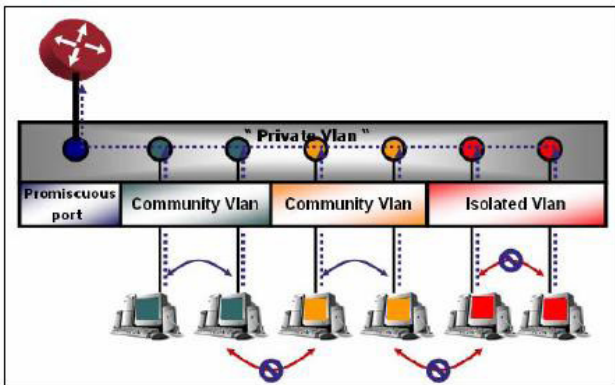
[자료출처]
(KrCert / CC 자료 中)

2) ARP 패킷 검사

앞서 살펴본 Port Security 기능과 유사한 기능으로써, 스위치에 수신되는 ARP 패킷들을 검사하여 마치 IP필터링을 하는 방화벽의 동작과 유사하게 지정된 경로로만 ARP 패킷이 전송되도록 하는 기능을 사용하는 것도 효과적이다. 시스코 장비의 경우 ARP Inspection이라고 한다.

3) 사설 VLAN 기능 활용

동일 서브네트워크지만, 지정된 호스트만 통신을 가능하도록 하는 사설 VLAN 기능을 활용하여 서로 통신할 필요가 없는 서버들을 관리하여 운용한다. 아래의 그림은 VLAN 개념도 이다.



예를 들어 서버호스팅의 경우 서로 다른 고객이 사용하는 서버가 같은 서브네트워크에 있다고 하더라도 서로 통신할 필요가 전혀 없기 때문에, 이러한 경우에는 고객별 사설 VLAN으로 격리한다면, 더욱더 안전한 시스템을 운용할 수 있다.