DS DATA

Security Consulting

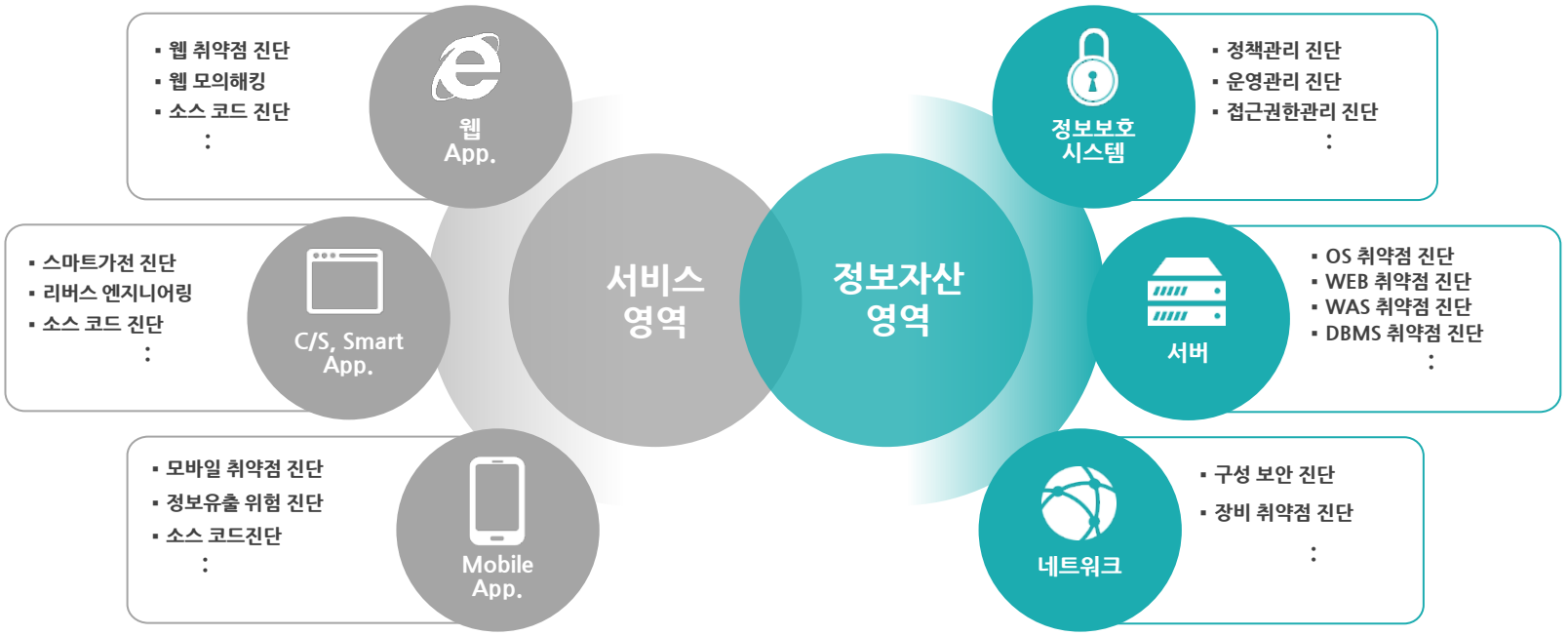
IT 인프라 취약점 진단 및 모의해킹

INDEX

01. 보안 컨설팅

개요

보안 취약점 진단 결과 및 모의해킹 결과를 토대로 전문 컨설턴트가 발견된 위협에 대한 대응방안을 제시하여 기업 및 기관의 보안 대응 전략 수립



01. 보안 컨설팅

관련 이슈

분류	내용	분류	내용
금융	• 금융부문 IT업무 전반에 대한 IT리스크 상시평가 강화 • (전자금융거래법 시행령 제11조의5) ② 법 제21조의3제1항에 따른 전자금융기반시설의 취약점 분석 · 평가는 사업연도마다 1회 이상 하여야 한다	여행/호텔	• 여름 휴가철을 맞아 국내 여행사의 웹사이트에 금융 악성코드 유포 • 웹사이트를 접속하는 사용자 대상으로 웹브라우저 및 플러그인 등의 취약점을 이용하여 사용자 PC에 몰래 악성코드 설치 • 감염된 악성코드는 가짜 인터넷 뱅킹 웹사이트로 접속되도록 파밍 유도, PC내 공인인증서를 검색/압축 후 외부로 전송하는 역할 수행 → 백신으로 검출되지 않는 경우도 있음
	• (전자금융감독규정 제37조의2) ③ 제1항에 따른 금융회사 및 전자금융업자 이외의 자의 경우 연 1회 이상(홈페이지는 6개월에 1회 이상) 실시하되 자체전담반을 구성하지 아니할 수 있다. 이 경우 취약점 분석·평가의 내용은 금융감독원장이 정한다.		• 일본 여행사 H.I.S 는 플래시가 실행되고 있는 페이지를 보는 것만으로도 바이러스에 감염되는 공격 받음. • 우리나라 여행사 홈페이지도 플래시 사용량이 많아 공격 받을 위험성이 큼
의료/제약	• 2021.12 제약사에 환자 20만명의 개인정보 유출로 검찰 송치		• 2017.09 하나투어 개인정보 3만 4천여건 유출로 정보보호 책임자에 벌금 1,000만원 확정 • DBMS를 관리하는 외주업체의 업무용 PC에 악성 원격제어 프로그램을 유포하는 수법을 통해, 고객 개인정보가 보관된 DB에 침입 • 유출내용 : 이메일, 여권번호, 주소, 전화번호, 성별 등 중요 개인정보
	• (의료기관 개인정보보호 가이드라인) 개인정보가 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 위험도 분석을 수행하고 필요한 보안조치 적용 등 대응방안을 마련하여야 한다. • 영상정보처리기기를 운영하는 의료기관은 개인영상정보가 분실·도난·유출·변조 또는 훼손되지 아니하도록 안전성 확보에 필요한 조치를 하여야 함		
	• 취급중인 개인정보가 인터넷 홈페이지, P2P, 공유설정, 공개된 무선망 이용 등을 통하여 열람권한이 없는 자에게 공개되거나 유출되지 않도록 개인정보처리시스템, 업무용 컴퓨터, 모바일 기기 및 관리용 단말기 등에 접근 통제 등에 관한 조치를 하여야 한다.		

정의

보안취약점(Vulnerability)이란?

보안취약점(vulnerability) 또는 취약점은 **보안상의 문제점을 안고 있는 컴퓨터 시스템의 약점**을 말하며
컴퓨터에 대한 범죄 행위 (해킹 등)나 자연 재해와 같이 외부로부터 가해지는 취약성 뿐만 아니라
컴퓨터 스스로가 만들어 낸 취약성까지도 포함한 것을 의미

⚠ 정보시스템에서 발생 할 수 있는 위협

- 불법적인 사용자의 접근을 허용
- 정상적인 서비스를 방해
- 중요 데이터의 유출, 변조, 삭제

01. 보안 컨설팅

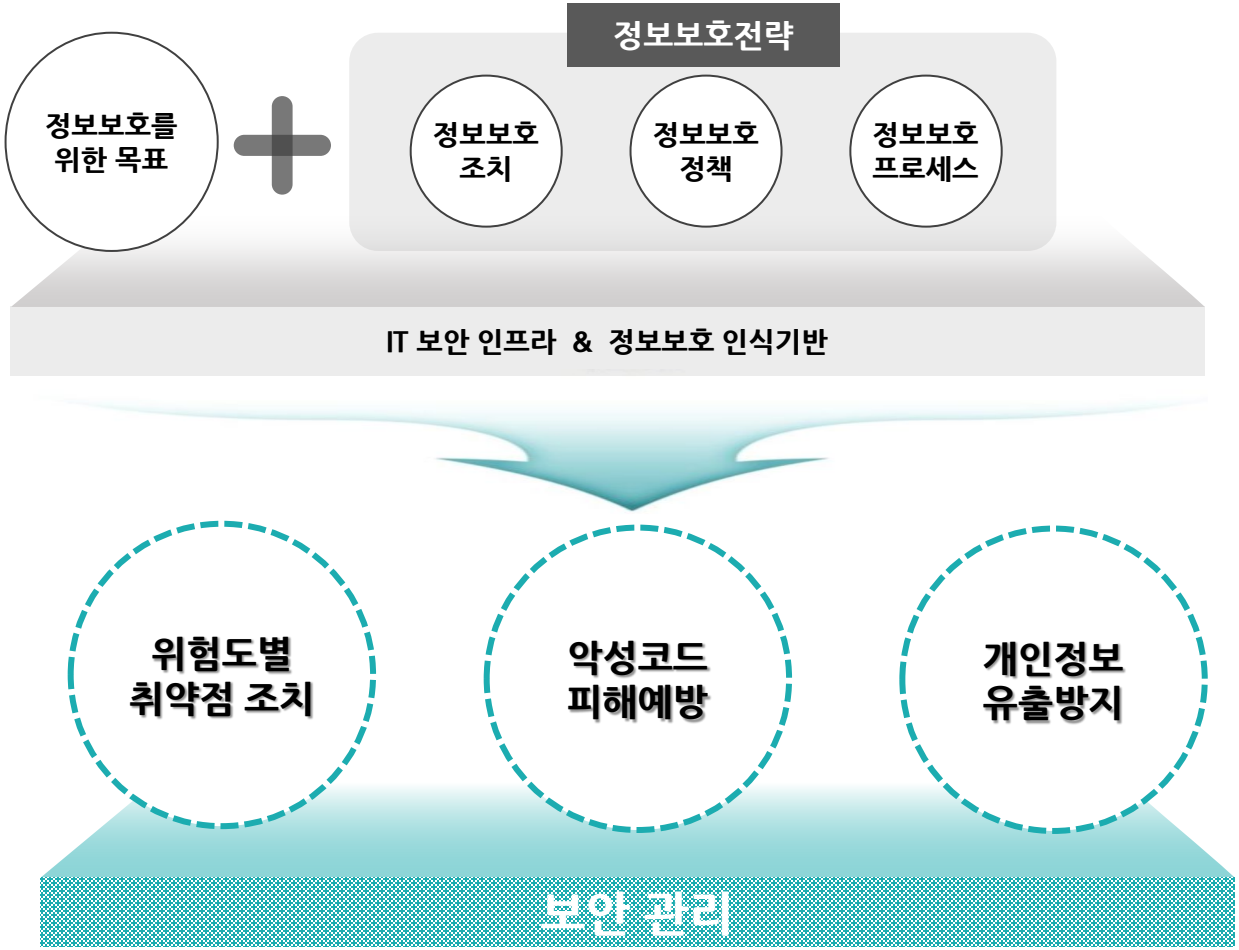
IT 인프라 자산 취약점 진단 범위

	IT 인프라 자산 시스템	웹 서비스	IT 인프라 주변기기
범위	• 사내 외부망/내부망에 위치한 고정된 전산 시스템 장비	• 공개/비공개 웹서버에서 서비스하고 있는 웹사이트	• 사무기기(프린터 등) • 이동성 PC(노트북)
진단대상	• Windows/Linux/Unix 및 해당 OS(운영체제)에서 돌아가고 있는 어플리케이션(서비스)	• 웹사이트(웹페이지)가 진단 대상으로 공격자가 웹브라우저 또는 프록시 툴을 이용하여 웹프로토콜(http/https)로 일으킬 수 있는 취약가능 부분	• 해당 주변기기의 OS
컴플라이언스	• ISO27001, PCIDSS, 기반시설 기술적 취약점(서버부문)	• OWASP 10 /SANSCWE 25/ 기반시설 기술적 취약점(웹서비스 부문)	• ISO27001, PCIDSS, 기반시설 기술적 취약점(서버부문)

01. 보안 컨설팅

기대 효과

보안컨설팅은 별도의 관리 인력 및 구축형 솔루션 없이 보안취약점 조치 등을 할 수 있게 결과를 제공합니다



01. 보안 컨설팅

수행절차 및 예상일정

IT인프라 취약점 진단 및 모의해킹은 다음 절차에 따라 수행합니다

[그림 1-1] IT인프라 취약점 및 모의해킹 진단 절차

IT인프라 취약점 진단 및 모의해킹 예상 일정은 다음과 같습니다 (진단 범위에 따라 상이)

구분	예상 일정
진단범위 협의 및 수행계획서 작성	3일
IT인프라 취약점 진단 수행	1일
IT인프라 취약점 진단 보고서 작성	7일
모의해킹 수행	1일
모의해킹 보고서 작성 및 최종 보고서 제출	7일

[표 1-1] IT인프라 취약점 및 모의해킹 예상 일정

02. 보안 취약점 진단

서비스 소개

IT인프라 취약점 진단은 Network 및 Server System, Web Application 그리고 Database 에 이르는 IT 인프라 환경 전반에 대한 보안 취약점 진단 및 조치 방법을 제시합니다.

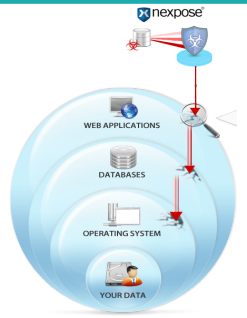
전체 가시성

- 조직 내 IT 인프라 전체에 대한 자산과 애플리케이션 검출
- 전체 취약점에 대한 통합 평가

위협 및 위험 검증

- 모의 해킹으로 취약점 검증
- RealRisk & RealContext로 지능형 평가

인공지능 스캔엔진



- 7만4천 개 이상의 취약점 진단 DB 보유
- 낮은 오탐률

02. 보안 취약점 진단

보안 취약점 검증 프로세스

발견된 보안취약점에 대한 검증 프로세스는 아래와 같습니다.

1. 공격 가능성 있는 보안취약점 파악

2. 취약점 진단 도구로부터 스캔 결과 자동 전송

4. 치료를 위해 검증된 취약점 우선순위 분석

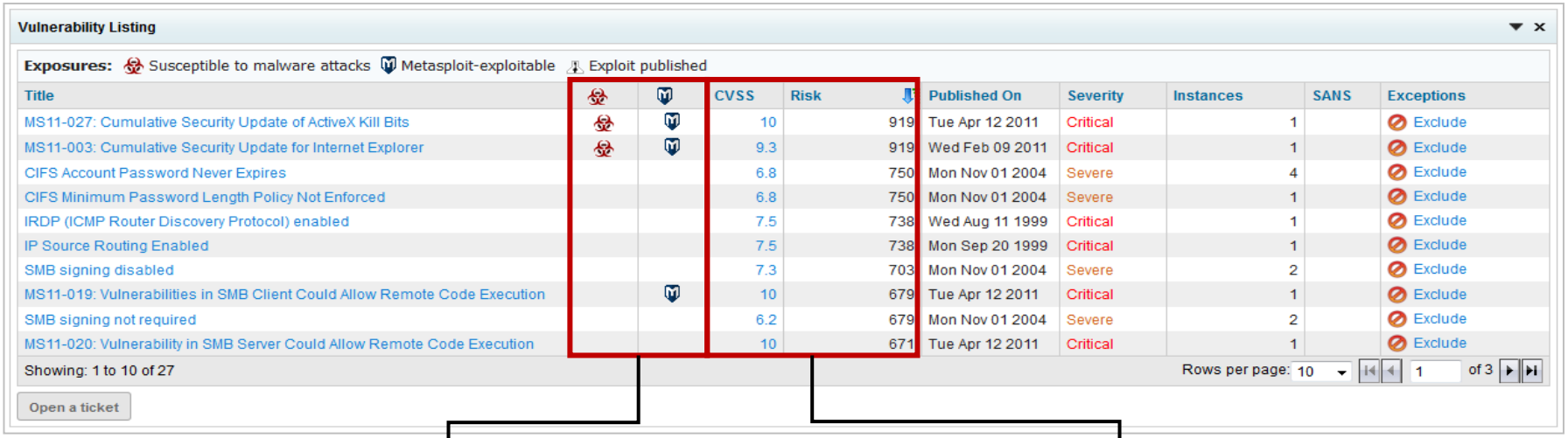
3. 공격 가능성 증명을 위해 간이 마법사 사용

02. 보안 취약점 진단

주요 기능

1. 위험의 우선순위 결정

위험의 우선순위를 결정하여 **고 위험의 취약점을 검출하고 즉각적인 조치를 취할 수 있도록** 결과 안내



고 위험 취약점에 즉각적인 조치

- 악성코드
- 취약점 공격

조치순서 설정을 위한 점수

- CVSS
- Risk

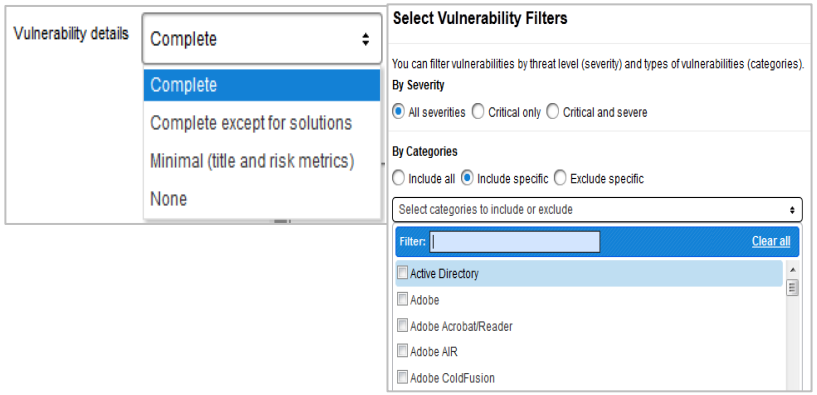
02. 보안 취약점 진단

주요 기능

2. 취약점 결과 산출 및 조치방법 제공

취약점 결과 정보를 여러 기준으로 분류하여 산출하고, 이에 대한 **해결 조치 방법을 순서 및 단계별 제공**

취약점 결과 산출



호스트필터 : IP, site, static group, dynamic group

취약점필터 : 150개의 카테고리 및 심각도에 따른 분류

취약점 세부정보 : 리포트 대상에 따라 4가지의 분류 옵션

예시> 위험 수준이 높은 웹 서버들로부터 발견된 심각도가 Critical인 모든 웹 관련 취약점만 추출해서 리포트를 생성

조치방안

3.1.1. For Microsoft Windows XP Professional SP2

These vulnerabilities can be resolved by performing the following 41 steps. The total estimated time to perform all of these steps is 19 hours 20 minutes.

Download and install Microsoft patch WindowsXP-KB936929-SP3-x86-ENU.exe (316.4 MB)

Estimated time: 20 minutes

Microsoft Windows XP Professional < SP3, Microsoft Winodws XP Home < SP3

Download and apply the upgrade from: http://download.microsoft.com/download/d/3/0/d30e32f8-418a-469d-b600-f32ce3edf42d/WindowsXP-KB936929-SP3-x86-ENU.exe

This will address the following 29 issues:

•Windows XP Service Pack 3 (KB936929) (servicepack-windows-xp-sp3)

•MS07-006: Vulnerability in Windows Shell Could Allow Elevation of Privilege (928255) (WINDOWS-HOTFIX-MS07-006)

•MS07-007: Vulnerability in Windows Image Acquisition Service Could Allow Elevation of Privilege (927802) (WINDOWS-HOTFIX-MS07-007)

Set the password expiration

Estimated time: 30 minutes

Microsoft Windows 2000 Professional, Microsoft Windows XP Professional

If the account is not used, delete or disable the account. If the account is a built-in system account such as the IUSR_ or IWAM_ accounts, enable the "User cannot change password" option to stop this vulnerability from being reported (Microsoft best practices dictate that built-in system accounts NOT be allowed to change their own passwords). Otherwise, ensure that the password expires by disabling the "Password never expires" option.

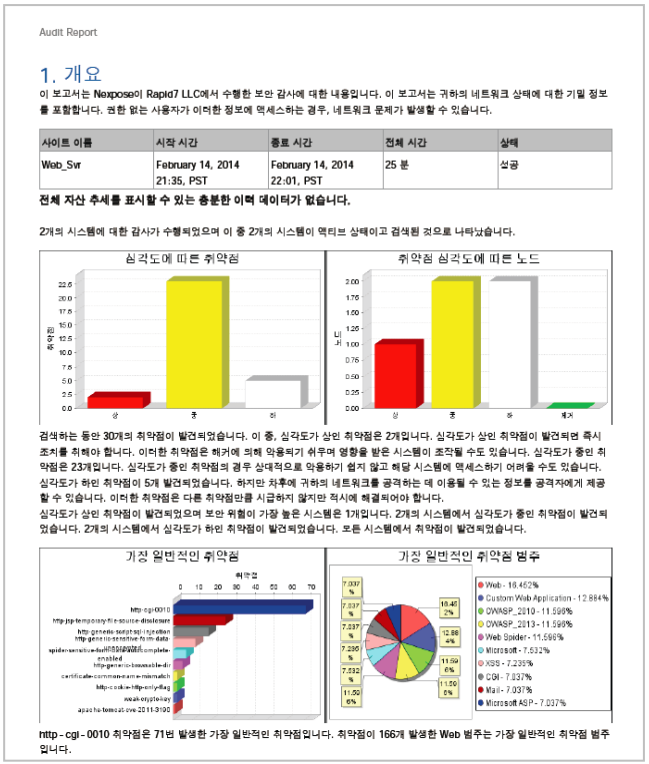
1. Right click on "My Computer"
2. Select "Manage"
3. Open the "Local Users and Groups" folder
4. Open the "Users" folder
5. Double-click on the desired user
6. Uncheck "Password never expires"

02. 보안 취약점 진단

보고서 제공

다양한 형태의 결과 리포트 제공으로 보안 취약점 결과 분석 및 관리 가능 (한글 지원 가능)

Audit Report (종합 결과보고서)


Audit Report

1. 개요

이 보고서는 Nexpose이 Rapid7 LLC에서 수행한 보안 감사에 대한 내용입니다. 이 보고서는 귀하의 네트워크 상태에 대한 기밀 정보를 포함합니다. 권한 없는 사용자가 이러한 정보에 액세스하는 경우, 네트워크 문제가 발생할 수 있습니다.

사이트 이름	시작 시간	종료 시간	전체 시간	상태
Web_Svr	February 14, 2014 21:35, PST	February 14, 2014 22:01, PST	25 분	성공

전체 자산 추세를 표시할 수 있는 충분한 이력 데이터가 없습니다.

2개의 시스템에 대한 감사가 수행되었으며 이 중 2개의 시스템이 액티브 상태이고 검색된 것으로 나타났습니다.

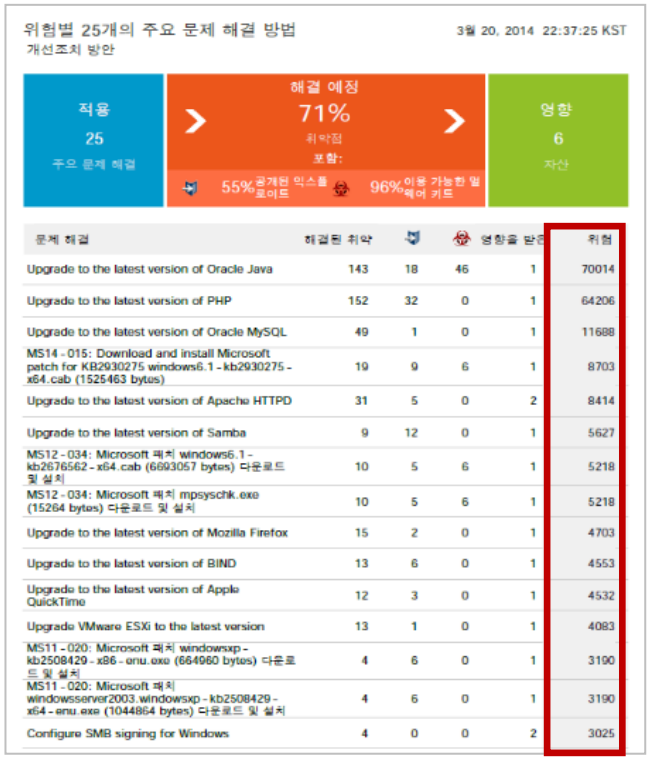
심각도에 따른 취약점 / 취약점 심각도에 따른 노드

검색하는 동안 30개의 취약점이 발견되었습니다. 이 중, 심각도가 상인 취약점은 2개입니다. 심각도가 상인 취약점이 발견되면 즉시 조치를 취해야 합니다. 이러한 취약점은 해커에 의해 악용되기 쉬우며 영향을 받은 시스템이 조작될 수도 있습니다. 심각도가 중인 취약점은 23개입니다. 심각도가 중인 취약점의 경우 상대적으로 악용하기 쉽지 않고 해당 시스템에 액세스하기 어려울 수도 있습니다. 심각도가 하인 취약점이 5개 발견되었습니다. 하지만 차후에 귀하의 네트워크를 공격하는 데 이용될 수 있는 정보를 공격자에게 제공할 수 있습니다. 이러한 취약점은 다른 취약점만큼 시급하지 않지만 적시에 해결되어야 합니다.
심각도가 상인 취약점이 발견되었으며 보안 위험이 가장 높은 시스템은 1개입니다. 2개의 시스템에서 심각도가 중인 취약점이 발견되었습니다. 2개의 시스템에서 심각도가 하인 취약점이 발견되었습니다. 모든 시스템에서 취약점이 발견되었습니다.

가장 일반적인 취약점 / 가장 일반적인 취약점 범주

http - cgi - 0010 취약점은 71번 발생한 가장 일반적인 취약점입니다. 취약점이 166개 발생한 Web 범주는 가장 일반적인 취약점 범주입니다.

Top Remediation Report


위험별 25개의 주요 문제 해결 방안

개선조치 방안

3월 20, 2014 22:37:25 KST

적용 25 주요 문제 해결 > 해결 예정 71% 취약점 포함: 55% 공개된 익스플로이드 96% 이용 가능한 멀웨어 키트 > 영향 6 자산

문제 해결	해결된 취약				위험
Upgrade to the latest version of Oracle Java	143	18	46	1	70014
Upgrade to the latest version of PHP	152	32	0	1	64206
Upgrade to the latest version of Oracle MySQL	49	1	0	1	11688
MS14 - 015: Download and install Microsoft patch for KB2930275 windows6.1 - kb2930275 - x64.cab (1525463 bytes)	19	9	6	1	8703
Upgrade to the latest version of Apache HTTPD	31	5	0	2	8414
Upgrade to the latest version of Samba	9	12	0	1	5627
MS12 - 034: Microsoft 패치 windows6.1 - kb2676562 - x64.cab (6693057 bytes) 다운로드 및 설치	10	5	6	1	5218
MS12 - 034: Microsoft 패치 mpsyschk.exe (15264 bytes) 다운로드 및 설치	10	5	6	1	5218
Upgrade to the latest version of Mozilla Firefox	15	2	0	1	4703
Upgrade to the latest version of BIND	13	6	0	1	4553
Upgrade to the latest version of Apple QuickTime	12	3	0	1	4532
Upgrade VMware ESXi to the latest version	13	1	0	1	4083
MS11 - 020: Microsoft 패치 windowsxp - kb2508429 - x86 - enu.exe (664960 bytes) 다운로드 및 설치	4	6	0	1	3190
MS11 - 020: Microsoft 패치 windowsserver2003.windowsxp - kb2508429 - x64 - enu.exe (1044864 bytes) 다운로드 및 설치	4	6	0	1	3190
Configure SMB signing for Windows	4	0	0	2	3025

진단 결과의 총평을 확인함으로 운영중인 자산의 취약점 현황 파악

고 위험 취약점에 대한 가시성 확대

02. 보안 취약점 진단

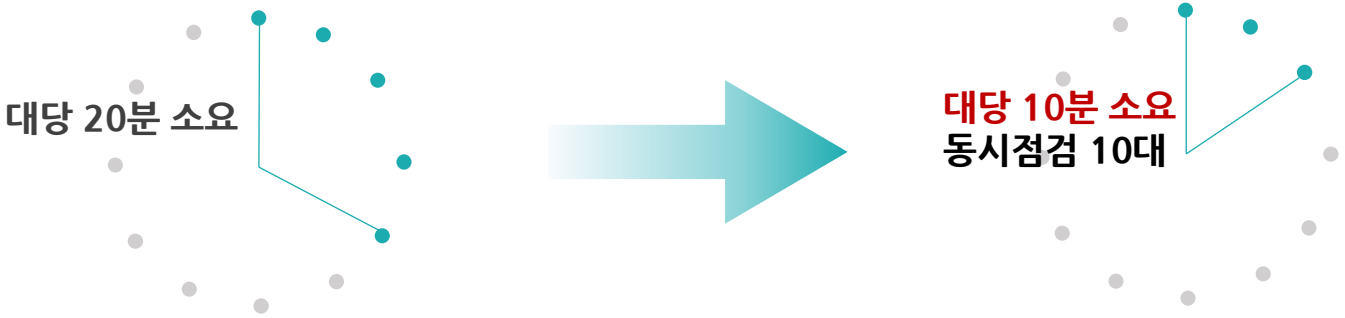
특장점

✓ 빠른 점검 속도

- 300대 기준 기존 점검방식 대비 20배 빠른 속도
- 최신 취약점 방식 포함하여 손쉽게 수행 가능
- 시간, 인력, 비용 절약 및 보안성 강화

✓ Agent-less 방식

- 별도의 에이전트 없이 대상 정보 입력만으로 원격을 통한 점검 가능
- 안전성, 편리성 제공



스크립트 작성 → 서버 배포 → 덤프파일 작성 → 보고서

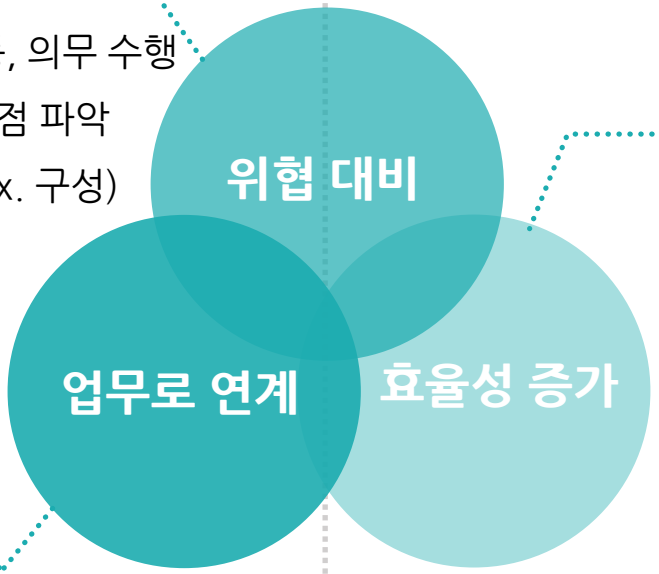
대상정보입력 → 점검수행 → 보고서

02. 보안 취약점 진단

기대 효과

가시성 확대

- ✓ 목표 지수를 이용하여 인지, 행동, 의무 수행
- ✓ 시스템 파악 및 네트워크의 취약점 파악
- ✓ “양호” 상태의 변경 원인 파악 (ex. 구성)



위험의 우선순위 관리

- ✓ 방어에 필요한 데이터 산출
- ✓ 단순 취약점만이 아닌, 이용가능성에 따른 치료방법의 우선순위 결정
- ✓ 위험 해결을 위한 수치화가 가능한 대책 마련

자동화

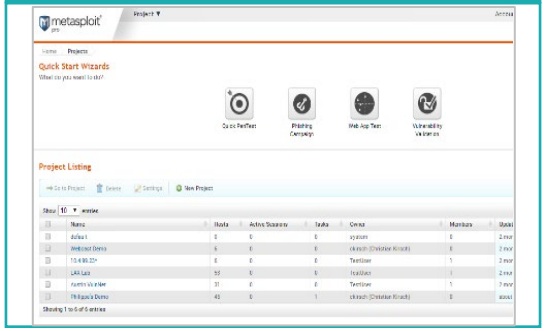
- ✓ 평가와 치료 주기의 자동화
- ✓ 데이터 정확성 증가를 위한 지속적인 평가 가능
- ✓ 업무 연관 IT 위험의 영향 산출

03. 모의해킹

서비스 소개

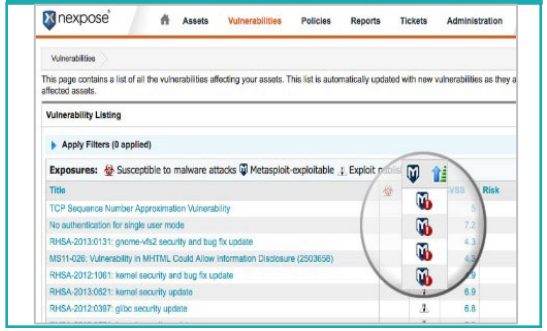
모의해킹은 보안 취약점 진단 결과를 토대로 **실제 공격자** 관점에서 전체 자산의 **보안 문제를 검증하여 취약점에 능동적으로 대처**하기 위한 모의 침투 테스트 입니다

침투 테스트



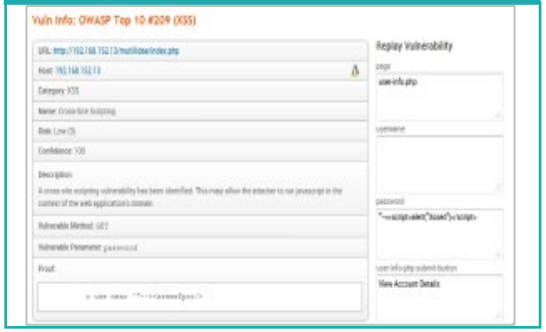
- 기업의 네트워크에 안전하게 공격 시뮬레이션
- 고급 회피 기술과 약한 인증 테스트

취약점 검증



- 실제 위험을 식별하고 설명
- 취약점 제거를 위해 Nexpose (보안 취약점 진단 툴)와 연동

웹 모의 침투 공격

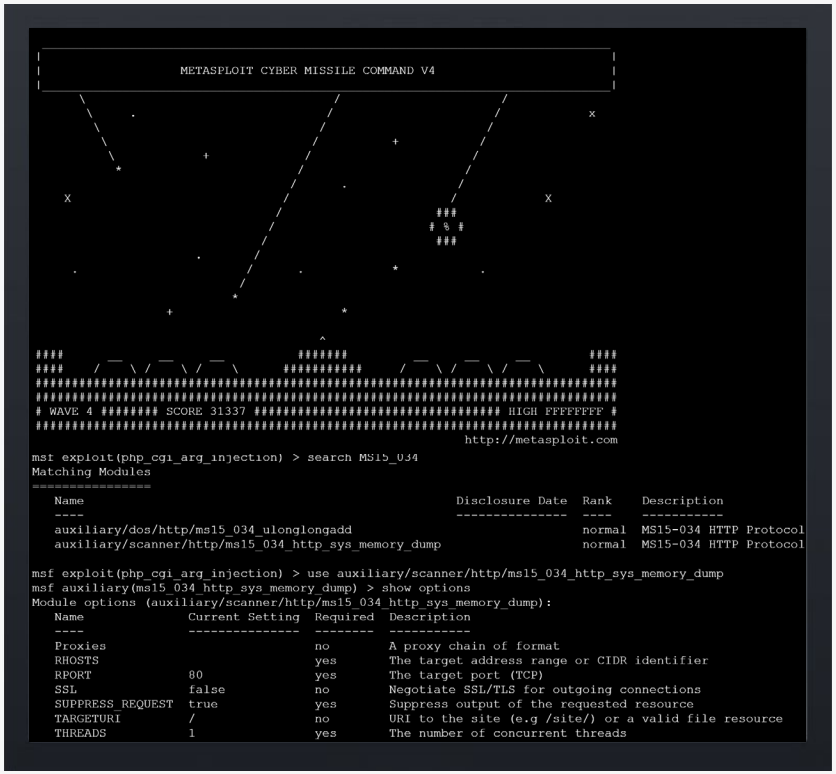


- 컴플라이언스 기반으로 발견된 취약점 검증 작업

03. 모의해킹

모의해킹 수행

실제 환경에서의 보안 테스트 및 위험 검증 및 외부 공격자와 같은 방법을 사용하여 침투 테스트 진행



- 안전한 **공격 시뮬레이션**
- 세계에서 가장 많은 품질이 **검증된 취약점 공격 모듈**을 선별
- Nexpose와 함께 사용하여 **보안 위험 상태를 검증**
- **실제 위험의 정확한 판별로 순위별 개선조치 업무 제시**
- Brute forcing, VPN pivoting 과 같은 **정교한 공격에 대한 대응 훈련**

03. 모의해킹

진단 범위

공격 범위를 최대화하여 서버 시스템, 네트워크 장비, RDBMS, 오피스 시스템, 이메일 사용자, 웹 애플리케이션 등에 대해 **빠르게 다중화된 공격을 수행하고 주요 정보 획득**

오피스 시스템 내부 사용자의 개인 사진, 파일, 문서 등을 획득할 수 있도록 공격 수행

데이타베이스

여러 경로를 통해 침투하여 결과적으로 DB에 있는 취약점을 이용하여 주요 정보 획득을 목적

서버시스템 취약점

내부 서버상의 OS 및 설치된 시스템의 공격 취약점 확인 후 공격을 수행하여 서버상의 주요 계정 및 정보를 취함

웹 애플리케이션

XSS, SQL 인젝션 등의 취약점을 이용하여 네트워크 침투하고, 피벗(Pivot) 기능을 이용하여 내부 시스템을 장악하기 위한 테스트 진행

네트워크 시스템

인프라의 핵심 구성으로 해커들에게 가장 많은 타겟이 되고 있으며, 장비운영체제 및 포트 중심으로 공격 수행

03. 모의해킹

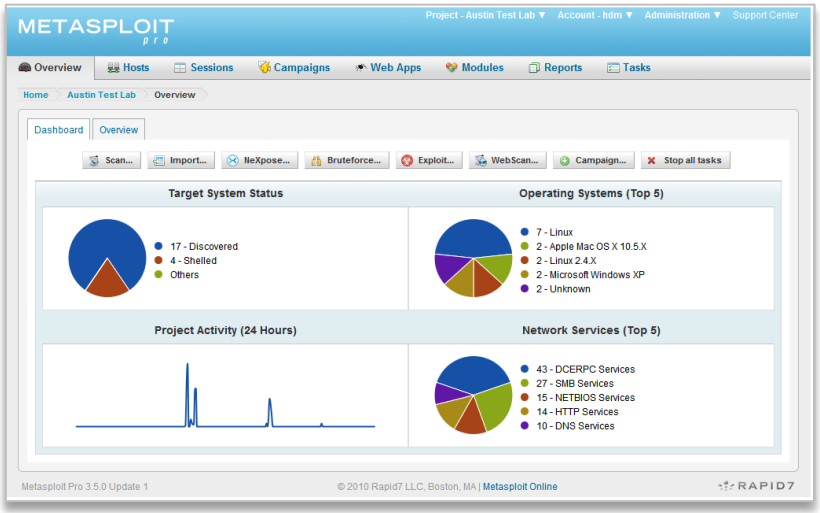
특장점

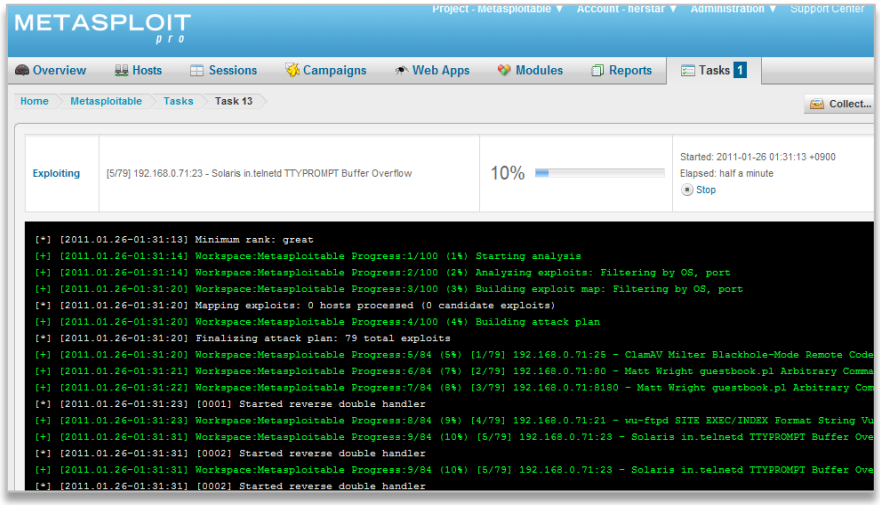
✓ 강력하고 신뢰도 있는 엔진 활용

- 20만 명의 커뮤니티 멤버가 제공하는 강력하고 신뢰도 있는 오픈 소스가 탑재된 Engine을 활용한 진단 결과 제공
- 광범위하고 품질이 증명된 exploit 모듈 제공

✓ 보안취약점 진단 결과와 연동

- 앞서 진행한 보안취약점 진단 결과와 연동 가능
- 최신 DB정보를 활용하여 도출된 취약점에 대한 침투 테스트 지원

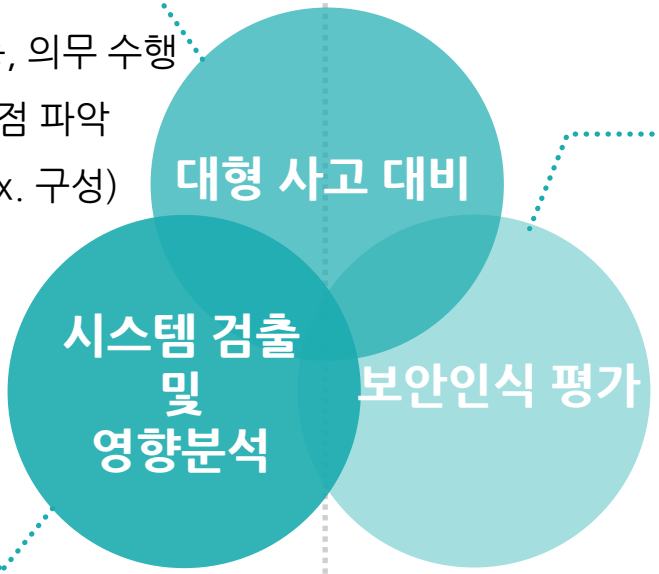




기대 효과

사전 위협 대비

- ✓ 목표 지수를 이용하여 인지, 행동, 의무 수행
- ✓ 시스템 파악 및 네트워크의 취약점 파악
- ✓ “양호” 상태의 변경 원인 파악 (ex. 구성)



위험의 우선순위 관리

- ✓ 방어에 필요한 데이터 산출
- ✓ 단순 취약점만이 아닌, 이용가능성에 따른 치료방법의 우선순위 결정
- ✓ 위험 해결을 위한 수치화가 가능한 대책 마련

자동화

- ✓ 평가와 치료 주기의 자동화
- ✓ 데이터 정확성 증가를 위한 지속적인 평가 가능
- ✓ 업무 연관 IT 위험의 영향 산출

04. 보안 컨설팅 산출물

IT 인프라 취약점 결과 보고서

IT 인프라 취약점으로 부터 생성된 보고서를 바탕으로 IP(자산)기반 및 상 취약점을 기준으로 결과 보고서 작성

1.1.1 127.0.0.1 (local)

1) MySQL 취약점

구분	상세 내용		
취약점 명	· MySQL Obsolete Version · MySQL dispatch_command() Multiple Format String Vulnerabilities · MySQL User Functions Buffer Overflow Vulnerability · MySQL User Functions Buffer Overflow Vulnerability 2 · MySQL Login Memory Disclosure Vulnerability · MySQL Multi-byte Encoding SQL Injection Vulnerability	위험도	상
상세 정보	· 3306 / TCP · Oracle MySQL 4.0.0		
취약점 설명	· MySQL 5.1 이전 버전은 제품에 대한 공식적인 지원기간이 종료 됨. 종료 이후의 심각한 보안문제 발생에 대하여 공식적인 보안패치를 제공하지 않음 · MySQL 4.0.0 ~ 5.0.83 버전의 dispatch_command 함수에서 Multiple format string 취약점으로 인해 원격 인증된 사용자가 서비스 거부를 일으킬 수 있음 · 특정 버전의 MySQL 은 user-defined 함수가 생성될 때 버퍼 오버플로우에 취약한 문제로 인증된 공격자가 MySQL 데몬을 제어할 수 있음 · MySQL 이 윈도우에서 실행 될 때, mysql.func 테이블에 삽입 권한이 있는 원격 인증된 사용자가 서비스 거부 및 임의의 코드를 실행할 수 있음 · MySQL 4.1.20 이전 4.1.x 및 5.0.22 이전 5.0.x 버전에서 SQL 인젝션 취약점은 SJIS, BIG5, GBK 와 같은 문자셋을 조작된 멀티 바이트 인코딩으로 공격자가 임의의 SQL 커멘드를 실행함		
해결방안	· MySQL 웹 사이트에서 최신 버전 다운로드 및 적용 http://dev.mysql.com/downloads/mysql		
주의사항	· 단, 업데이트 시 시스템/서비스에 미치는 영향도 확인 후 적용		
참고자료	CVE-2009-2446 CVE-2005-2572 CVE-2006-1516 CVE-2006-1517 CVE-2006-1518 CVE-2006-1931 CVE-2006-2426 CVE-2006-2453 CVE-2006-2458 CVE-2006-2753 http://www.mysql.com/support/eol-notice.html http://downloads.mysql.com/archives.php		

자산 별 취약점

자산이 가지고 있는 상 취약점 (상 취약점 기준: CVSS 7.5 이상)

자산에 설치 되어 있는 버전 정보 및 서비스 포트 정보

해당 취약점에 대한 상세 설명

취약점 해결 방안

취약점 조치 시 주의사항

해당 취약점에 대한 CVE 코드 및 참고 페이지 링크

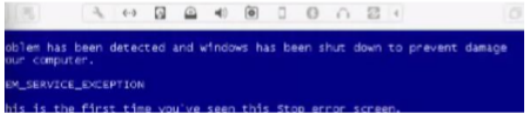
04. 보안컨설팅 산출물

모의해킹 결과 보고서

IT인프라 취약점 진단 결과에서 위험도가 높은 정보자산 및 취약점 중 대상을 선정하여 모의해킹 수행 후 결과 보고서 작성

1.1.1 127.0.0.1 (local)

1) MS15_034 (HTTP.sys 의 취약성으로 인한 원격 코드 실행 문제)

구분	상세 내용		
취약점 명	· MS15-034 HTTP Protocol Stack Request Handling HTTP.SYS Memory Information Disclosure/ Denial-of-Service	위험도	상
취약점 내용	· 이 취약점은 CVE-2015-1635 로 2015 년도에 발견되었으며 이 취약점을 이용하여, 해당 서비스에 대한 메모리에 실행코드를 삽입 하거나, 랜덤 값을 통한 시스템 메모리 정보 노출 및 DOS 공격이 가능 함. · 해당 취약점은 취약한 IIS 7.5 버전을 사용하며, 다음의 response 를 하는 것을 취약함의 증거로 확인 함 · HTTP/1.1 416 Content-Range: bytes 0-9/10 Content-Length: 10 [10 bytes FILE CONTENT HERE]		
발생가능 위험정보	· 이 취약점은 window 8.1/ windows server 에서 발생한다고, 알려져 있음 (단, Vmware 환경이 운영중이라면, 이 취약점 모듈을 통해 BSOD(blue screen of death)가 발생할 수 있으므로 주의해야 함) · HTTP.sys 가 특수하게 조작 된 HTTP 요청을 부적절하게 구문 분석 할 때 발생하는 원격 코드 실행 취약점이 HTTP 프로토콜 스택 (HTTP.sys)에 존재 함. 이 취약점을 성공적으로 악용 한 공격자는 시스템 계정의 컨텍스트에서 임의 코드를 실행할 수 있음		
검증관련 상세정보	· 실 대상 서버를 간접 exploit(공격)를 통해 해당 취약점에 대한 취약성이 있는지 검증을 수행한 화면으로 'Stand by...' 하여 메모리 덤프 파일 생성을 시도 하는 것을 확인 함 (실 서버 영향도를 고려하여 Stand by 확인 후 중지) · 또한 해당 자산은 IIS 기본 페이지가 활성화 되어 있으므로 비활성화 해야 함 (IIS 기본 페이지를 공격코드에 삽입하여 공격 코드를 실행할 수 있으며 이 공격명령이 정상적으로 수행되면 BSOD 가 발생될 수 있음) [+] Target may be vulnerable... [+] Stand by... · 참고: 테스트 서버 (맥북 내 가상머신으로 구동 중인 window server 2008R2)에서 MS15-034 취약점을 공격한 결과 이며 BSOD 가 되는 것을 확인 함  		
조치방안	· 보안 패치 적용 https://technet.microsoft.com/ko-kr/library/security/ms15-034.aspx 위 사이트에서 해당 자산에 맞는 버전의 보안 업데이트를 찾아 패치 함.		
주의사항	· 윈도우가 제공하는 보안 업데이트는 버전에 따라 중지가 되었을 가능성이 있음. · 해당 자산의 소프트웨어 엔지니어와의 충분한 협의 후 적용		

자산 별 모의해킹 수행

자산이 가지고 있는 상 취약점 (상 취약점 기준: CVSS 7.5 이상)

해당 취약점에 대한 상세 설명

해당 취약점으로 인한 발생 가능한 위험 정보

모의해킹 수행결과 (단, 모의해킹 진행 시 실 서버에 영향도를 고려)

취약점 조치 방안

취약점 조치 시 주의사항

감사합니다

DS data
Digital Security

Contact us.

Homepage :
https://www.dsdata.co.kr

Email :
sales@dsdata.co.kr

Tel :
031-698-2066