

# MS One-day 취약점 분석 방법론

제갈공맹

d7795gmail@gmail.com

# 목 차

- ▶ Zero-day & One-Day ?
- ▶ Microsoft Patch & CVE ?
- ▶ 분석 하기 전 사전 정보 수집
- ▶ MS11-002 분석
- ▶ 시연

# What is Zero-Day & One-Day?

## ▶ Zero-Day ?

- ▶ 컴퓨터 소프트웨어의 취약점을 공격하는 기술적 위협으로, 해당 취약점에 대한 패치가 나오지 않은 시점에서 이루어지는 공격

## ▶ One-Day ?

- ▶ 공격자가 이미 벤더 측에 제보를 하여 패치가 되었으나 Exploit 이 없는 상태를 의미

# Microsoft Patch

- ▶ Microsoft 는 매달 두 번째 화요일
- ▶ 보안 패치 공지 화면

## 2013 년 10 월 Microsoft 보안 공지 요약

게시된 날짜: 2013년 10월 9일 수요일 | 업데이트된 날짜: 2013년 10월 11일 금요일

버전: 1.1

이 공지 요약 목록에는 2013년 10월에 발표된 보안 공지가 포함되어 있습니다.

2013년 10월 보안 공지 발표와 함께 이 공지 요약이 2013년 10월 3일에 게시된 공지 사전 알림을 대체합니다. 보안 사전 알림 서비스에 대한 자세한 내용은 [Microsoft 보안 공지 사전 알림](#)(영문)을 참조하십시오.

Microsoft 보안 공지가 게시될 때 자동 알림을 받는 방법은 [Microsoft 기술 보안 알림](#)을 참조하십시오.

Microsoft는 2013년 10월 9일 오전 11:00(태평양 표준시, 미국 및 캐나다)에 이 공지에 대한 고객 문의 사항에 답변을 제공하는 웹캐스트를 진행합니다. [10월 보안 공지 웹캐스트에 지금 등록하십시오](#)(영문).

Microsoft는 월별 보안 업데이트와 동일한 날짜에 발표되는 비보안 업데이트와 보안 업데이트의 우선 순위를 고객이 결정하는 데 도움이 되는 정보도 제공합니다. 기타 정보 섹션을 참조하십시오.

# Microsoft Patches name

마이크로소프트

MS

해당 연도

-13

패치 나온 갯수

-088

# CVE란?

- ▶ Common Vulnerabilities and Exposures
- ▶ CVE 는 잘 알려진 보안취약점 및 노출된 정보를 모아둔 곳
- ▶ <http://cve.mitre.org>

# CVE names

Common  
Vulnerabilities and  
Exposures

해당 연도

패치 나온 갯수

CVE

-2013

-088

## New CVE-ID Syntax

The new CVE-ID syntax is variable length and includes:

CVE prefix + Year + Arbitrary Digits

**IMPORTANT:** The variable length arbitrary digits will begin at four (4) fixed digits and expand with arbitrary digits *only when needed* in a calendar year, for example, CVE-YYYY-NNNN and if needed CVE-YYYY-NNNNN, CVE-YYYY-NNNNNNN, and so on. This also means there will be no changes needed to previously assigned CVE-IDs, which all include 4 digits.

# 취약점 기본 정보를 얻는 방법

▶ <http://technet.microsoft.com/ko-kr/security/bulletin>

Security TechCenter

Bing으로 TechNet 검색



한국 (한국어) 로그인

홈 **보안 공지** 라이브러리 학습 다운로드 지원 커뮤니티

## 보안 공지

### 최신 릴리스

- 2013년 11월 Microsoft 보안 공지 요약  
Microsoft는 2013년 11월 정기 보안 업데이트 8건을 발표했습니다.

### 예정된 릴리스

- 차기 릴리스: 2013년 12월 11일

고객용 안전 및 보안센터에서 보다 일반적인 자료를 확인하거나 Microsoft Update에서 업데이트를 다운로드 하십시오.

### Related Links



#### 보안 공지 알림 받기

RSS, 인스턴트 메시지, 모바일 장치 또는 이메일 형식에 대한 안내를 받으십시오.



#### 보안 권고

공지가 필요하지 않지만 고객에게 영향을 줄 수 있는 보안 변경 사항을 확인하십시오.



#### Microsoft 보안 대응 센터(MSRC) 블로그 (영문)

공지 및 권고에 대한 자세한 내용은 MSRC 웹캐스트, 포스트 및 Q&A를 확인하십시오.



#### 취약점 보고 (영문)

보안 취약점에 대한 MSRC 조사에 의견을 제공해 주십시오.



#### 이전에 릴리스된 보안 공지 요약 읽기

지난 Microsoft 보안 공지 요약을 참조하십시오.



# 취약점 기본 정보를 얻는 방법

## 2013 년 11 월 Microsoft 보안 공지 요약

게시된 날짜: 2013년 11월 13일 수요일

버전: 1.0

이 공지 요약 목록에는 2013년 11월에 발표된 보안 공지가 포함되어 있습니다.

2013년 11월 보안 공지 발표와 함께 이 공지 요약이 2013년 11월 8일에 게시된 공지 사전 알람을 대체합니다. 보안 사전 알람 서비스에 대한 자세한 내용은 [Microsoft 보안 공지 사전 알람](#)을 참조하십시오.

Microsoft 보안 공지가 게시될 때 자동 알람을 받는 방법은 [Microsoft 기술 보안 알람](#)을 참조하십시오.

Microsoft는 2013년 11월 13일 오전 11:00(태평양 표준시, 미국 및 캐나다)에 이 공지에 대한 고객 문의 사항에 답변을 제공하는 웹캐스트를 진행합니다. [11월 보안 공지 웹캐스트에 지금 등록하십시오.](#)

Microsoft는 월별 보안 업데이트와 동일한 날짜에 발표되는 비보안 업데이트와 보안 업데이트의 우선 순위를 고객이 결정하는 데 도움이 되는 정보도 제공합니다. 기타 정보 섹션을 참조하십시오.

### 공지 정보

#### 요약

다음 표에는 이번 달의 보안 공지가 심각도 순으로 요약되어 있습니다.

영향을 받는 소프트웨어에 대한 자세한 내용은 다음 항목 영향을 받는 소프트웨어를 참조하십시오.

| 공지 번호                    | 공지 제목 및 요약   | 최대 심각도 및 취약점 영향                | 다시 시작 요구 사항 | 영향을 받는 소프트웨어                            |
|--------------------------|--|--------------------------------|-------------|---|
| <a href="#">MS13-088</a> | <p>Internet Explorer 누적 보안 업데이트(2888505)</p> <p>이 보안 업데이트는 Internet Explorer에서 발견되어 비공개적으로 보고된 취약점 10건을 해결합니다. 가장 위험한 취약점으로 인해 사용자가 Internet Explorer를 사용하여 특수하게 조작된 웹 페이지를 볼 경우 원격 코드 실행이 허용될 수 있습니다. 가장 위험한 취약점 악용에 성공한 공격자는 현재 사용자와 동일한 권한을 얻을 수 있습니다. 시스템에 대한 사용자 권한이 적게 구성된 계정의 사용자는 관리자 권한으로 작업하는 사용자에 비해 영향을 적게 받습니다.</p> | <a href="#">긴급</a><br>원격 코드 실행 | 재시작 필요      | Microsoft Windows,<br>Internet Explorer |

# 취약점 기본 정보를 얻는 방법

## Microsoft Security Bulletin MS13-088 - 긴급

### Internet Explorer 누적 보안 업데이트 (2888505)

게시된 날짜: 2013년 11월 13일 수요일

버전: 1.0

#### 일반 정보

##### 요약

이 보안 업데이트는 Internet Explorer에서 발견되어 비공개적으로 보고된 취약점 10건을 해결합니다. 가장 위험한 취약점으로 인해 사용자가 Internet Explorer를 사용하여 특수하게 조작된 웹 페이지를 볼 경우 원격 코드 실행이 허용될 수 있습니다. 가장 위험한 취약점 악용에 성공한 공격자는 현재 사용자와 동일한 권한을 얻을 수 있습니다. 시스템에 대한 사용자 권한이 적게 구성된 계정의 사용자는 관리자 권한으로 작업하는 사용자에 비해 영향을 적게 받습니다.

이 보안 업데이트의 심각도는 영향을 받는 Windows 클라이언트의 Internet Explorer 6, Internet Explorer 7, Internet Explorer 8, Internet Explorer 9, Internet Explorer 10 및 Internet Explorer 11에 대해 긴급이며 영향을 받는 Windows 서버의 Internet Explorer 6, Internet Explorer 7, Internet Explorer 8, Internet Explorer 9 및 Internet Explorer 10에 대해 중요합니다. 또한 영향을 받는 Windows 서버의 Internet Explorer 11에 대해서는 보통입니다. 자세한 내용은 이 섹션에서 **영향을 받는 소프트웨어 및 영향을 받지 않는 소프트웨어**를 참조하십시오.

이 보안 업데이트는 Internet Explorer가 CSS 특수 문자를 처리하는 방식, 인쇄 미리 보기를 생성할 때 특수하게 조작된 웹 콘텐츠를 처리하는 방식 및 메모리의 개체를 처리하는 방식을 수정하여 취약점을 해결합니다. 취약점에 대한 자세한 내용은 **취약점 정보**에서 각 취약점 항목의 자주 제기되는 질문 사항(FAQ)을 참조하십시오.

**권장 사항.** 대부분의 고객은 자동 업데이트를 사용하고 있기 때문에 따로 조치를 취할 필요가 없습니다. 이 보안 업데이트가 자동으로 다운로드되고 설치됩니다. 자동 업데이트를 사용하고 있지 않은 고객은 수동으로 업데이트를 확인하고 이 업데이트를 설치해야 합니다. 자동 업데이트의 특정 구성 옵션에 대한 자세한 내용은 [Microsoft 기술 자료 문서 294871](#)을 참조하십시오.

관리자 및 기업 설치의 경우나 이 보안 업데이트를 수동으로 설치하려는 최종 사용자의 경우에는 고객이 업데이트 관리 소프트웨어를 사용하거나 [Microsoft Update](#) 서비스를 통해 업데이트를 확인하여 업데이트를 즉시 적용하는 것이 좋습니다.

이 공지 뒷부분에 있는 **검색, 탐지 도구 및 지침** 섹션도 참조하십시오.

↗ 섹션 맨 위로 이동

#### 기술 자료 문서

| 기술 자료 문서     | 2888505 |
|--------------|---------|
| 파일 정보        | 예       |
| SHA1/SHA2 해시 | 예       |
| 알려진 문제점      | 없음      |

# 취약점 기본 정보를 얻는 방법

## 영향을 받는 소프트웨어

| 운영 체제                                       | 구성 요소                         | 최대 보안 영향 | 전체 심각도 | 대체된 업데이트          |
|---|-------------------------------|----------|--------|-------------------|
| Internet Explorer 6                         |                               |          |        |                   |
| Windows XP 서비스 팩 3                          | Internet Explorer 6 (2888505) | 원격 코드 실행 | 긴급     | MS13-080의 2879017 |
| Windows XP Professional x64 Edition 서비스 팩 2 | Internet Explorer 6 (2888505) | 원격 코드 실행 | 긴급     | MS13-080의 2879017 |
| Windows Server 2003 서비스 팩 2                 | Internet Explorer 6 (2888505) | 원격 코드 실행 | 중요     | MS13-080의 2879017 |
| Windows Server 2003 x64 Edition 서비스 팩 2     | Internet Explorer 6 (2888505) | 원격 코드 실행 | 중요     | MS13-080의 2879017 |
| Windows Server 2003 SP2(Itanium 기반 시스템용)    | Internet Explorer 6 (2888505) | 원격 코드 실행 | 중요     | MS13-080의 2879017 |

# 취약점 기본 정보를 얻는 방법

## 취약점 정보

### 심각도 및 취약점

#### Internet Explorer 정보 유출 취약점(CVE-2013-3908)

Internet Explorer가 인쇄 미리 보기를 생성할 때 특수하게 조작된 웹 콘텐츠를 처리하는 방식에 정보 유출 취약점이 존재합니다. 이 취약점 악용에 성공한 공격자는 공격 대상자가 보고 있는 모든 페이지에서 정보를 수집할 수 있습니다.

이 취약점을 CVE(Common Vulnerabilities and Exposures) 목록의 표준 항목으로 보려면 [CVE-2013-3908\(영문\)](#)을 참조하십시오.

완화 요소

대안

FAQ

↑ 섹션 맨 위로 이동

#### Internet Explorer 정보 유출 취약점(CVE-2013-3909)

Internet Explorer가 CSS 특수 문자를 처리하는 방식에 정보 유출 취약점이 존재합니다. 공격자는 사용자가 웹페이지를 볼 경우 정보 유출이 발생하는 특수하게 조작된 웹페이지를 구성하여 이 취약점을 악용할 수 있습니다. 이 취약점 악용에 성공한 공격자는 다른 도메인이나 Internet Explorer 영역의 콘텐츠를 볼 수 있습니다.

이 취약점을 CVE(Common Vulnerabilities and Exposures) 목록의 표준 항목으로 보려면 [CVE-2013-3909\(영문\)](#)을 참조하십시오.

완화 요소

대안

FAQ

# 취약점 기본 정보를 얻는 방법

## 보안 업데이트 배포

영향을 받는 소프트웨어

영향을 받는 소프트웨어에 해당하는 보안 업데이트에 대한 내용을 보려면 적절한 링크를 클릭하십시오.

## 파일 정보

[Microsoft 기술 자료 문서 2888505](#) 참조

## Internet Explorer 6

지원되는 모든 32비트 버전의 Windows XP용 Internet Explorer 6

| File name    | File version  | File size | Date        | Time  | Platform       | SP requirement | Service branch |
|--------------|---------------|-----------|-------------|-------|----------------|----------------|----------------|
| Browseui.dll | 6.0.2900.6462 | 1,025,024 | 12-Oct-2013 | 14:54 | x86            | SP3            | SP3QFE         |
| Html.iec     | 2011.1.31.10  | 369,664   | 12-Oct-2013 | 11:54 | Not applicable | SP3            | SP3QFE         |
| leencode.dll | 2011.1.31.10  | 81,920    | 12-Oct-2013 | 14:54 | x86            | SP3            | SP3QFE         |
| lepeers.dll  | 6.0.2900.6462 | 251,904   | 12-Oct-2013 | 14:54 | x86            | SP3            | SP3QFE         |
| Mshtml.dll   | 6.0.2900.6462 | 3,094,528 | 13-Oct-2013 | 04:24 | x86            | SP3            | SP3QFE         |
| Mshtml.dll   | 6.0.2900.6462 | 450,048   | 12-Oct-2013 | 14:54 | x86            | SP3            | SP3QFE         |
| Mstime.dll   | 6.0.2900.6462 | 532,480   | 12-Oct-2013 | 14:54 | Not applicable | SP3            | SP3QFE         |
| Shdocvw.dll  | 6.0.2900.6462 | 1,510,400 | 12-Oct-2013 | 14:54 | x86            | SP3            | SP3QFE         |
| Tdc.ocx      | 1.3.0.3131    | 61,952    | 12-Oct-2013 | 14:54 | x86            | SP3            | SP3QFE         |
| Url.dll      | 6.0.2900.6462 | 37,888    | 12-Oct-2013 | 14:54 | x86            | SP3            | SP3QFE         |
| Urlmon.dll   | 6.0.2900.6462 | 633,856   | 12-Oct-2013 | 14:54 | x86            | SP3            | SP3QFE         |
| Vgx.dll      | 6.0.2900.6462 | 852,992   | 12-Oct-2013 | 14:54 | x86            | SP3            | SP3QFE         |
| Wininet.dll  | 6.0.2900.6462 | 668,672   | 12-Oct-2013 | 14:54 | x86            | SP3            | SP3QFE         |



# 패치 되기전 최신 파일 구하기

| 운영 체제  | 구성 요소                            | 최대 보안 영향 | 전체 심각도 | 대체된 업데이트          |
|--|----------------------------------|----------|--------|-------------------|
| <b>Internet Explorer 6</b>                     |                                  |          |        |                   |
| Windows XP 서비스 팩 3                             | Internet Explorer 6<br>(2879017) | 원격 코드 실행 | 긴급     | MS13-069의 2870699 |
| Windows XP Professional x64<br>Edition 서비스 팩 2 | Internet Explorer 6<br>(2879017) | 원격 코드 실행 | 긴급     | MS13-069의 2870699 |
| Windows Server 2003 서비스 팩 2                    | Internet Explorer 6<br>(2879017) | 원격 코드 실행 | 보통     | MS13-069의 2870699 |
| Windows Server 2003 x64 Edition 서<br>비스 팩 2    | Internet Explorer 6<br>(2879017) | 원격 코드 실행 | 보통     | MS13-069의 2870699 |
| Windows Server 2003 SP2(Itanium<br>기반 시스템용)    | Internet Explorer 6<br>(2879017) | 원격 코드 실행 | 보통     | MS13-069의 2870699 |

# Get File

| 운영 체제              | 구성 요소  | 최대 보안 영향 | 전체 심각도 | 이 업데이트로 대체된 공지 |
|--------------------|--|----------|--------|----------------|
| Windows XP 서비스 팩 3 | Microsoft Data Access Components 2.8 서비스 팩 1 (KB2419632) | 원격 코드 실행 | 긴급     | 없음             |

## 고급검색

다음 기준으로 페이지 검색...

다음 단어 모두 포함:

다음 단어 또는 문구 정확하게 포함:

Odbc32.dll

다음 단어 중 아무거나 포함:

다음 단어 제외:

숫자 범위:

~

"3.525 3012.0"

"Odbc32.dll" .."3.525 3012.0"

웹문서

이미지

지도

동영상

블로그

더보기 ▾

검색 도구

검색결과 약 3,940개 (0.11초)

도움말: [한국어 검색결과만 검색합니다.](#) [환경설정](#)에서 검색 언어를 지정할 수 있습니다.

웹문서

[MS11-002: 2011년 1월 11일자 Microsoft Data Access Components ... support.microsoft.com/kb/2419632/ko ▾](#)

**Odbc32.dll, 3.525.3012.0**, 249,856, 09-Nov-2010, 14:52, x86, SP3, SP3GDR. Msadco.dll, 2.81.3012.0, 143,360, 09-Nov-2010, 14:50, x86, SP3, SP3QFE.

이 페이지를 13. 11. 29에 방문했습니다.

[Odbc32.dll - Microsoft Files](#)

[www.mskbfiles.com/odbc32.dll.php ▾](#) 이 페이지 번역하기

40개 항목 - Microsoft Data Access - ODBC Driver Manager. **Odbc32.dll** version ...

2828649 A backup application that uses a third-party ODBC driver crashes ...

2856310 64-bit ODBC application crashes when it configures a statement ...

이 페이지를 2번 방문했습니다. 최근 방문 날짜: 13. 11. 29

# 보안 패치에서 dll 파일 추출 하기

▶ [패치 파일명] /extract:[path]

|              |                  |                    |         |
|--------------|------------------|--------------------|---------|
| SP3GDR       | 2013-11-27 오후... | 파일 폴더              |         |
| SP3QFE       | 2013-11-28 오후... | 파일 폴더              |         |
| update       | 2013-11-27 오후... | 파일 폴더              |         |
| diff.dgf     | 2013-11-27 오후... | DarunGrim2.0 Da... | 4,735KB |
| spmsg.dll    | 2010-02-22 오후... | 응용 프로그램 확장         | 16KB    |
| spuninst.exe | 2010-02-22 오후... | 응용 프로그램            | 222KB   |

설치 프로그램을 설치하지 않고  
파일을 추출 하는 명령어

| 지원되는 보안 업데이트 설치 스위치 |  |
|---------------------|--|
| 전환                  | 설명   |
| /help               | 명령줄 옵션을 표시합니다.   |
| 설치 모드               |  |
| /passive            | 무인 설치 모드입니다. 사용자 조력이 필요 없으나, 설치 상태는 표시됩니다. 설치 완료 후 다시 시작이 필요한 경우 컴퓨터가 30초 후에 다시 시작한다는 타이머 경고가 있는 대화 상자가 사용자에게 표시됩니다.       |
| /quiet              | 자동 모드 무인 설치 모드와 동일하지만 상태 또는 오류 메시지가 표시되지 않습니다.   |
| /integrate:path     | Windows 원본 파일에 업데이트를 통합합니다. 이 파일은 스위치에서 정의된 경로에 위치합니다.   |
| /extract:path       | 설치 프로그램을 시작하지 않고 파일을 추출합니다.  |
| /ER                 | 확장 오류 보고를 사용합니다.   |
| /verbose            | 세부 정보 표시 로깅을 사용합니다. 설치 시 %Windir%\CabBuild.log를 생성합니다. 이 로그에는 복사할 파일이 상세하게 나열되어 있습니다. 이 스위치를 사용하면 설치 과정이 더 느리게 진행될 수 있습니다. |

<http://support.microsoft.com/kb/262841>

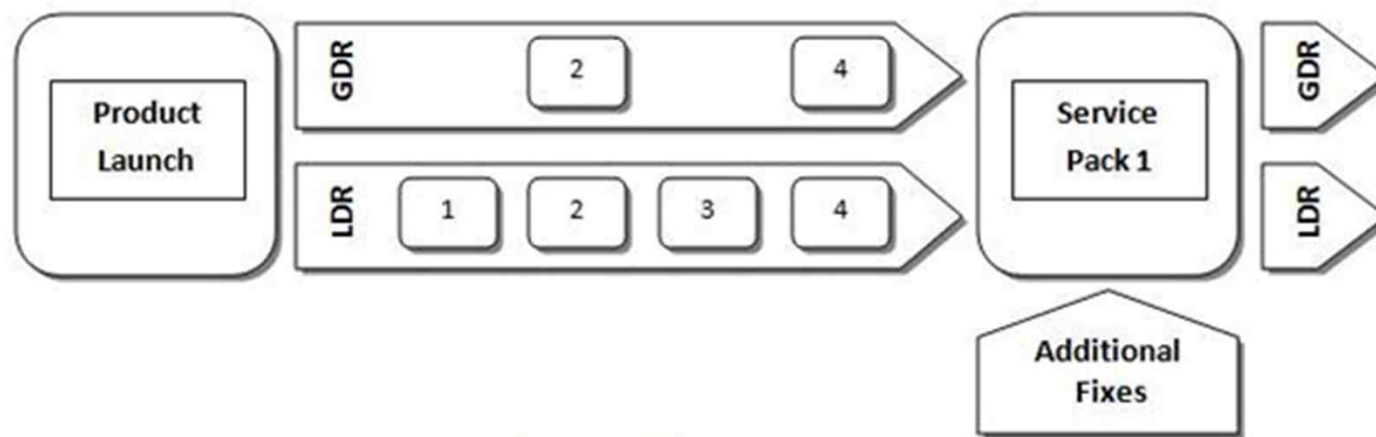


# 보안 패치에서 dll 파일 추출 하기

- ▶ 오피스 보안 패치 파일 /C /T:[보안패치 절대 경로]
- ▶ msix [파일명].msp /ext /out [경로]
- ▶ mst 및 cab 파일 추출
- ▶ cab 파일 안에 해당 패치 파일 추출
- ▶ msix 다운로드 경로
  - ▶ <http://www.windowswiki.info/wp-content/uploads/2009/07/msix.zip>

# Get more

- ▶ GDR
  - ▶ 보안에 큰 영향을 주는 부분이 있을때 제공
- ▶ LDR or QFE
  - ▶ 급하게 보안 패치를 내야 할 때 제공



# Get more

- ▶ 분석 하기 이전에 알아 두면 좋은것들

- ▶ 윈도우 오픈 소스 프로젝트

- ▶ <http://www.reactos.org/ko>

- ▶ 인터넷 브라우저 오픈 소스

- ▶ <http://www-archive.Mozilla.org/projects/firefox/index.html>

- ▶ 오피스 오픈소스

- ▶ <http://www.openoffice.org/download/source/>

- ▶ 사전에 윈도우, 브라우저, 오피스 오픈 소스를 이용하여 어떤 방식 프로그래밍 되어 있는지 확인



알아볼 취약점

# Buffer OverFlow



# 취약한 함수들

strcpy  
strncpy  
strcat  
strncat  
sprintf  
vsprintf  
gets  
strlen

# strsafe.h

StringCbCopy

StringCbCopyN

StringCbCat

StringCbCatN

StringCbPrintf

StringCbVPrintf

StringCbGets

StringCchLength

StringCbCopyEx

StringCbCopyNEx

StringCbCatEx

StringCbCatNEx

StringCbPrintfEx

StringCbVPrintfEx

StringCbGetsEx

StringCbLength

알아볼 취약점

Use After Free



# 해당 취약점 파일 찾기?

## Microsoft Security Bulletin MS13-088 - 긴급

### Internet Explorer 누적 보안 업데이트 (2888505)

게시된 날짜: 2013년 11월 13일 수요일

버전: 1.0

#### 일반 정보

##### 요약

이 보안 업데이트는 Internet Explorer에서 발견되어 **비공개적으로 보고된 취약점 10건을 해결**합니다. 가장 위험한 취약점으로 인해 사용자가 Internet Explorer를 사용하여 특수하게 조작된 웹 페이지를 볼 경우 원격 코드 실행이 허용될 수 있습니다. 가장 위험한 취약점 악용에 성공한 공격자는 현재 사용자와 동일한 권한을 얻을 수 있습니다. 시스템에 대한 사용자 권한이 적게 구성된 계정의 사용자는 관리자 권한으로 작업하는 사용자에 비해 영향을 적게 받습니다.

이 보안 업데이트의 심각도는 영향을 받는 Windows 클라이언트의 Internet Explorer 6, Internet Explorer 7, Internet Explorer 8, Internet Explorer 9, Internet Explorer 10 및 Internet Explorer 11에 대해 긴급이며 영향을 받는 Windows 서버의 Internet Explorer 6, Internet Explorer 7, Internet Explorer 8, Internet Explorer 9 및 Internet Explorer 10에 대해 중요입니다. 또한 영향을 받는 Windows 서버의 Internet Explorer 11에 대해서는 보통입니다. 자세한 내용은 이 섹션에서 **영향을 받는 소프트웨어 및 영향을 받지 않는 소프트웨어**를 참조하십시오.

이 보안 업데이트는 Internet Explorer가 CSS 특수 문자를 처리하는 방식, 인쇄 미리 보기를 생성할 때 특수하게 조작된 웹 콘텐츠를 처리하는 방식 및 메모리의 개체를 처리하는 방식을 수정하여 취약점을 해결합니다. 취약점에 대한 자세한 내용은 **취약점 정보**에서 각 취약점 항목의 자주 제기되는 질문 사항(FAQ)을 참조하십시오.














**권장 사항.** 대부분의 고객은 자동 업데이트를 사용하고 있기 때문에 따로 조치를 취할 필요가 없습니다. 이 보안 업데이트가 자동으로 다운로드되고 설치됩니다. 자동 업데이트를 사용하고 있지 않은 고객은 수동으로 업데이트를 확인하고 이 업데이트를 설치해야 합니다. 자동 업데이트의 특정 구성 옵션에 대한 자세한 내용은 [Microsoft 기술 자료 문서 294871](#)을 참조하십시오.

관리자 및 기업 설치의 경우나 이 보안 업데이트를 수동으로 설치하려는 최종 사용자의 경우에는 고객이 업데이트 관리 소프트웨어를 사용하거나 [Microsoft Update](#) 서비스를 통해 업데이트를 확인하여 업데이트를 즉시 적용하는 것이 좋습니다.

이 공지 뒷부분에 있는 **검색, 탐지 도구 및 지침** 섹션도 참조하십시오.



# 보안패치 파일 추출 후

|   |                  |             |         |
|---|------------------|-------------|---------|
|  browseui.dll  | 2013-08-01 오후... | 응용 프로그램 확장  | 1,001KB |
|  html.iec      | 2013-08-01 오후... | IEC 파일      | 358KB   |
|  ieencode.dll  | 2013-08-01 오후... | 응용 프로그램 확장  | 80KB    |
|  iepeers.dll   | 2013-08-01 오후... | 응용 프로그램 확장  | 245KB   |
|  mshtml.dll    | 2013-08-01 오전... | 응용 프로그램 확장  | 3,042KB |
|  mshtml.dll    | 2013-08-01 오후... | 응용 프로그램 확장  | 439KB   |
|  mstime.dll    | 2013-08-01 오후... | 응용 프로그램 확장  | 520KB   |
|  shdocvw.dll | 2013-08-01 오후... | 응용 프로그램 확장  | 1,475KB |
|  tdc.ocx     | 2013-08-01 오후... | ActiveX 컨트롤 | 61KB    |
|  url.dll     | 2013-08-01 오후... | 응용 프로그램 확장  | 37KB    |
|  urlmon.dll  | 2013-08-01 오후... | 응용 프로그램 확장  | 609KB   |
|  vgx.dll     | 2013-08-01 오후... | 응용 프로그램 확장  | 833KB   |
|  wininet.dll | 2013-08-01 오후... | 응용 프로그램 확장  | 643KB   |

해당 취약점 파일 찾기?

HOW????

# 해당 취약점 파일 찾기?

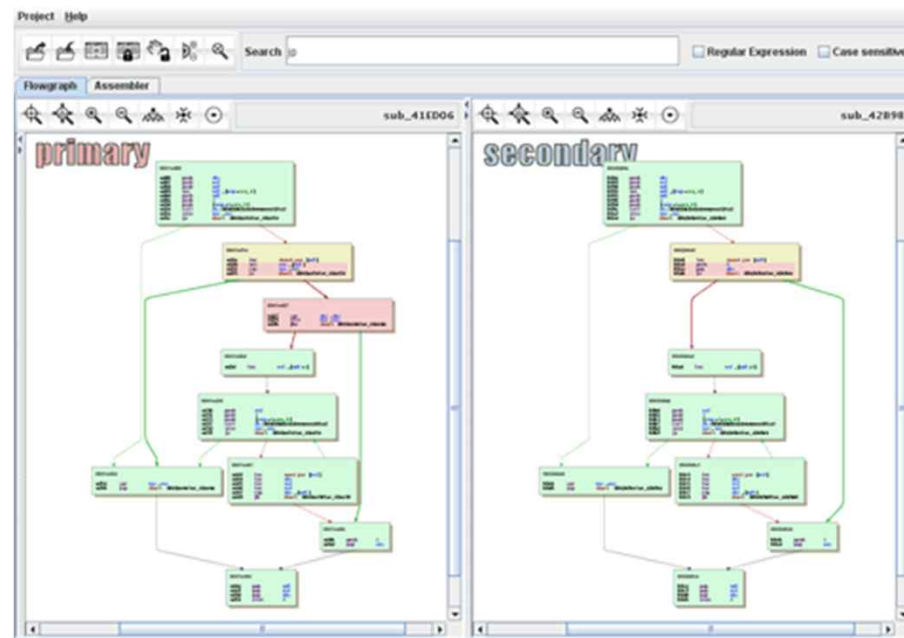
- ▶ 취약점이 존재 하나 어떠한 취약점이 있는지 알 수 없음
- ▶ 또한 어떤 파일에서 취약점이 발생 하는지도 역시 알 수 없음
- ▶ 그럼??? 어떻게 해야 할까?
- ▶ 공개된 취약점을 분석한 뒤 어떠한 방식으로 취약점을 패치하는지 확인
- ▶ 그럼 필요한 툴은???

# Tool

- ▶ Diffing Tool
  - ▶ Darungrim
  - ▶ TurboDiff
  - ▶ PatchDiff
  - ▶ BinDiff
- ▶ IDA

# Diffing 이란?

- Diffing은 소스 파일과 타겟 파일 간에 변경 된 점을 보여주기 위해서 사용 하는 기법
- 대부분의 binary Diffing의 경우 IDA의 데이터 베이스를 기반으로 분석



# Diffing을 하는 이유?

- ▶ 현재 어떠한 부분에 대해서 오류가 발생 하였는지 알지 못함
- ▶ 많은 시간 소모
- ▶ 변경 된 부분을 찾아야지만 분석 가능

# Diffing의 대상은??

- ▶ 패치 파일 과 이전 패치 간의 파일 Diffing
- ▶ 새로운 운영체제와 이전 운영체제 간의 파일 Diffing

MS11-002



# 분석 하기전 사전 조사

## ▶ MS11-002

### 일반 정보

#### 요약

이 보안 업데이트는 Microsoft Data Access Components에서 발견되어 **비공개적으로 보고된 취약점 2건을 해결합니다.** 이 취약점으로 인해 사용자가 특수하게 조작된 웹 페이지를 볼 경우 원격 코드 실행이 허용될 수 있습니다. 취약점 악용에 성공한 공격자는 **로컬 사용자와 동일한 권한을 얻을 수 있습니다.** 시스템에 대한 사용자 권한이 적게 구성된 계정의 사용자는 관리자 권한으로 작업하는 사용자에 비해 영향을 적게 받습니다.

이 보안 업데이트의 심각도는 지원 대상인 모든 Windows XP, Windows Vista 및 Windows 7 에디션에 대해 긴급이며, 지원 대상인 모든 Windows Server 2003, Windows Server 2008 및 Windows Server 2008 R2 에디션에 대해 중요합니다. 자세한 내용은 이 섹션에서 **영향을 받는 소프트웨어 및 영향을 받지 않는 소프트웨어**를 참조하십시오.

보안 업데이트는 MDAC가 문자열 길이와 메모리 할당의 유효성을 올바르게 검사하도록 하여 취약점을 해결합니다. 취약점에 대한 자세한 내용은 다음 섹션, **취약점 정보**에서 각 취약점 항목의 자주 제기되는 질문 사항(FAQ)를 참조하십시오.

**권장 사항.** 대다수의 고객은 자동 업데이트를 사용하고 있기 때문에 따로 조치를 취할 필요가 없습니다. 이 보안 업데이트가 자동으로 다운로드되고 설치됩니다. 자동 업데이트를 사용하고 있지 않은 고객은 수동으로 업데이트를 확인하고 이 업데이트를 설치해야 합니다. 자동 업데이트의 특정 구성 옵션에 대한 자세한 내용은 [Microsoft 기술 자료 문서 294871](#)을 참조하십시오.

관리자 및 기업 설치의 경우나 이 보안 업데이트를 수동으로 설치하려는 최종 사용자의 경우에는 고객이 업데이트 관리 소프트웨어를 사용하거나 [Microsoft Update](#) 서비스를 통해 업데이트를 확인하여 업데이트를 즉시 적용하는 것이 좋습니다.

이 공지 뒷부분에 있는 **검색, 탐지 도구 및 지침** 섹션도 참조하십시오.

## 취약점 정보

### ⊕ 심각도 및 취약점

#### ☐ DSN 오버플로 취약점(CVE-2011-0026)

Microsoft Data Access Components에서 타사 API 사용의 유효성을 검사하는 방식에 원격 코드 실행 취약점이 존재합니다. 이 취약점으로 인해 사용자가 특수하게 조작된 웹 페이지를 방문할 경우 코드 실행이 허용될 수 있습니다. 사용자가 관리자 권한으로 로그인한 경우, 이 취약점을 악용한 공격자는 영향을 받는 시스템을 완전히 제어할 수 있습니다. 이렇게 되면 공격자가 프로그램을 설치할 수 있을 뿐 아니라 데이터를 보거나 변경하거나 삭제할 수 있고 모든 사용자 권한이 있는 새 계정을 만들 수도 있습니다. 시스템에 대한 사용자 권한이 적게 구성된 계정의 사용자는 관리자 권한으로 작업하는 사용자에게 비해 영향을 적게 받습니다.

이 취약점을 CVE(Common Vulnerabilities and Exposures) 목록의 표준 항목으로 보려면 [CVE-2011-0026 \(영문\)](#)을 참조하십시오.

#### ⊕ DSN 오버플로 취약점(CVE-2011-0026)에 대한 완화 요소

#### ⊕ DSN 오버플로 취약점(CVE-2011-0026)에 대한 대안

#### ⊕ DSN 오버플로 취약점(CVE-2011-0026)에 대한 FAQ

↗ 섹션 맨 위로 이동

#### ☐ ADO 레코드 메모리 취약점(CVE-2011-0027)

Microsoft Data Access Components에서 메모리 할당의 유효성을 검사하는 방식에 원격 코드 실행 취약점이 존재합니다. 이 취약점으로 인해 사용자가 특수하게 조작된 웹 페이지를 방문할 경우 코드 실행이 허용될 수 있습니다. 사용자가 관리자 권한으로 로그인한 경우, 이 취약점을 악용한 공격자는 영향을 받는 시스템을 완전히 제어할 수 있습니다. 이렇게 되면 공격자가 프로그램을 설치할 수 있을 뿐 아니라 데이터를 보거나 변경하거나 삭제할 수 있고 모든 사용자 권한이 있는 새 계정을 만들 수도 있습니다. 시스템에 대한 사용자 권한이 적게 구성된 계정의 사용자는 관리자 권한으로 작업하는 사용자에게 비해 영향을 적게 받습니다.

이 취약점을 CVE(Common Vulnerabilities and Exposures) 목록의 표준 항목으로 보려면 [CVE-2011-0027 \(영문\)](#)을 참조하십시오.

#### ⊕ ADO 레코드 메모리 취약점(CVE-2011-0027)에 대한 완화 요소

#### ⊕ ADO 레코드 메모리 취약점(CVE-2011-0027)에 대한 대안

#### ⊕ ADO 레코드 메모리 취약점(CVE-2011-0027)에 대한 FAQ

|  |   |
|--|---|
| <b>CVE-ID</b>  |   |
| <b>CVE-2011-0026</b>   | <a href="#">Learn more at National Vulnerability Database (NVD)</a><br>• Severity Rating • Fix Information • Vulnerable Software Versions • SCAP Mappings |
| <b>Description</b>   |   |
| Integer signedness error in the SQLConnectW function in an ODBC API (odbc32.dll) in Microsoft Data Access Components (MDAC) 2.8 SP1 and SP2, and Windows Data Access Components (WDAC) 6.0, allows remote attackers to execute arbitrary code via a long string in the Data Source Name (DSN) and a crafted szDSN argument, which bypasses a signed comparison and leads to a buffer overflow, aka "DSN Overflow Vulnerability."   |   |
| <b>References</b>  |   |
| <b>Note:</b> References are provided for the convenience of the reader to help distinguish between vulnerabilities. The list is not intended to be complete.   |   |
| <ul style="list-style-type: none"> <li>MISC:<a href="http://www.zerodavinitiative.com/advisories/ZDI-11-001/">http://www.zerodavinitiative.com/advisories/ZDI-11-001/</a></li> <li>CONFIRM:<a href="http://support.avaya.com/css/P8/documents/100124846">http://support.avaya.com/css/P8/documents/100124846</a></li> <li>MS:MS11-002</li> <li>URL:<a href="http://www.microsoft.com/technet/security/Bulletin/MS11-002.msp">http://www.microsoft.com/technet/security/Bulletin/MS11-002.msp</a></li> <li>CERT:TA11-011A</li> <li>URL:<a href="http://www.us-cert.gov/cas/techalerts/TA11-011A.html">http://www.us-cert.gov/cas/techalerts/TA11-011A.html</a></li> <li>BID:45695</li> <li>URL:<a href="http://www.securityfocus.com/bid/45695">http://www.securityfocus.com/bid/45695</a></li> <li>OSVDB:70443</li> <li>URL:<a href="http://osvdb.org/70443">http://osvdb.org/70443</a></li> <li>oval:oval.mitre.org:oval:def:12333</li> <li>URL:<a href="http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:12333">http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:12333</a></li> <li>SECTrack:1024947</li> <li>URL:<a href="http://www.securitytracker.com/id?1024947">http://www.securitytracker.com/id?1024947</a></li> <li>SECUNIA:42804</li> <li>URL:<a href="http://secunia.com/advisories/42804">http://secunia.com/advisories/42804</a></li> <li>VUPEN:ADV-2011-0075</li> <li>URL:<a href="http://www.vupen.com/english/advisories/2011/0075">http://www.vupen.com/english/advisories/2011/0075</a></li> </ul> |   |

# 사전 조사로 얻은 정보

- ▶ 두가지 취약점
  - ▶ DSN 취약점
  - ▶ ADO 취약점
- ▶ DSN 란?
  - ▶ Database Source Name 으로 DB를 사용하는 어플리케이션에서 DB를 불러 올때 해당하는 DB를 연결시키기 위해 구분 짓는 이름
- ▶ SQLConnectW function in an ODBC API (odbc32.dll)

# BinDiff를 이용하여 Diffing

C:\Users\test\Documents\codeengn\codeengn.BinDiffWorkspace - zynamics BinDiff

File Diffs Settings Help

Workspace **\_StringCchLengthA@12**

Single Function Diff Views (0)  
EXCELunpatched vs EXCELPatched  
odbc32 vs odbc32  
Call Graph (1071/1078)  
Matched Functions (1071)  
**Primary Unmatched Functions (0/1071)**  
Secondary Unmatched Functions (7/1078)  
odbc32 vs odbc32t

0 / 0 Primary Unmatched Functions

| Address | Name | Type | Basic Blocks | Jumps | Instructions | Callers | Callees |
|---------|------|------|--------------|-------|--------------|---------|---------|
|---------|------|------|--------------|-------|--------------|---------|---------|

7 / 7 Secondary Unmatched Functions

| Address         | Name                              | Type          | Basic Blocks | Jumps     | Instructions | Callers  | Callees  |
|-----------------|-----------------------------------|---------------|--------------|-----------|--------------|----------|----------|
| 7353CB7A        | _ULongLongToUInt@12               | Normal        | 5            | 7         | 16           | 3        | 0        |
| 7353CBA7        | _SizeTAdd@12                      | Normal        | 3            | 3         | 17           | 2        | 0        |
| 7353CBD2        | _StringLengthWorkerA@12           | Normal        | 9            | 13        | 27           | 0        | 0        |
| <b>7353D701</b> | <b>_StringCchLengthA@12</b>       | <b>Normal</b> | <b>13</b>    | <b>18</b> | <b>39</b>    | <b>1</b> | <b>0</b> |
| 7353FE41        | _ValidateNullTerminatedStringW@12 | Normal        | 6            | 7         | 28           | 6        | 1        |
| 7354D56B        | _bidTraceMark@8                   | Normal        | 4            | 4         | 18           | 3        | 1        |
| 7355087B        | sub_7355087B                      | Normal        | 6            | 8         | 23           | 10       | 2        |

# Diffing 결과로 얻은 정보

- ▶ 총 7 가지의 새로운 함수를 확인
- ▶ ValidateNullTerminatedStringW 유효성을 검사
- ▶ StringCchLengthA 길이를 체크 하는 함수

| 7 / 7 Secondary Unmatched Functions                        |  |               |
|--|--|---------------|
| <div><div></div><div>▼</div><div>✕</div><div>⚙</div></div> |  |               |
| Address  | Name                                     | Type          |
| 7353CB7A   | _ULongLongToUInt@12                      | Normal        |
| 7353CBA7   | _SizeTAdd@12                             | Normal        |
| 7353CBD2   | _StringLengthWorkerA@12                  | Normal        |
| 7353D701   | _StringCchLengthA@12                     | Normal        |
| <b>7353FE41</b>  | <b>_ValidateNullTerminatedStringW@12</b> | <b>Normal</b> |
| 7354D56B   | __bidTraceMark@8                         | Normal        |
| 7355087B   | sub_7355087B                             | Normal        |



시연



# 감사합니다