2013년 사이버 보안 백서

- 보안 취약점 -

2013년 12월

HNS Pioneer of Security Research

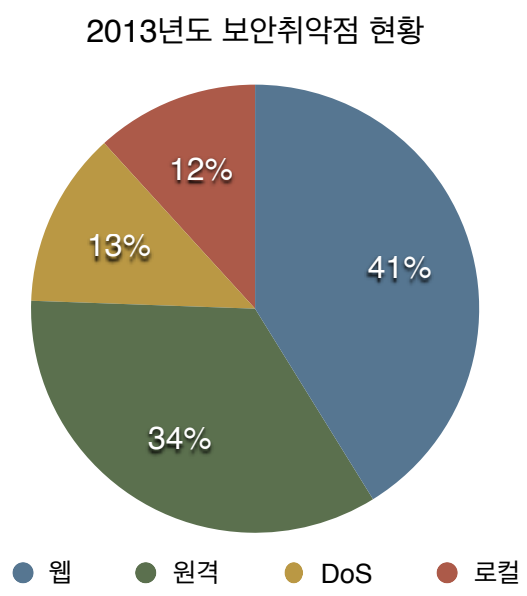
http://www.hacknsecurity.com

1. 개요

exploit-db.com[1]의 자료(1월 1일 ~ 11월 15일 기준)에 의하면 2013년 보안 취약점은 총 910개가 발표되었다. 2013년 발표된 취약점을 exploit-db의 구분에 따라 살펴보면 웹 취약점은 463개, 원격 취약점은 226개, DoS 취약점은 124개, 로컬 취약점은 97개이다.

분류	웹	원격	DOS	로컬	합계
2011년	774	260	238	180	1,452
2012년	697	251	242	106	1,296
2013년	463	226	124	97	910

2011년(12.31) / 2012년(12.15) / 2013(11.15) 보안 취약점 수



표를 보면 쉽게 알 수 있듯이 여전히 웹 보안 취약점들이 가장 많이 발견되고 있다. 플랫폼별로 구분해보면 이것의 이유가 더욱 뚜렷해진다.

플랫폼별로 구분하면 PHP, Windows, 하드웨어, 리눅스 등의 순으로 많은 취약점들이 발표되었다. 이 순서는 2012년과 동일하다.

PHP의 취약점이 다수를 차지하는 것은 웹 애플리케이션의 취약점이 그만큼 많이 발견되었으며, 웹 취약점은 발견하기가 쉽다는 것을 입증하는 것이기도 하다. PHP 관련 취약점들 중 294개가 웹 애플리케이션의 취약점이고, PHP에 대한 직접적인 공격이 가능한 취약점은 31개였다. 2013년에 공개된 웹 취약점 중 SQL Injection 취약점이 148개를 차

[1] exploit-db.com의 자료를 보안 취약점 현황 분석에서 활용하는 것은 충실한 업데이트와 더불어 공격 코드도 같이 포함되어 포스팅되기 때문이다. 취약점을 DoS, 로컬 취약점, 원격 취약점, 웹 취약점 4가지로 분류하고 있으며, 또한 플랫폼별로 구분을 하고 있어 데이터 활용이 용이하다. 그러나 비공개 취약점과 타 사이트에서만 공개되는 취약점들도 있으므로 전체 보안 취약점을 포함하는 절대적인 자료는 될 수 없다. 대신 전체 보안 취약점의 흐름을 파악할 수 있는데 도움을 받을 수 있다.

지하고, XSS 취약점이 122개이다. 웹 취약점은 악성코드 유포에 이용될 수 있다는 것을 고려했을 때 웹 애플리케이션의 취약점은 심각한 수준임을 확인할 수 있다.

일부 웹 애플리케이션은 하드웨어 시스템을 통제하는데 사용되기도 하는데, 이 애플리케이션들 중 일부는 디폴트 패스워드를 사용하고 있어 검색엔진을 통해 디폴트 패스워드를 확인한 후 관리자 페이지에 로그인하여 시스템에 접근 및 통제할 수 있는 취약점들도 존재했다. POC2013에서도 발표된 CCTV 관련 취약점도 이에 일부 해당된다고 할 수 있다.

플랫폼	수(개)
PHP	325
Windows	274
하드웨어	157
리눅스	62
OSX	7

PHP 다음으로 많이 발표된 취약점은 Windows 관련 취약점으로, 총 274개 중 DoS 공격에 사용될 수 있는 취약점은 123개, 웹 해킹에 이용될 수 있는 취약점은 18개, Windows 시스템에 대한 로컬 공격 취약점은 63개, 원격 공격 취약점은 107개에 이른다. 대부분 컴퓨터 사용자가 Windows 운영체제를 사용하고 있는 것을 고려해보면 많은 사용자가 보안 위협에 노출되어 있음을 알 수 있다.

Windows 다음으로 많은 취약점이 공개된 것은 하드웨어 관련 취약점이다. 보안 취약점을 가지고있는 하드웨어 부분이 문제가 되는 경우는 네트워크와 연결되어 있을 때가 대부분이다. 하드웨어 부분에서 취약점이 발견된 것들 중 대표적인 것이 라우터, 프린터기, 스마트 TV, SCADA 시스템, VoIP 케이블 모뎀 등이다. 하드웨어 취약점들 중 관리자 권한을 획득할 수 있는 취약점들도 다수가 포함되어 있는데, 이는 산업시설 파괴 등으로 이어질 수도 있다. 보안 취약점을 많이 가지고 있는 대표적인 하드웨어 장비들로서는 D-Link, Linksys, Netgear 등이다.

62개의 보안 취약점이 발견된 리눅스의 경우 원격 취약점은 24개로, 여전히 overflow 취약점이 많았는데, 리눅스 커널 취약점 등을 포함한 리눅스 자체의 취약점은 5개가 발견되었고, 그 외는 모두 리눅스 시스템에서 사용되고 있는 다른 애플리케이션들의 취약점들이었다. Novell 제품에는 원격으로 root 권한을 획득할 수 있는 취약점도 존재했으며, 보안 제품으로는 Sophos Web Protection Appliance에 원격으로 코드를 실행할 수 있는 취약점 등이 공개되었다.

보안 회사 제품 관련 취약점들도 다수 공개되었다. 앞에서 언급한 Sophos를 비롯해 McAfee, Symantec 등의 제품들에서도 보안 취약점들이 다수 발견되었다. 이를 통해 보안

제품 역시 취약점을 가지고 있을 수 있으므로 절대 맹신해서는 안되며, 해당 보안회사 입장에서도 취약점 정보를 은폐할 것이 아니라 신속하게 공개하여 더 큰 피해를 막는 것이 신뢰를 형성하는데 도움이 될 것이다.

지금까지 살펴본 것은 exploit-db.com에 공개된 것을 토대로 한 것이다. 그러나 exploit-db.com을 통해 공개되지 않는 취약점들도 많이 있다는 것을 간과해서는 안된다. 따라서 '(2) 상세분석' 섹션에서는 주요 벤더의 제품들에 존재하는 보안 취약점들을 비롯해 국내 관련 보안 취약점들도 살펴보기로 한다.

2. 상세 분석

1) 주요 벤더별 분석

이 섹션에서는 Adobe, Apple, Microsoft, Oracle, Symantec, Cisco 등의 제품에서 발견된 보안 취약점들에 대해 기술한다.

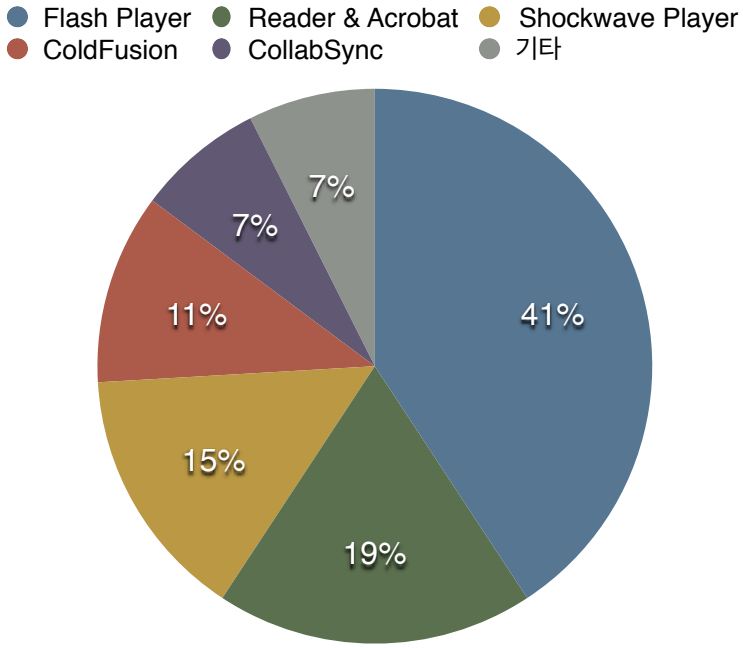
exploit-db.com의 자료에는 Adobe사 제품의 보안 취약점은 6개가 공개되어 있다. 그러나 Adobe Security Bulletins and Advisories[2]의 자료를 살펴보면 11월 현재 총 27개의 보안 취약점이 발견되었다는 것을 알 수 있다. 20개 정도의 차이는 exploit-db.com의 경우 보안 취약점에 대한 정보 뿐만 아니라 공격 코드가 포함된 것만 공개되었기 때문인 것으로 추측된다. 이는 다른 벤더들의 경우도 마찬가지다.

그러나 주목할 점은 벤더들의 Security Bulletin에는 포함되어 있지 않은 취약점이 exploit-db.com에는 포함되어 있다는 것이다. 이는 모든 보안 취약점에 대해 벤더들이 파악을 하지 못하고 있다는 것을 의미하며, 공개되지 않은 제로데이 취약점들도 다수 있으므로, 벤더들의 Security Bulletin과 exploit-db.com에 공개되어 있는 취약점들이 전부가 아니라는 것을 인식해야 한다.

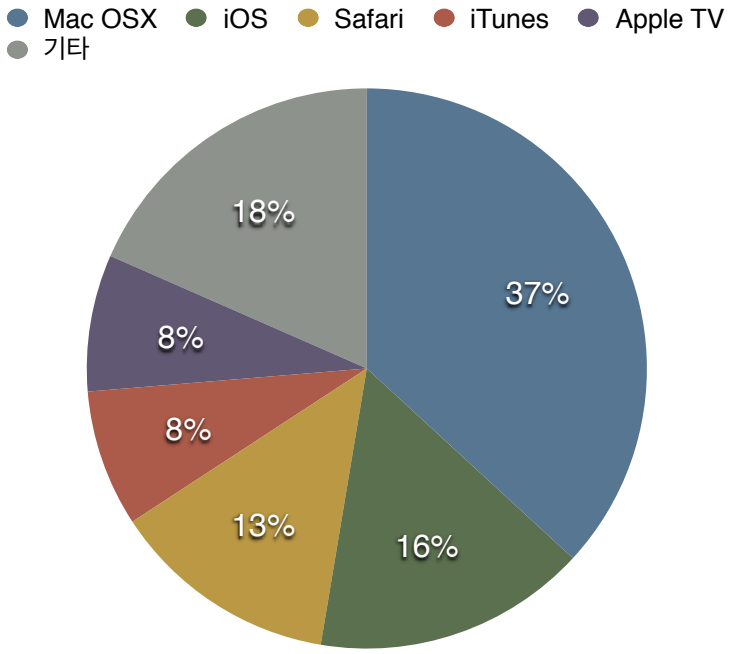
먼저 Adobe사의 제품에 존재하는 취약점들에 대해 살펴보자. 다음 차트에서 보듯 Adobe사의 제품에서 가장 많은 보안 취약점이 공개된 것은 Flash Player이다. Flash Player에서 보안 취약점을 발생시키는 가장 큰 원인은 buffer overflow와 memory corruption이다. Flash Player 다음으로 많은 취약점들이 공개된 Reader와 Shockwave Player의 취약점 원인 역시 buffer overflow와 memory corruption으로 확인되었다.

[2] http://www.adobe.com/support/security/

다음은 Apple 제품들의 보안 취약점에 대해 알아보자. exploit-db.com에는 8개가 공개되어 있고, Apple Security Update는 38개가 있었다.

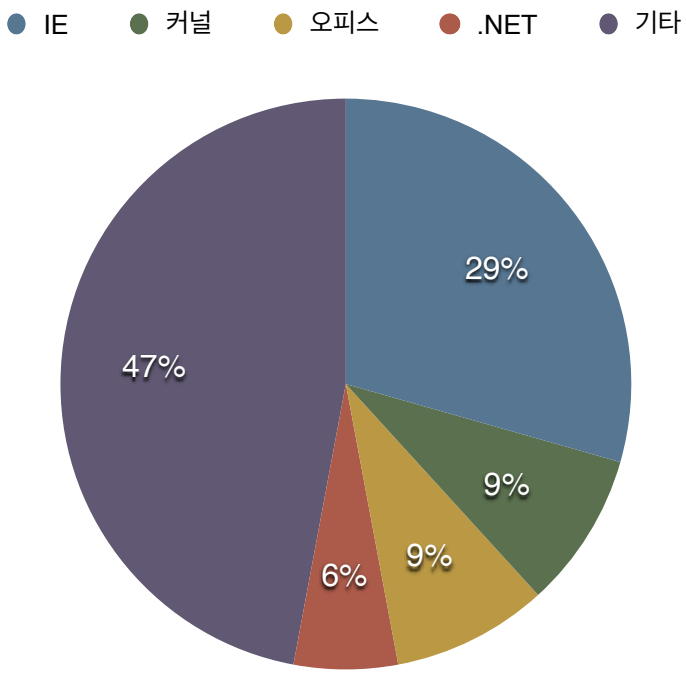


Apple의 제품에서 가장 많은 취약점이 발견된 것은 Mac OSX 상의 취약점들로, 14개이며, 그 다음으로 iOS 6, 7에서 6개의 취약점이, Safari에서는 5개의 보안 취약점이 발견되었다. 기타 iTunes, Quick Time Player, Xcode 등에서도 보안 취약점들이 발견되었다.



다른 벤더들의 제품과 비교하면 여전히 적은 수지만 2012년과 비교했을 때 Apple사의 제품에서 발견되는 보안 취약점이 점차 증가하고 있다는 것을 알 수 있다. 최근에는 IceFog APT 공격에서도 Mac OSX용 악성코드가 사용되었음을 볼 때 그동안 상대적으로 안전한 시스템으로 인식되었던 Apple사의 제품에 대한 보안 인식도 새롭게 할 필요가 있을 것이다.

11월 15일을 기준으로, Microsoft사의 제품 관련 보안 취약점은 exploit-db.com에서 17개, Microsoft Security Bulletin[3]에서 87개가 등록되어 있다. 이중 Critical한 것으로 분류된 것은 34개이고, Important로 분류된 것은 53개, Moderate로 분류된 것은 0개이다. Critical로 분류된 것들 중 Internet Explore 관련 취약점 10개, 커널 취약점 3개, 오피스 관련 취약점 3개, 그리고 .NET 관련 취약점 2개, 기타 16개이다.



웹 브라우저의 보안이 특히 중요해진 요즘 Critical로 분류된 취약점들 중 다수를 IE가 차지하고 있어 IE 사용에 신중해야 할 것으로 판단된다. 그리고 IE의 각 버전들과 컴포넌트 버전을 고려해본다면 실제로 10개 이상의 취약점들이 발견된 것으로 생각할 수 있다.

구글 Chrome의 경우 11월 현재까지 총 35번의 업데이트가 있었다. Chrome 업데이트의 경우 보안 업데이트와 일반 기능 업데이트까지 포함되어 있어 정확하게 몇 번의 보안 업데이트가 있었는지 제공되는 정보가 없다.

[3] http://technet.microsoft.com/en-us/security/bulletin

기타 벤더들을 살펴보면 다른 OS나 브라우저 등에도 영향을 미치는 Oracle의 Java 관련 취약점은 140여개에 이르고, Symantec의 제품들의 보안 취약점은 12개, Cisco 관련 취약점은 393개가 공개되었다.

국내 보안 취약점

이 섹션은 KISA, 데일리시큐, exploit-db, Secunia 등을 참고로 작성되었다. 외국에 많이 알려진 국내 애플리케이션과 시스템은 Gomplayer, 한컴 오피스, 삼성 스마트 TV 등이다. 특히 한컴 오피스의 취약점은 최근 우리나라를 타깃으로 하는 APT 공격에도 자주 사용되고 있는 것이 현실이다.

애플리케이션 이외에도 국내에서 생산되는 하드웨어와 이를 관리하는 프로그램들의 취약점들도 많으며, 국내 웹 사이트의 취약점을 이용한 공격도 많았으므로 웹 애플리케이션에 많은 취약점이 존재할 것으로 판단된다. 여기서는 공개된 취약점들의 목록을 다음과 같이 제시하고, 자세한 취약점 정보는 링크를 참고하자.

- Gomplayer

- 임의코드 실행 취약점(10/14)
  https://www.krcert.or.kr/kor/data/secNoticeView.jsp?p_bulletin_writing_sequence=3363
- 버퍼오버플로우 취약점(9/10)
  http://secunia.com/advisories/54744/
- GOMPlayer 2.2.53.5169 (.wav) - Crash POC(9/4)
  http://www.exploit-db.com/exploits/28080
- 원격코드 실행 - 버퍼오버플로우 취약점(8/7)
  https://www.krcert.or.kr/kor/data/secNoticeView.jsp?p_bulletin_writing_sequence=2503
- 원격코드 실행 취약점(5/31)
  https://www.krcert.or.kr/kor/data/secNoticeView.jsp?p_bulletin_writing_sequence=2293
- 원격코드 실행 취약점(2/28)
  https://www.krcert.or.kr/kor/data/secNoticeView.jsp?p_bulletin_writing_sequence=1953

- 한컴 오피스

- 임의코드 실행 취약점(11/18)
  https://www.krcert.or.kr/kor/data/secNoticeView.jsp?p_bulletin_writing_sequence=20108

- 임의코드 실행 취약점(11/2)
  https://www.krcert.or.kr/kor/data/secNoticeView.jsp?p_bulletin_writing_sequence=20024

- 임의코드 실행 취약점(10/16)
  https://www.krcert.or.kr/kor/data/secNoticeView.jsp?p_bulletin_writing_sequence=3383

- 임의코드 실행 취약점(8/30)
  https://www.krcert.or.kr/kor/data/secNoticeView.jsp?p_bulletin_writing_sequence=3196

- 임의코드 실행 취약점(7/24)
  https://www.krcert.or.kr/kor/data/secNoticeView.jsp?p_bulletin_writing_sequence=2455

- 임의코드 실행 취약점 (7/19)
  http://dailysecu.com/news_view.php?article_id=4828

- 임의코드 실행 취약점(7/11)
  https://www.krcert.or.kr/kor/data/secNoticeView.jsp?p_bulletin_writing_sequence=2410

- 임의코드 실행 취약점(6/24)
  https://www.krcert.or.kr/kor/data/secNoticeView.jsp?p_bulletin_writing_sequence=2363

- 임의코드 실행 취약점(5/30)
  https://www.krcert.or.kr/kor/data/secNoticeView.jsp?p_bulletin_writing_sequence=2292

- 임의코드 실행 취약점(5/3)
  https://www.krcert.or.kr/kor/data/secNoticeView.jsp?p_bulletin_writing_sequence=2164

- 원격코드 실행 취약점(2/6)
  https://www.krcert.or.kr/kor/data/secNoticeView.jsp?p_bulletin_writing_sequence=1864

- 이스트소프트

- 알씨 임의코드 실행 취약점(11/19)

https://www.krcert.or.kr/kor/data/secNoticeView.jsp?p_bulletin_writing_sequence=20109

- 알마인드 임의코드 실행 취약점(9/12)
  https://www.krcert.or.kr/kor/data/secNoticeView.jsp?p_bulletin_writing_sequence=3228

- 알집 버퍼오버플러우 취약점(7/6)
  http://dailysecu.com/news_view.php?article_id=196

- 제로보드

- XSS 및 CSRF 취약점(10/2)
  https://www.krcert.or.kr/kor/data/secNoticeView.jsp?p_bulletin_writing_sequence=3305

- XSS 취약점(7/23)
  http://dailysecu.com/news_view.php?article_id=4848

- 로컬 파일 include 취약점(5/3)
  https://www.krcert.or.kr/kor/data/secNoticeView.jsp?p_bulletin_writing_sequence=2223

- 그누보드

- 파일 업로드 취약점(10/20)
  http://dailysecu.com/news_view.php?article_id=5708

- XSS 취약점(2/6)
  http://dailysecu.com/news_view.php?article_id=3746

- 삼성

- Samsung Galaxy S4 Polaris Viewer DOCX Buffer Overflow Vulnerability(9/4)
  http://secunia.com/advisories/54701/

- Samsung DVR Firmware 1.10 - Authentication Bypass(8/21)
  http:/www.exploit-db.com/exploits/27753

- Samsung PS50C7700 TV - Denial of Service(7/23)
  http:/www.exploit-db.com/exploits/27043

- Samsung Galaxy S III Emergency Contacts Home Button "Passcode Lock" Bypass Weakness(2/25)
  http://secunia.com/advisories/52384/

- Samsung CCTV 관리 웹 애플리케이션
  POC2013 발표자료 참고

국내 관련 보안 취약점들은 공개된 것보다 공개되지 않은 것들이 더 많을 수 있다. 그러므로 국내 관련 보안 취약점들에 대한 연구가 국내 보안 인력들에 의해 더 많이 진행되어야 한다. 특히 '한컴 오피스'의 경우 우리나라 공공기관들이 공식적으로 사용하는 워드프로세스 프로그램이므로 종합적인 보안 취약점 연구가 진행되어야 할 것이다.

3. 제로데이 거래 업체

제로데이 확보는 이제 각국 사이버 전략의 핵심이 되었다. 제로데이의 확보는 강력한 사이버 무기를 확보하는 것이고, 이는 한 국가의 사이버 능력과 직결되기 때문이다. 따라서, 제로데이에 대한 다양한 수요가 발생했고, 이 수요를 적절하게 처리할 수 있는 조직이나 회사들이 등장하고, 다양한 수단과 방법들이 동원되고 있다. 여기서는 공개적으로 제로데이를 구매하는 업체들의 목록과 간단한 소개를 첨부한다.

- Beyond Security SecuriTeam Secure Disclosure
- http://www.beyondsecurity.com/ssd.html
- 이스라엘 보안 업체 Beyond Security 운영
- 취약점 제보자를 구매자와 연결해주고 중간에서 가격 협상을 도와줌

- COSEINC
- http://www.coseinc.com/en/index.php?rt=advisory
- 싱가폴 보안 업체 COSEINC 운영
- Windows, Linux, Solaris 취약점 구매
- 내부 연구진이 직접 취약점을 찾아 공개하기도 함

- Exodus Intelligence Program
• https://www.exodusintel.com/eip
• Exodus Intelligence 운영
• 취약점 제보자 보상과 함께 해당 벤더가 버그 픽스 및 취약점 개선을 할 수 있게 함
• 대상 소프트웨어는 널리 사용되는 소프트웨어 제품에 한하며, 단일 사이트(페이스북, 지메일 등)에서 발생하는 취약점은 구매하지 않음
• 북한, 이란, 쿠바, 시리아 출신 제보자에게는 구매하지 않음

- iDefense Vulnerability Management Services
• http://www.verisigninc.com/en_US/products-and-services/network-intelligence-availability/idefense/vulnerability-intelligence/index.xhtml
• VeriSign iDefense 운영

- iSight Partners GVP Program
• https://gvp.isightpartners.com/program_details.gvp?title=1&page=1
• iSight Partners 운영
• iSight 고객사(일반적인 상용 제품 벤더 및 정부) 제품 취약점 구매
• 해당 취약점이 개선될 수 있게 함

- Netragard Exploit Acquisition Program
• http://www.netragard.com/zero-day-exploit-acquisition-program
• Netragard 운영
• 구매한 취약점은 미국 기반의 클라이언트들에게만 판매함

- Packet Storm Bug Bounty
• http://packetstormsecurity.com/bugbounty
• 보안 포탈 웹사이트 Packet Storm에서 제공하는 취약점 구매 프로그램
• 제로데이 취약점뿐만 아니라 Windows, Java 등 주요 소프트웨어에 한해서는 exploit이 나오지 않은 0.5-day 취약점도 구매
• 제보자가 취약점 정보를 외부에 공개할 시 Packet Storm에서도 전체 공개함
• Microsoft, Mozilla, Adobe 등 주요 제품 취약점에 대해서는 최대 가격(1천달러 대 ~ 7천달러)을 명시해 두고 있으며, 다음은 공개된 거래 내역임

레퍼런스	취약점 내용	거래 가격	거래 일시
APSB13-02	Adobe Reader / Acrobat Code Execution	$7,000.00	2013-01-15
APSB13-01	Adobe Flash Player Code Execution	$7,000.00	2013-01-15
MS13-008	Microsoft Internet Explorer Remote Code Execution	$7,000.00	2013-01-15
MS13-005	Microsoft Windows Kernel-mode Driver Privilege Escalation	$3,500.00	2013-01-15
MS13-002	Microsoft XML Core Services Remote Code Execution	$3,500.00	2013-01-15
MS13-001	Microsoft Print Server Remote Code Execution	$5,600.00	2013-01-15
MS12-082	Microsoft DirectPlay Remote Code Execution	$1,050.00	2013-01-15
MS12-080	Microsoft Exchange Server Remote Code Execution	$2,100.00	2013-01-15
MS12-079	Microsoft Word Remote Code Execution	$2,100.00	2013-01-15
MS12-078	Microsoft Windows Kernel-mode Driver Remote Code Execution	$3,500.00	2013-01-15
MS12-077	Microsoft Internet Explorer Remote Code Execution	$3,500.00	2013-01-15
MS12-076	Microsoft Excel Remote Code Execution	$350.00	2013-01-15
MS12-075	Microsoft Windows Kernel-mode Driver Remote Code Execution	$1,400.00	2013-01-15
MS12-074	Microsoft .NET Framework Remote Code Execution	$350.00	2013-01-15

- Secunia Vulnerability Coordination Reward Program
  - http://secunia.com/community/research/svcrp
  - 덴마크 보안 업체 Secunia 운영
  - 벤더 협상을 포함해 기존에 외부에 공개되지 않은 취약점만 구매
  - 매년 가장 가치 있는 취약점에 대해 시상을 하고 보안 컨퍼런스 참가 기회 제공

- White Fir Design WordPress Security Bug Bounty Program
  - http://www.whitefirdesign.com/about/wordpress-security-bug-bounty-program.html
  - 미국 웹 개발, 보안, 마케팅 업체 White Fir Design 운영
  - 워드프레스와 워드프레스 플러그인 취약점만 구매
  - 워드프레스 취약점은 최소 $100에서 최대 $1,000 사이로 구매
  - 워드프레스 외에도 Drupal, Piwik, DataparkSearch 등 특정 서비스 대상 취약점 구매

- Zero Day Initiative (ZDI)
  - http://www.zerodayinitiative.com/about/benefits/

- HP TippingPoint 운영
- 취약점 등급에 따라 해당 가격과 ZDI 포인트를 부여하고, 포인트에 따라 보너스 금액과 보안 컨퍼런스 참가 기회 제공
- CanSecWest와 PacSec에서 Pwn2Own 이벤트 운영을 통해 제로데이를 구입함

- Injector
- http://www.1337day.com
- 제로데이 취약점 구매와 판매를 동시에 하고 있음
- 거래는 웹머니와 BitCoin을 사용

- Exploit Hub
- https://exploithub.com
- 미국 보안 업체 NSS Labs 운영
- 직접 취약점을 사고 팔 수 있는 합법적 마켓
- 이미 패치가 된 non-0day 취약점만 제보할 수 있고, 허가 받은 바이어들이 이를 직접 구매함

4. Bug Bounty 프로그램

최근 들어 기업들이 버그 바운티 프로그램들을 많이 도입하고 있는 것은 과거와는 달리 자사 관련 보안 취약점들이 높은 가격으로 언더그라운드 시장을 비롯해 폐쇄적인 구조에서 거래가 되고 있어 적절한 대책을 세우기가 용이하지 않기 때문이다. 폐쇄적 구조에서 제로데이 취약점들이 거래되는 것을 막고, 취약점에 대한 신속한 처리를 통해 자사 제품의 신뢰성을 유지하여 보안 취약점으로 인한 수익구조의 악화를 막기 위한 방편이 기업들이 도입하는 버그 바운티 프로그램이라고 할 수 있다.

이 섹션은 취약점 제보 시 금전적인 보상(Rewards), Hall of Fame 등재(Acknowledgement), 기념품 제공 등의 보상을 하는 주요 기업의 취약점 보상 프로그램을 기술하고 있으며, 본 내용은 2013년 11월 27일을 기준으로 작성되었고, 아래 페이지를 주로 참고하여 작성되었다.

- http://bugcrowd.com/list-of-bug-bounty-programs
- http://computersecuritywithethicalhacking.blogspot.kr/2012/09/web-product-vulnerabilty-bug-bounty.html

- http://blog.nibblesec.org/2011/10/no-more-free-bugs-initiatives.html
- http://www.bugsheet.com

Adobe

- 프로그램: Notifying Adobe of Security Issues
- 대상 제품: Adobe 데스크탑, 모바일 전 제품 및 웹사이트를 포함한 모든 온라인 서비스
- 보상 제도: Hall of Fame(공개적으로는 명예의 전당 시스템만 운영한다고 하지만 비공개적으로는 보안팀에서 제로데이를 구매하고 있음)
- 참고: http://helpx.adobe.com/security/alertus.html
  http://helpx.adobe.com/security/acknowledgements.html

Apple

- 프로그램: Apple Product Security
- 대상 제품: Apple 전 제품 및 웹사이트를 포함한 모든 온라인 서비스
- 보상 제도: 웹 취약점에 한해서 Hall of Fame, 제품 취약점에 대해서는 보안 업데이트 공지를 통해 CVE ID 함께 해당 취약점 발견자(제보자) 공개
- 참고: https://ssl.apple.com/support/security/
  http://support.apple.com/kb/HT1318

Artifex

- 프로그램: Bug Bounty Program
- 대상 제품: ghostscript
- 보상 제도: 보상금 $500~$1,000
- 부가 설명: ghostscript는 Artifex에서 제작한 포스트스크립트 PDF 인터프리터 소프트웨어. 각 버그와 이슈를 bugzilla에 공개하고 있음
- 참고: http://www.ghostscript.com/Bug_bounty_program.html

AT&T

- 프로그램: AT&T Bug Bounty Program
- 대상 제품: AT&T 웹사이트, API, 모바일 애플리케이션 등 모든 일반 공개 제품
- 보상 제도: 보상금 $100~$5,000 / Hall of Fame
- 부가 설명: 제보된 취약점을 분기별로 위험도 Top 10으로 선정하여 이를 제보한 사람에게 보상

- 참고: http://developer.att.com/developer/apiDetailPage.jsp?passedItemId=10700235
  http://developer.att.com/developer/apiDetailPage.jsp?passedItemId=13400790

avast!

- 프로그램: The avast! Bug bounty program
- 대상 제품: avast! 제품 중 상용 Windows 버전
- 보상 제도: 보상금 $200~, $3,000~$5,000+(원격코드 실행 취약점)
- 부가 설명: 리비야, 쿠바, 북한 등 미국 제재 국가에서는 취약점 제보 받지 않음, 보상금은 PayPal로 지급
- 참고: http://www.avast.com/bug-bounty

Barracuda Networks

- 프로그램: Bug Bounty Program
- 대상 제품: Barracuda Networks 제품 일부(대상 제품 목록 공개)
- 보상 제도: 보상금 $100~$3,133.7 / Hall of Fame
- 부가 설명: Barracuda Networks는 네트워크, 방화벽, 서버 등 보안 제품 제조 업체
- 참고: http://barracudalabs.com/research-resources/bug-bounty-program
  http://barracudalabs.com/research-resources/bug-bounty-program/bug-bounty-hall-of-fame/

BlackBerry

- 프로그램: Reporting Security Issues
- 대상 제품: BlackBerry 전 제품
- 보상 제도: Hall of Fame
- 참고: https://www.blackberry.com/profile/?eventId=8322
  http://us.blackberry.com/business/topics/security/incident-response-team/collaborations.html

CCBill

- 프로그램: Vulnerability Reward Program
- 대상 제품: CCBill 도메인 일부 웹사이트(대상 사이트 목록 공개)
- 보상 제도: 보상금 $300~$500 / Hall of Fame

- 부가 설명: CCBill은 온라인 영수, 청구 등의 서비스를 제공하는 온라인 지불 업체. 2013년 11월 27일 현재, 취약점 패치 작업 중으로 일시적으로 바운티 프로그램을 중단하고 있음
- 참고: http://www.ccbill.com/developers/security/vulnerability-reward-program.php

Cisco Meraki

- 프로그램: Cisco Meraki Vulnerability Rewards Program
- 대상 제품: Cisco Meraki 웹서비스 및 하드웨어 제품
- 보상 제도: $100~$2,500
- 부가 설명: Cisco Meraki 자체 판단 기준으로 보상금 선정, 리비야, 쿠바, 북한 등 미국 제재 국가에서는 취약점 제보 받지 않음
- 참고: http://meraki.cisco.com/trust/#srp

Coinbase

- 프로그램: Coinbase Bug Bounty Program
- 대상 제품: Coinbase 웹사이트
- 보상 제도: 보상금 비트코인 5+(비트코인 환율) / Hall of Fame
- 부가 설명: Coinbase는 비트코인 거래 업체, 보상금은 비트코인으로 지급
- 참고: https://coinbase.com/whitehat

Cryptocat

- 프로그램: Cryptocat Bug Hunt
- 대상 제품: Cryptocat 소스코드를 포함한 웹서비스
- 보상 제도: 보상금 비공개 / Hall of Fame
- 부가 설명: Cryptocat은 오픈소스 암호화 웹 채팅 서비스
- 참고: https://crypto.cat/bughunt/

djbdns

- 프로그램: The djbdns security quarantee
- 대상 제품: djbdns 소프트웨어 패키지 최신버전
- 보상 제도: 보상금 $1,000
- 부가 설명: djbdns는 개인이 제작 운영하는 DNS 설치 및 구현 패키지
- 참고: http://cr.yp.to/djbdns/guarantee.html

Dropbox

- 프로그램: Dropbox Security
- 대상 제품: Dropbox 웹서비스
- 보상 제도: Hall of Fame
- 참고: https://www.dropbox.com/special_thanks

eBay

- 프로그램: Report a Problem
- 대상 제품: eBay 웹사이트
- 보상 제도: Hall of Fame
- 참고: http://pages.ebay.com/securitycenter/Researchers.html#Researchers, http://pages.ebay.com/securitycenter/ResearchersAcknowledgement.html

Etsy

- 프로그램: Bug Bounty Program
- 대상 제품: Etsy 웹사이트, API, 모바일 애플리케이션
- 보상 제도: 보상금 $500~ / Hall of Fame
- 부가 설명: Etsy는 각종 아이템들을 판매하는 온라인 쇼핑몰
- 참고: http://www.etsy.com/help/article/2463

Evernote

- 프로그램: Evernote Security
- 대상 제품: Evernote 애플리케이션, 플랫폼
- 보상 제도: Hall of Fame
- 참고: https://evernote.com/security/

Facebook

- 프로그램: Bug Bounty Program
- 대상 제품: Facebook 웹사이트 및 사용자 데이터
- 보상 제도: 보상금 $500~ / Hall of Fame
- 부가 설명: 리비야, 쿠바, 북한 등 미국 제재 국가에서는 취약점 제보 받지 않음, 2011년 7월에 버그 바운티 시작, 2013년 8월까지 보상금으로 총 백만 달러 이상 지급, 현재까지 1개 버그 당 최대 보상금은 $20,000

• 참고: https://www.facebook.com/whitehat/
https://www.facebook.com/whitehat/thanks/

Foursquare

• 프로그램: Foursquare Security
• 대상 제품: Foursquare 애플리케이션
• 보상 제도: Hall of Fame
• 참고: https://foursquare.com/about/security

Gallery

• 프로그램: Security Bug Bounties
• 대상 제품: Gallery 3 최신버전
• 보상 제도: 보상금 $100~$1,000 / Hall of Fame
• 부가 설명: Gallery는 온라인 사진 앨범 관리 서비스
• 참고: http://codex.galleryproject.org/Bounties

GitHub

• 프로그램: GitHub White Hat
• 대상 제품: GitHub 웹서비스
• 보상 제도: Hall of Fame
• 참고: https://help.github.com/articles/responsible-disclosure-of-security-vulnerabilities

Google

• 프로그램: Chromium Vulnerability Rewards Program
• 대상 제품: Google Chrome, Google Chrome OS
• 보상 제도: 보상금 $1,000~$10,000+
• 부가 설명: Google 서비스 제품 중 처음 버그 바운티 프로그램 시행, 2013년 8월까지 보상금으로 총 백만 달러 이상 지급, 현재까지 1개 버그 당 최대 보상금은 $60,000
• 참고: http://www.chromium.org/Home/chromium-security/vulnerability-rewards-program
http://www.chromium.org/Home/chromium-security/hall-of-fame

• 프로그램: Web Vulnerability Reward Program
• 대상 제품: Google, Youtube, Blogger, Orkut 웹사이트

- 보상 제도: 보상금 $100~$20,000 / Hall of Fame
- 부가 설명: 2010년 버그 바운티 시작 , 2013년 6월 보상 규모 확대, 취약점 항목별 상세 보상금 공개, 최대 보상금 $20,000는 원격 코드 실행 취약점에 해당, 2013년 8월까지 보상금으로 총 백만 달러 이상 지급
- 참고: http://www.google.com/about/appsecurity/reward-program/
  http://www.google.com/about/appsecurity/hall-of-fame/
- 프로그램: Patch Rewards
- 대상 제품: 오픈소스 프로젝트 일부(대상 오픈소스 프로젝트 목록 공개)
- 보상 제도: 보상금 $500~$3,133.7
- 부가 설명: 2013년 10월 첫 시행, 해당 오픈소스 프로젝트에 패치까지 한 이후 이를 Google에 제보하여 보상받는 방식, 버그 바운티 프로그램에 적용되는 오픈소스 프로젝트를 점차 확대 중
- 참고: http://www.google.com/about/appsecurity/patch-rewards/

Hex-Rays

- 프로그램: Hex-Rays Security Bug Bounty Program
- 대상 제품: IDA, Hex-Rays Decompiler
- 보상 제도: 보상금 ~$3000 / Hall of Fame
- 참고: https://www.hex-rays.com/bugbounty.shtml

IntegraXor

- 프로그램: IntegraXor HMI/SCADA Bug Bounty Program
- 대상 제품: IntegraXor 최신 버전(현재는 4.1 버전)
- 보상 제도: $149~$3,999에 상응하는 I/O 태그(IntegraXor 제품 사용시 필요한 일종의 포인트)
- 부가 설명: IntegraXor는 SCADA 시스템을 관제하는 웹 서버 소프트웨어
- 참고: http://www.integraxor.com/blog/integraxor-hmi-scada-bug-bounty-program

Kaneva

- 프로그램: Kaneva Security Bug Bounty Program
- 대상 제품: Kaneva 게임 서버
- 보상 제도: 보상금 $100(출처) / Hall of Fame
- 부가 설명: Kaneva는 3D 가상 게임

• 참고: http://docs.kaneva.com/mediawiki/index.php/Bug_Bounty

LaunchKey

• 프로그램: LaunchKey Bug reporting & bounty Program
• 대상 제품: LaucnKey 웹서비스, SDK, 라이브러리, 플러그인 등
• 보상 제도: $200~
• 부가 설명: LaunchKey는 패스워드 대체 웹 인증 서비스, 리비야, 쿠바, 북한 등 미국 제재 국가에서는 취약점 제보 받지 않음, 보상금은 PayPal, 비트코인 등으로 지급
• 참고: https://launchkey.com/docs/whitehat

ManageWP

• 프로그램: White Hat Reward
• 대상 제품: ManageWP 웹사이트 및 사용자 데이터
• 보상 제도: 보상금 미공개 / Hall of Fame
• 부가 설명: ManageWP는 WordPress 관리 도구 서비스로 웹 취약점 취급
• 참고: https://managewp.com/white-hat-reward

MEGA

• 프로그램: MEGA Vulnerability Reward Program
• 대상 제품: MEGA 웹서비스
• 보상 제도: 보상금 ~€10,000
• 부가 설명: MEGA는 가상 스토리지 서비스, 2013년 1월 MEGA 웹서비스를 런칭한 이후 바로 버그 바운티 시작
• 참고: https://mega.co.nz/#blog_6

Microsoft

• 프로그램: Report a Computer Security Vulnerability
• 대상 제품: 'Microsoft Online Service'를 포함한 Microsoft 전 제품
• 보상 제도: 'Microsoft Online Service'에 한해서 Hall of Fame 공개
• 참고: http://technet.microsoft.com/da-dk/security/ff852094.aspx
http://technet.microsoft.com/en-us/security/cc308589

• 프로그램: Mitigation Bypass Bounty

- 대상 제품: Windows OS 최신버전(현재는 Windows 8.1)
- 보상 제도: 보상금 ~$100,000
- 부가 설명: 2013년 6월 시작, 2013년 10월에 첫 바운티 수상이 있었음. 프로그램 시작 당시에는 최신 Windows OS에 적용된 보안 기법을 새로운 우회 기법을 이용해 뚫는 것에 한정되어 있었지만, 2013년 11월 1일 프로그램을 확대 개편 하고 나서는 보안 취약점 발견하는 것만으로도 보상 대상이 됨
- 참고: http://technet.microsoft.com/en-us/security/dn425049, http://blogs.technet.com/b/bluehat/archive/2013/11/01/bounty-evolution-100-000-for-new-mitigation-bypass-techniques-wanted-dead-or-alive.aspx

- 프로그램: BlueHat Bonus for Defense
- 대상 제품: Windows OS 최신버전(현재는 Windows 8.1)
- 보상 제도: 보상금 ~$50,000
- 부가 설명: 2013년 6월 시작, Mitigation Bypass Bounty 프로그램과 함께 운영되는 것으로, 제보된 보안 취약점을 개선(방어)하는 방안에 대한 방법을 제보 받음
- 참고: http://technet.microsoft.com/en-us/security/dn425049

- Microsoft는 올 해 6월, 'Mitigation Bypass Bounty'와 'BlueHat Bonus for Defense'를 포함해 3가지 새로운 버그 바운티 프로그램을 발표하였는데, 나머지 하나는 'Internet Explorer 11 Preview Bug Bounty'(http://technet.microsoft.com/en-us/security/dn425036) 프로그램으로, Internet Explorer 11 Preview 버전 테스트를 위해 약 30일 동안 한시적으로 진행된 것으로, 현재는 종료됨

Mozilla

- 프로그램: Security Bug Bounty Program
- 대상 제품: Mozilla 클라이언트 제품 중 Thunderbird, Firefox 등의 공개 버전과 Aurora, EarlyBird 등의 최신 개발 버전(대상 목록 공개), Mozilla 웹 서비스 일부(대상 목록 공개)
- 보상 제도: 보상금 $500~$3,000
- 부가 설명: 2004년 기업 최초로 버그 바운티 프로그램 시작, 각 취약점 별 등급 공개
- 참고: http://www.mozilla.org/security/bug-bounty.html

Nokia

- 프로그램: Nokia Vulnerability Research
- 대상 제품: Nokia 제공 애플리케이션 및 모든 제품(단, Nokia corporate infrastructure 제외)
- 보상 제도: 보상금 비공개 / Hall of Fame
- 참고: http://www.nokia.com/global/security/security/

Oracle

- 프로그램: Report Security Vulnerabilities
- 대상 제품: Oracle 전 제품
- 보상 제도: Hall of Fame
- 부가 설명: 정기 보안 업데이트 'Critical Patch Updates' 공지를 통해 발견된 취약점과 함께 제보자 공개
- 참고:
  http://www.oracle.com/us/support/assurance/vulnerability-remediation/reporting-security-vulnerabilities/index.html

PayPal

- 프로그램: Bug Bounty Program
- 대상 제품: PayPal 웹사이트 일부 및 파트너사 사이트(대상 사이트 목록 공개)
- 보상 제도: 보상금 $100~$10,000 / Hall of Fame
- 부가 설명: PayPal은 인터넷 결제 서비스로 eBay의 자회사, 각 취약점 별 등급 상세 보상금 공개, 리비야, 쿠바, 북한 등 미국 제재 국가에서는 취약점 제보 받지 않음
- 참고: https://www.paypal.com/webapps/mpp/security-tools/reporting-security-issues

Piwik

- 프로그램: Piwik Security Bug Bounty Program
- 대상 제품: Piwik 소프트웨어 또는 관련 플러그인
- 보상 제도: 보상금 $200~$500
- 부가 설명: Piwik은 이메일, SMS 등의 자동 웹 분석 서비스, 2011년부터 프로그램 시행, 보상금은 PayPal로 지급
- 참고: http://piwik.org/security/

Prezi

- 프로그램: Prezi Bug Bounty
- 대상 제품: Prezi 웹서비스(대상 목록 공개)
- 보상 제도: 보상금 $500~ / Hall of Fame
- 부가 설명: Prezi는 클라우드 기반 프레젠테이션 서비스
- 참고: http://prezi.com/bugbounty/

qmail

- 프로그램: The qmail security guarantee
- 대상 제품: qmail 본 서비스와 이와 관련된 NFS, DNS 서버, OS 등
- 보상 제도: 보상금 $500~$1,000
- 부가 설명: qmail은 UNIX 메시지 전송 에이전트
- 참고: http://cr.yp.to/qmail/guarantee.html

Red Hat

- 프로그램: Red Hat Security Contacts
- 대상 제품: Red Hat 제품 또는 서비스
- 보상 제도: Hall of Fame
- 참고: https://access.redhat.com/site/security/team/contact/
  https://access.redhat.com/site/articles/66234

Ripple

- 프로그램: Bug Bounty
- 대상 제품: Ripple 웹서비스 및 사용자 데이터
- 보상 제도: $10~$50에 상응하는 XRP(Ripple 통화 단위)
- 부가 설명: Ripple은 비트코인과 유사한 가상화폐 서비스
- 참고: https://ripple.com/bug-bounty/

Samsung

- 프로그램: Samsung Smart TV Security Bug Contest
- 대상 제품: 삼성 스마트 TV/BD 2011년 모델(D-Series) 및 2012년 모델(E-Series)
- 보상 제도: 보상금 $1,000~ / Hall of Fame

- 부가 설명: 각 제품 출시 이후 2년까지 취약점 제보 받음, 2013년 모델에 대해서는 웹사이트에 업데이트가 되지 않고 있음
- 참고: https://samsungtvbounty.com/Home.aspx
  https://samsungtvbounty.com/HallOfFame.aspx

Tarsnap

- 프로그램: Tarsnap Bug Bounties
- 대상 제품: Tarsnap 소스코드 포함 공개 버전, Preview 버전
- 보상 제도: 보상금 $1~$2,000($100 미만은 Tarsnap 계정 캐쉬로 지급되고, 이 이상은 계정 캐쉬 또는 USD 달러로 지급)
- 부가 설명: Tarsnap은 UNIX 기반 온라인 백업 시스템 서비스, 각 취약점 별 상세 보상금 제시
- 참고: https://www.tarsnap.com/bugbounty.html

Twitter

- 프로그램: Twitter Security
- 대상 제품: Twitter 웹사이트 및 API
- 보상 제도: Hall of Fame
- 참고: https://about.twitter.com/company/security

Yahoo

- 프로그램: Yahoo Bug Bounty Program
- 대상 제품: Yahoo, Flickr 웹서비스, 모바일 애플리케이션
- 보상 제도: 보상금 $250~$15,000 / Hall of Fame
- 부가 설명: 2013년 10월 초 보안 취약점에 대한 보상이 터무니 없이 낮아 여론의 비난을 받은 뒤 곧바로 버그 바운티 프로그램을 시작함, 아직까지는 Yahoo와 Flickr 서비스만 바운티 적용 대상임
- 참고: http://bugbounty.yahoo.com

Yandex

- 프로그램: Bug Bounty Program

- 보상 제도: 보상금 $100~$3,133.7 / Hall of Fame
- 부가 설명: Yandex는 러시아 최대 포털 사이트, OWASP Top-10을 기준으로 보상금 차등 지급
- 참고: http://company.yandex.com/security/index.xml

Zynga

- 프로그램: Zynga Whitehats
- 대상 제품: Zynga 웹서비스, 플랫폼
- 보상 제도: Hall of Fame
- 참고: http://company.zynga.com/security/whitehats