S/W 신규 취약점 신고포상제 운영 안내서

과학기술정보통신부
Ministry of Science and ICT

KISA 한국인터넷진흥원
KOREA INTERNET & SECURITY AGENCY

목 차

제1장
개요

제1장 개요

1.1 운영 배경

> **버그바운티(Bug Bounty)**
> 소프트웨어 또는 웹 서비스의 취약점을 찾아낸 사람에게 포상금을 지급하는 제도

o 구글, MS, 페이스북 등 주요 글로벌 기업은 자사 제품 및 서비스의 취약점 발굴 및 보안강화를 위해 버그바운티를 운영 중

- 소프트웨어 외에 온라인 서비스에도 버그바운티를 도입하는 기업이 증가

o 국내 기업들은 취약점을 제보하면 기업에 대한 간섭으로 인식하거나 공격행위로 간주, 자사 이미지 실추 등의 이유로 제도 도입에 소극적임

- (민간) 삼성전자가(스마트TV) 유일하게 버그바운티를 자체 운영

- (정부) NCSC('07년), KISA('12년)는 취약점을 악용한 침해사고 예방을 위해서 신고포상제를 운영

구분	시행사	프로그램	대상	보상	시행시기
국내	NCSC	국가 사이버안전 위협정보 신고제	모든 S/W, 서비스	~1,000만원	'07
	KISA	S/W 신규 취약점 신고포상제	모든 S/W	5만원~1,000만원	'12.10
	네이버	네이버 보상 프로그램	네이버 서비스, S/W		'15. 2분기
	삼성전자	스마트TV 보상 프로그램	스마트TV	$1,000+α/명예의 전당	'12
국외	구글	구글 취약점 포상 프로그램	웹 서비스	$100~$20,000/명예의 전당	'10.11
		크롬 보상 프로그램	크롬 브라우저, 운영체제	$500~$15,000/명예의 전당	'10.1
		패치 보상 프로그램	오픈소스 S/W 일부	$500~$10,000	13.10
	페이스북	페이스북 버그바운티 프로그램	웹 서비스	$500~/명예의전당	'11.7
	마이크로소프트	보안기법 우회	윈도우 플랫폼	~$100,000/명예의 전당	'13.6
		블루햇 보너스 포 디펜스	윈도우 플랫폼	~$200,000	'13.6
		온라인 서비스 버그바운티	온라인 서비스	$500~$1,500/명예의 전당	'14.9
		스파르탄 프로젝트 버그바운티	최신 브라우저	~$15,000/명예의 전당	'15.4~6
		.NET Core, ASP.NET 버그바운티	웹 개발 툴	~$15,000	'15.10~'16.1
	ZDI	제로데이 이니셔티브	모든 S/W	자체 평가 포상금 / 마일리지 제도	'05.8
	라인	라인 버그바운티	라인 메신저	$500~$20,000/명예의 전당	'15.8~9

<표 1-1> 국내외 기업의 신고포상제 운영사례

1.2 운영 효과

o 신고포상제 운영이 자체 발굴보다 보안 연구비를 절감하고 대량의 취약점을 발견하는데 효율적임

구분	구글 크롬(3년간)		모질라 파이어폭스(3년간)	
	자체 발굴	신고포상제	자체 발굴	신고포상제
취약점 건수	263	371	48	148
지출비용($)	547,500	393,161	547,500	444,000
취약점 건당 지출비용($)	2,082	1,060	11,406	3,000

※ 출처 : 캘리포니아 대학 “취약점 보상프로그램 실증적 연구결과”, 2013

< 신고포상제 운영기업 인터뷰 >

o 한컴社는 “보안 이슈에 적극적으로 참여하는 기업으로 인식되어 기업의 대외 이미지가 향상되고 보안 업데이트 필요성에 대한 고객들의 인식이 변화되기 시작하였다. 또한, 화이트해커 및 관련 업계 담당자와의 소통을 통해 정보 수집이 빨라졌다.”라고 평가함

o 구글은 “버그바운티로 찾아낸 취약점 반 이상이 크롬 베타 버전 향상 등 보안 강화에 큰 보탬이 되었다. 덕분에 사용자들의 불편을 미연에 방지할 수 있었다”고 평가함

o 버그크라우드社는 “버그바운티는 모의침투 테스트나 보안 컨설팅을 받는 것보다 비용적으로 저렴하다. 현재까지 버그바운티 시행 추이를 살펴볼 때 동일한 비용을 투자하여 5배 정도 많은 취약점을 발견할 수 있었다”라고 말함

o 폴리페이먼트社는 “버그바운티를 통해 38개의 버그를 발견한데 반해 두 배 이상의 비용이 들어간 모의침투 테스트에서는 몇 개의 버그만이 발견되었다”라고 말함

1.3 운영 현황

o 보안 취약점을 악용한 침해사고를 사전에 예방하고 취약점 발굴에 대한 보상 체계 마련을 위해 “S/W 신규 보안 취약점 신고포상제”를 운영(’ 12. 10월)

구분	‘12년	‘13년	‘14년	‘15년	‘16년	‘17년	합계
신고건수	23건	179건	274건	321건	696건	810건	2,303건
평가 건수	18건	108건	204건	251건	495건	521건	1,597건
포상건수	14건	89건	177건	215건	382건	253건	1,130건
KISA 포상금액	1,970만원	10,685만원	15,290만원	18,470만원	25,065만원	19,360만원	90,840만원
공동운영사 포상금액	-	-	1,140만원	3,440만원	4,820만원	5,830만원	15,230만원
전체 포상금액	1,970만원	10,685만원	16,430만원	21,910만원	29,885만원	25,190만원	106,070만원

※ 한글(‘14년 2분기), 네이버(‘15년 2분기), 카카오(‘16년 1분기), 네오위즈게임즈(‘16년 3분기), 이스트시큐리티(‘17년 1분기), 이니텍(‘17년 2분기), 잉카인터넷, LG전자(‘17년 3분기), 지니언스, 카카오뱅크, 안랩(‘17년 4분기), 하우리(‘18년 1분기) 자사 취약점 대해 포상금 지급

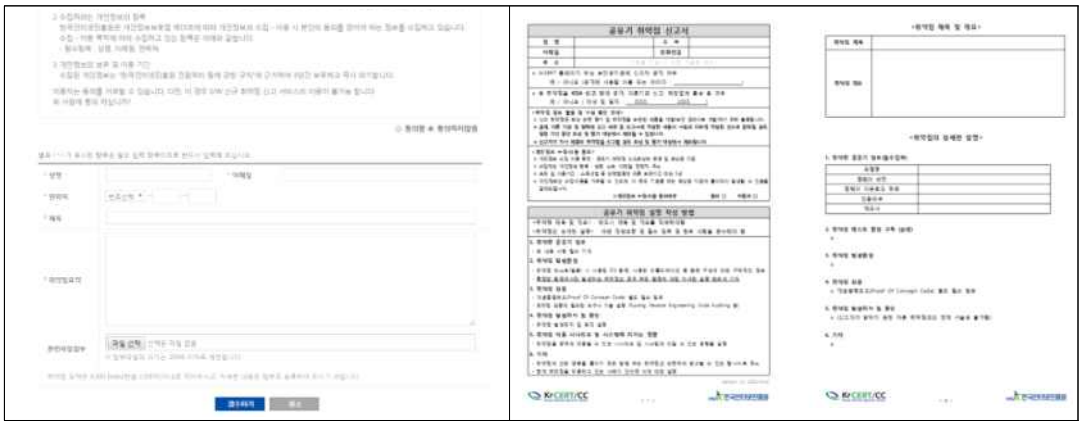
o 한컴社의 경우 지속적인 취약점 발굴 및 보완으로 최신버전인 한글 2014에서는 보안성이 강화되었음(’15. 5, 취약점 신고포상제 자문회의)

제2장
신고포상제 절차

제2장 신고포상제 절차

o (신고접수) 인터넷침해대응센터 홈페이지(www.krcert.or.kr)의 취약점 신고 코너를 통해 메일로 접수

<그림 2-1> 신고포상제 신고접수 및 신고양식



o (신고대상) 최신 버전의 소프트웨어에 영향을 줄 수 있는 신규 취약점

※ 홈페이지 등 현재 운영 중인 서비스에 대한 취약점은 불법적인 해킹 조장 우려 및 관련법(망법 제48조)에 따른 검증권한 부재로 평가 및 포상 대상에서 제외

o (취약점 평가) 검증→ 1차 평가 → 2차 평가 3단계로 평가

① 검증(KISA) : 취약점 기본 정보 파악 및 신규 취약점 여부 판단

※ 신고된 내용만으로 검증이 불가능한 경우 보완 요청, 신규 취약점이 아닌 경우 신고자에 피드백

② 1차 평가(KISA) : 취약점별 분석환경 구축·테스트 및 평가기준 기반 평가

③ 2차 평가 : 외부 평가위원회에서 1차 평가결과 검토 및 포상금 결정

※ 평가위원은 교수, 취약점 전문가(화이트해커), S/W제조사 등 5명으로 구성하되, 공동운영사 제품이 포함된 경우 공동운영사를 평가위원에 포함

o (평가대상) 평가일이 속한 월의 3개월 전의 초일부터 평가일 전월 말일까지 접수된 취약점 중 평가요건에 부합한 건을 대상으로 함

※ 평가요건 : 최신 버전의 소프트웨어에 영향을 줄 수 있는 신규 취약점으로 국내 파급력이 있으며, 외부에 공개되지 않은 취약점

차수	평가일	접수기간
1차	3월 둘째주 목요일	전년 12월 1일 ~ 금년 2월 말일
2차	6월 둘째주 목요일	금년 3월 1일 ~ 금년 5월 31일
3차	9월 둘째주 목요일	금년 6월 1일 ~ 금년 8월 31일
4차	12월 첫째주 목요일	금년 9월 1일 ~ 금년 11월 30일

<신고포상제 평가일정>

2.1 취약점 평가기준

o (기본방향) 보안 취약점 평가 국제 표준(CVSS), 해외 취약점 평가 체계(CWSS)를 기반으로 평가기준 수립

o (평가기준) 취약점에 영향 받는 시스템 측면에서 출현도와 영향도를 평가하고, 취약점을 악용하는 정도와 취약점 발굴 수준을 평가

대분류	소분류	내용
출현도	보급범위	해당 취약점이 발견된 소프트웨어 등 제품의 보급정도를 평가
	영향범위	침해 가능한 버전 범위(전 버전, 일부버전 영향정도)
영향도	기밀성	공격 성공시 영향받는 시스템에 끼치는 기밀성 측면에서의 영향
	무결성	공격 성공시 영향받는 시스템에 끼치는 무결성 측면에서의 영향
	가용성	공격 성공시 영향받는 시스템에 끼치는 가용성 측면에서의 영향
	피해의심각성	공격 성공시 비즈니스 혹은 임무에 미치게 되는 잠재적인 영향
공격 효과성	접근벡터	공격을 수행하기 위한 경로의 접근 용이성 정도
	권한요구도	공격을 수행하기 위한 접근 권한의 정도
	상호작용정도	공격을 성공시키는데 피해자의 협조적인 행동의 요구 수준
	공격의 신뢰성	취약점을 이용하여 공격이 성공할 비율
발굴 수준	발굴 난이도	취약점 발굴 시 기술의 난이도
	문서완성도	신고문서에 대한 내용의 충실도 및 구성의 완성도

<평가항목 개요>

2.2 포상금 지급기준

o (포상기준) 평가점수 25점(100점 만점) 이상인 취약점을 대상으로 평가점수에 따라 차등지급(최소 5만원~최대 1,000만원/건)

점수	포상금액	비고
0~25 미만	-	-
25~30 미만	5	
30~35 미만	10	+40
35~40 미만	50	
40~45 미만	90	
45~50 미만	150	+60
50~55 미만	210	
55~60 미만	270	
60~65 미만	350	+80
65~70 미만	430	
70~75 미만	510	
75~80 미만	590	
80~85 미만	670	
85~90 미만	750	
90~95 미만	830	
95~100 미만	910	
100	1,000	+90

<취약점 평가점수별 포상금액>

※ 포상금은 분기별 평가위원회에서 제반사항 고려하여 최종적으로 결정

※ 공동운영사 직원 및 가족, 협력업체 직원 등 회사와 이해관계가 있는 경우 포상대상에서 제외

※ 무작위 대입 공격, 서비스 거부 공격, 제3자의 계정이나 데이터에 접근, 허가되지 않은 서버 침투 시도 등 취약점 분석 과정에서 비즈니스, 서비스, 사용자들에게 피해를 끼치는 경우 포상대상에서 제외

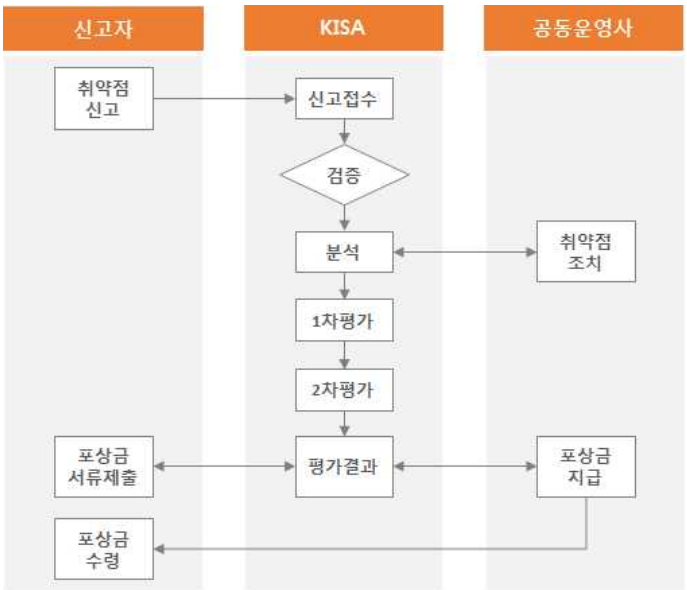
제3장

공동 운영사

제3장 공동 운영사

3.1 공동운영 협의사항

o (업무분장) KISA는 취약점 접수 및 평가를 실시하며, 공동운영사는 취약점 평가 회의 참석 및 포상금 지급



o 공동운영사는 운영시기, 신고대상, 포상대상, 포상금 지급방식 등을 KISA와 협의 후 결정

- 신고/포상 대상은 공동운영사의 일부 제품만을 대상으로도 운영 가능
- 포상금 지급을 위한 관련 서류는 KISA에서 취합 후 공동운영사에 전달

제4장

참고자료

[붙임1] 버그바운티 운영의 필요성 보도자료

국내 기업들, 시큐리티 버그 바운티 적극 도입해야! (데일리시큐, 2013-06-21)
http://dailysecu.com/news_view.php?article_id=4584

특히 “구글은 시큐리티 버그 바운티(Security Bug Bounty) 제도를 도입해 취약점을 찾아주면 돈을 준다. OS의 메인 취약점을 찾아주면 8만불, 우리돈으로 거의 9천만원에 가까운 돈을 지불하고 취약점을 산다. 페이스북도 마찬가지로 취약점을 찾아주면 돈을 주고 이 과정을 통해 서비스 안정화를 도모하고 있다. 처음에는 취약점이 많아 돈이 많이 나가지만 점차 취약점이 줄어들어 나중에는 지출이 줄어들게 돼 있다. MS도 이 제도를 도입하기로 결정했다. 결국 **미국 기업들은 서비스 안정화를 위해 아낌없이 돈을 지불하고 결국 그 투자가 비즈니스에 도움이 된다**는 것을 알고 있다”고 말했다.

한편 한국에 대해서도 그는 “한국도 요즘 KISA에서 취약점을 찾아주면 돈을 준다. 하지만 너무 작다. 좀더 투자가 필요하다. 여전히 기업들은 취약점을 찾아주면 싫어한다. 이는 KISA나 정부기관보다는 한국 대기업들이 앞장서서 제도 도입을 해야 한다”며 “특히 군 내부에서도 버그 바운티를 실시해 취약점을 찾아주는 장병에게 휴가를 준다든지 좋은 방향으로 사용한다면 군 시스템 안정화에 큰 도움이 되지 않을까 생각한다. **취약점을 방치하면 대형 사고를 당해 더 큰 비용이 지출된다는 것을 알아야 한다”**고 강조했다.

[붙임2] 보호나라&KrCERT 홈페이지 게시

□ 신고포상제 안내 페이지

o 상담 및 신고 > 취약점 신고 하단에
포상제 운영 안내서 및 공동운영사의 정보보호 활동 안내 및 게시