소프트웨어 개발자를 위한

취약점 공개 가이드라인

정보 보호 조기 경보 파트너쉽 가이드라인 부록 5

목차

2008년 7월

INFORMATION-TECHNOLOGY PROMOTION AGENCY, JAPAN
JAPAN COMPUTER EMERGENCY RESPONSE TEAM COORDINATION CENTER
JAPAN ELECTRONICS AND INFORMATION TECHNOLOGY INDUSTRIES ASSOCIATION
COMPUTER SOFTWARE ASSOCIATION OF JAPAN
JAPAN INFORMATION TECHNOLOGY SERVICES INDUSTRY ASSOCIATION
JAPAN NETWORK SECURITY ASSOCIATION

한국어 번역 : 구동언 (8con@nchovy.kr)
NCHOVY 인터넷 스톰 센터

1. 소개

품질과 신뢰성 보장의 측면에서, 소프트웨어를 제작하는 개인과 기업(소프트웨어 개발자로 통칭한다)이 사용자에게 안전한 소프트웨어를 제공하는 것은 중요한 일이다. 보안을 철저히 고려해서 설계한 소프트웨어라도 보안 구멍을 가질 수 있기 때문이다.

소프트웨어 개발자가 제품이 가지고 있는 취약점을 공개하지 않거나, 문제를 일으킬 수 있는 결함을 숨기거나, 충분하지 않거나 잘못된 정보를 제공할 경우, 소프트웨어는 사용자의 중요한 정보를 위험에 빠뜨릴 수 있다. 그렇기 때문에 소프트웨어 개발자는 문제가 생겼을 경우 가능한 빨리 조치를 취해야 하며, 사용자에게 취약점에 관한 정확한 정보를 제공해야 한다.

그러나 현재 많은 소프트웨어 개발자들은 제품의 취약점을 공개해 본 경험이 없거나 좋지 않은 방법으로 잘못된 정보를 사용자에게 알려주어, 사용자가 필요로 하는 정확한 정보를 취득하지 못하도록 하고 있다.

이 가이드라인의 최우선 목표는 사용자가 필요로 하는 취약점 정보를 제대로 전달할 수 있는 정책과 절차를 소프트웨어 개발자들에게 알리는 것이다.

2. 취약점 정보 : 사용자가 원하는 정보를 제공하라

소프트웨어 개발자가 취약점을 공개함에 있어 개발자는 사용자가 취약점에 관한 어떤 정보를 필요로 하는지 알아야 한다. 소프트웨어 개발자가 보안 패치를 제공하면서 충분한 정보를 공개하지 않는다면, 이 패치로 인해 사용자가 혼란에 빠질 수 있다. 아래에 나오는 내용들은 사용자들이 원하는 정보들의 목록과 그에 관한 설명이다.

(1) 제품 이름과 버전

일단, 사용자들은 공개된 취약점이 자신에게 해당되는지 알고 싶어 한다. 그렇기에 공개된 취약점이 어느 제품의 어느 버전에 해당하는지 쉽게 파악할 수 있도록 정보를 제공해야 한다.

(2) 취약점 정보 공개 일자

사용자는 웹사이트에 있는 오래된 정보라도 최근의 것이라고 생각할 수 있다. 그러나 취약점 정보는 최근에 공개된 것일수록 사용자에게 더 많은 영향을 끼칠 가능성이 크다. 다시 말하면 오래된 취약점은 이미 해결된 것일 수도 있다는 것이다. 취약점 정보와 함께 날짜를 제공한다면, 사용자는 해당 취약점을 패치했는지 확인할 필요가 없게 된다.

(3) 위협

몇몇 사용자는 공개된 취약점의 위험도가 낮으면 조치를 취하지 않고, 위험도가 높으면 조치를 취한다. 그렇기 때문에 이 패치를 하지 않았을 경우 생길 수 있는 문제점을 구체적으로 공개해야 한다.

(4) (패치를 하지 못할 경우) 차선책

사용자가 보안 패치를 하지 못하는 여러가지 경우가 있다. 그러나 패치를 하지 않고도 문제를 회피할 수 있거나 위험을 낮출 수 있는 차선책이 있다면, 그 방법을 공개해야 한다. 개발자가 보안 패치만 제공하고 상세한 정보를 제공하지 않는다면 차선책을 사용하기 힘들어지고, 보안 패치를 할 수 없는 상황에 놓인 사용자는 위험에 빠질 수 있다. 개발자가 차선책을 알고 있다면, 그것을 어떻게 적용해야 하는지 공개해야 한다.

(5) 추가 정보

사용자는 취약점에 대해 자세히 파악하기 위해 개발자가 공개한 정보 이외에도 다른 추가적인 정보를 찾아본다. 따라서 사용자가 참조할 수 있는 추가정보를 제공해야 한다.

3. 어떤 정보를 공개해야 하는가 : 취약점 정보 항목 및 공개 예제

3장에서는 소프트웨어 개발자가 취약점을 웹사이트에 공개할 때 포함해야 하는 항목과, 좋은 공개 예제/나쁜 공개 예제를 설명한다.

3.1 취약점 정보에 포함해야 하는 항목들

사용자에 따라 필요로 하는 정보의 항목은 다르다. 시스템 관리자는 취약점의 위협에 관한 자세한 정보와 회피할 수 있는 방법을 원한다. 그에 반해, 일반 사용자는 취약점을 가진 제품을 사용하고 있는 경우 어떤 방법으로 확인하고, 취약점을 해결할 수 있는지 쉽게 쓰여진 설명을 필요로 한다. 그렇기에 개발자는 자신의 제품을 사용하는 사람들이 어떤 사람인지, 그리고 어떤 정보를 제공해야 하는지 확인해야 한다.

아래의 목록은 일반적으로 취약점 정보를 공개할 때 사용하는 순서이다.

3.1.1 제목

사용자가 검색 엔진을 이용하여 들어올 경우, 정확히 파악하고 들어올 수 있도록 제품 이름을 포함해야 한다. 또한 한 제품이 여러가지 취약점을 가질 수 있기 때문에, 각각의 취약점을 구분할 수 있도록 취약점 번호와 취약점의 이름을 포함한다.

3.1.2 요약

사용자가 중요한 내용을 빨리 파악할 수 있도록 취약점에 관해 요약한 내용을 문서에서 가장 먼저 제공한다.

3.1.3 취약점을 가지고 있는 제품 이름

취약점을 가지고 있는 제품의 이름과 버전을 공개하고, 어떻게 제품의 이름과 버전을 확인할 수 있는지 설명한다.

3.1.4 설명

사용자들이 이 제품에 관련된 다른 취약점과 혼동하지 않도록 이름, 원인 그리고 추가 정보를 정확하게 설명한다.

3.1.5 위협
취약점이 얼마나 위험한 것인지 확인할 수 있는 정보를 제공한다. 예를 들면 취약점이 공격에 노출되었을 때의 위험의 정도와 공격의 성공 가능성 등이다.

3.1.6 해결책
취약점이 수정된 제품을 설치하거나, 제품을 업데이트 하거나, 보안 패치를 적용하는 방법을 제공한다.

3.1.7 차선책
운영 중이거나 기타 다른 이유로 보안 패치를 적용하지 못하는 경우, 사용자가 취약점이 공개된 제품을 보호할 수 있는 다른 방법이 있다면 공개한다.

3.1.8 참조
사용자가 참조할 수 있는 추가 정보가 있다면, 링크를 참조 형태로 제공한다.

3.1.9 공헌
많은 소프트웨어 개발자들은 취약점을 발견하고 알려준 공헌자들에게 감사를 표시한다.

3.1.10 변경 내역
취약점이 공개된 날짜를 확실히 알 수 있도록 한다. 취약점에 관한 정보가 수정되면, 언제 무엇이 바뀌었는지 추가로 기재한다.

3.1.11 연락처
보안 패치에 문제가 있거나, 공개된 정보가 명확하게 이해되지 않을 경우 연락할 수 있는 연락처를 제공한다

3.1.12 정보 공개 예제
아래에 나오는 취약점 공개 형식은 사용자 층을 알 수 없는 경우 취약점 정보를 공개하기 위한 방법으로써, 소비자 제품 리콜 안내서의 예제와 관련이 있다.

- **바람직한 취약점 공개 예제**

보안 취약점 정보 > 제품명 : 가나다

IPASA2007-001 : 가나다의 버퍼 오버플로우 취약점

최초 작성일 : 2007년 1월 1일
마지막 수정일 : 2007년 1월 9일

■개요

가나다의 버전 1.5.4와 그 이전 버전에서 버퍼 오버플로우 취약점이 발견되었습니다. 가나다가 설치된 컴퓨터가 공격을 당하게 되면, 원격 공격자에게 임의의 바이너리를 실행할 수 있는 권한을 허용합니다.

■취약 제품 목록

아래의 제품들이 이번에 공개된 취약점을 가지고 있습니다.

제품명 : 가나다
취약점을 가지고 있는 버전
1.5.4(윈도우즈 XP SP2)와 그 이전 버전
1.5.4(리눅스)와 그 이전 버전

가나다의 버전 확인하기
1. 가나다를 실행한 후, 도움말 메뉴에서 버전 정보를 클릭합니다.
2. 팝업창의 마지막 줄에 버전 정보가 있습니다.

■설명

가나다는 압축 해제 기능을 가지고 있습니다. 데이터 어플리케이션 스위트의 데이터 관리 서비스의 한 부분인 이 압축 해제 기능은 취약점을 가지고 있어, 원격 공격자가 인터넷을 통해 임의의 코드를 실행할 수 있도록 허용합니다.

IPASA2007-001 기술 정보

■위협

이 소프트웨어가 시스템 관리자 계정으로 작동할 때 공격을 성공한다면, 원격 공격자는 시스템의 전체 권한을 가질 수 있습니다. 공격자는 시스템 관리자 권한으로 악성 코드를 심거나, 데이터를 변조/삭제 하는 등 임의의 행동을 할 수 있습니다.

■해결책

1.0.0 혹은 그 이전 버전을 사용하는 경우, 삭제하고 새 버전을 설치합니다.
1.0.0 이후의 버전을 사용하는 경우, 보안 패치를 설치합니다.

자세한 설치 방법은, 보안 패치 혹은 새 버전에 포함되어 있는 readme.txt를 참고하세요.

제품명 가나다
다운로드 할 수 있는 보안 패치
1.5.5 patch.zip (윈도우즈 XP SP2용) 2007.1.4
1.5.5 patcg.tgz (리눅스용) 2007.1.4

- 패치 작업을 통해 아래의 설정 파일이 교체됩니다.
  xxxxx.cfg, yyyyy.dif

■차선책

아래의 방법으로 취약점을 감소시킬 수 있을 것입니다.

- 차선책
  신뢰할 수 있는 사용자만 가나다의 관리 권한을 이용할 수 있도록 IP를 필터링 합니다.

■참조

JVN#12345678 가나다의 버퍼 오버플로우 취약점

■공헌

이 취약점을 찾아주신 아무개 님께 감사 드립니다.

■변경 내역

2007.01.4 문서 공개
2007.01.9 소프트웨어가 특정한 권한으로 실행되었을 때 생기는 경우에 관한 정보를 추가했습니다.

■연락처

전화 123-456-7890 (근무시간 10:00 - 17:00)
이메일 example@example.co.jp

- **바람직하지 않은 취약점 공개 예제 (1)**

가나다 업데이트 안내

최근 저희는 가나다의 압축 해제 기능이 몇가지 특정한 상황에서 불안정하게 작동하는 것을 파악하였습니다. 제한된 상황에서 발생할 수 있는 문제임에도 불구하고, 저희는 가나다의 업데이트를 제공합니다. 저희는 사용자 분들께 도움을 드릴 것이며, 제품을 안전하게 만들기 위해 최선을 다하겠습니다.

■업데이트 프로그램

가나다 1.5.5.zip (윈도우용) 가나다 1.5.5.tgz (리눅스용)

이 예제에서 잘못된 점

- 취약점이 있는 제품을 업데이트 하라고 하는 것처럼 보이지만, 사용자가 이 문서의 정확한 의도가 무엇인지 파악하기 힘들다.
- 이런 문서 형식은 사용자들에게 종종 보내는 홍보메일과 비슷하다. 그렇기 때문에 사용자들이 취약점 정보에 대해 관심을 보이지 않는다.
- 이 문서는 취약점의 위험성에 대해 명확하지 않게 설명한다. 그리고 사용자가 즉각 취해야 하는 확실한 조치가 무엇인지 알 수 없다.
- 사용자는 업데이트 된 프로그램을 어떻게 설치하는지 알 수 없기 때문에 조치를 취할 수 없다.
- 이 문서의 발행 날짜를 알 수 없기 때문에, 취약점에 대해 조치를 취했는지 안 했는지 확실하게 파악할 수 없다.

- **바람직하지 않은 취약점 공개 예제 (2)**

가나다 릴리즈 노트

2007.1.4 버전 1.5.5

- 이메일 보내기 기능에 헤더 수정 기능 추가
- 파일 업로드 기능에서 너무 긴 파일이름이 전송될 경우 생기는 버퍼 오버플로우 문제 해결
- 소소한 버그 해결

2006.11.28 버전 1.5.4

- 파일 업로드 기능 추가

이 예제에서 잘못된 점

- 사용자들은 이 문서가 기능 추가에 관한 문서인지, 취약점에 관한 문서인지 알 수 없다.

4. 어떻게 제공할까 : 취약점 정보를 웹사이트에서 전달하기 위한 네비게이션

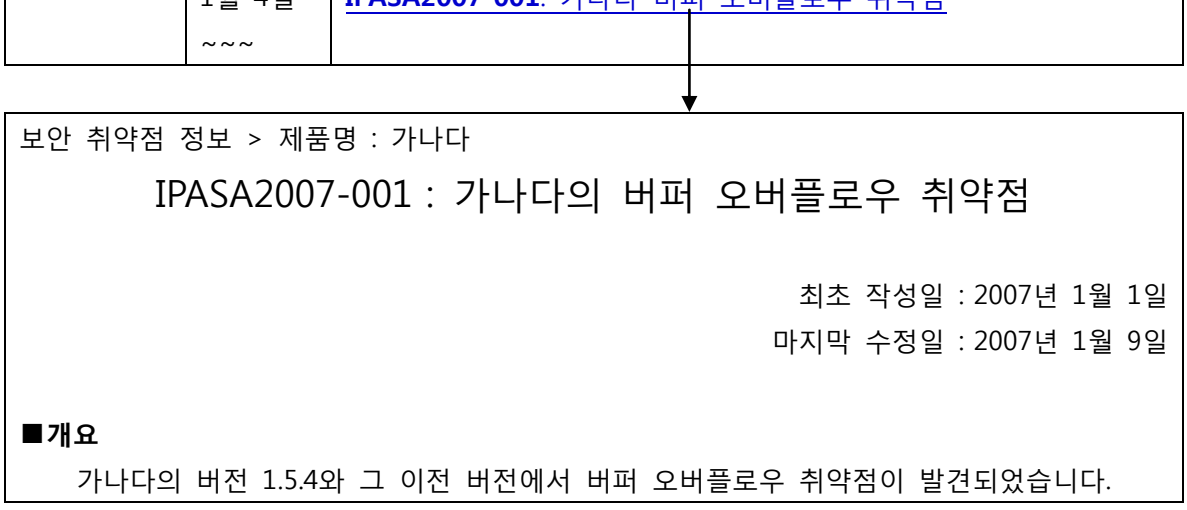
이 장은 웹 사이트에서 취약점 정보를 접근하게 하는 방법에 관한 권고를 제시한다. 예제를 통해 추천하는 방법과 추천하지 않는 방법을 다룬다.

취약점 정보를 위한 좋은 웹 사이트 디자인

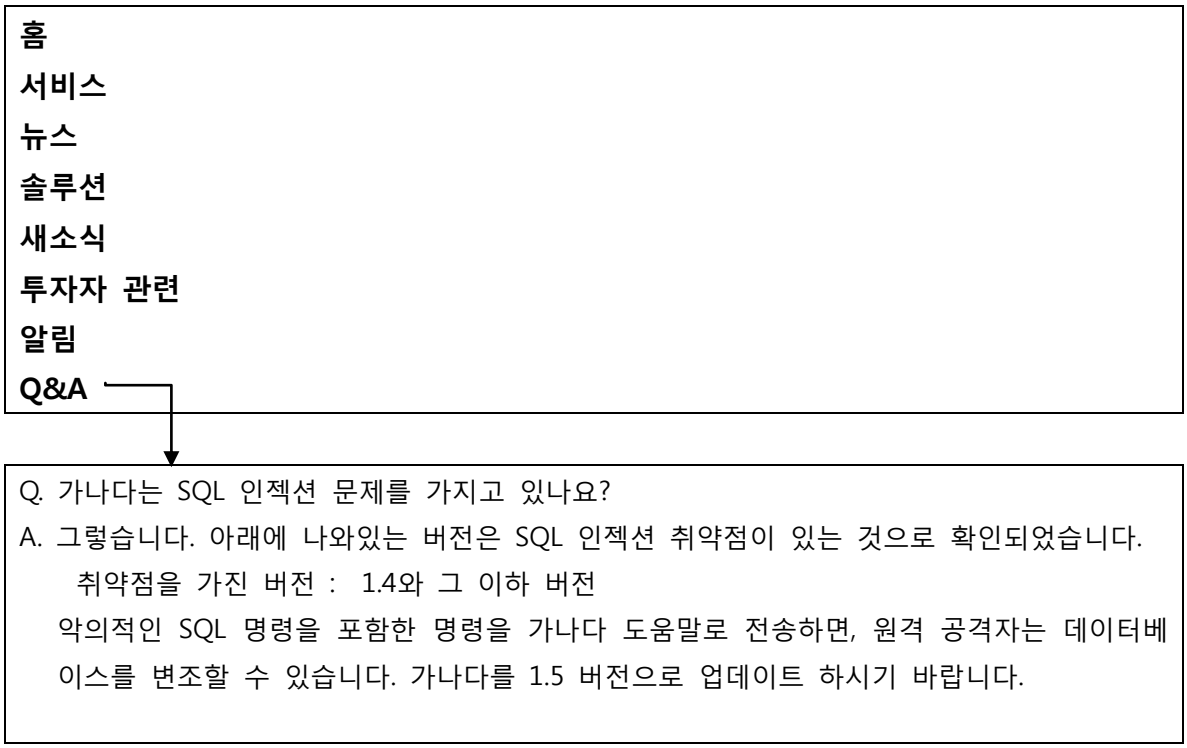
- 사용자들이 취약점 정보를 보기 위해 여러 계층을 통하지 않고, 쉽게 접근할 수 있도록 해야 한다. 취약점 정보를 제공하는 사이트가 복잡한 계층을 가지고 있다면, 사용자들이 취약점 정보에 접근하는 것이 힘들다.
- 각각의 취약점 제목에 취약점 정보를 볼 수 있는 링크를 제공한다.
- 마지막 변경 일자를 제공한다

- **추천하는 웹 디자인 예시**

홈 **최근 소식** **투자자 관련** **연락처**	2007년 **취약점** **정보** 1월 15일 1월 6일 1월 4일 ~~~	**중요 알림 : 보안 권고** **IPASA2007-003**: 가나다2 버퍼 오버플로우 취약점 보안 패치 공개 **IPASA2007-002**: 가나다2 임의 코드 실행 취약점 보안 패치 공개 **IPASA2007-001**: 가나다 버퍼 오버플로우 취약점



- **바람직하지 않은 웹 디자인의 예**



이 예제에서 잘못된 점

1. 취약점 정보가 다른 정보와 섞여있다.
2. 취약점 정보가 다른 정보와 섞여있어서 취약점 정보인지 아닌지 구분하기 힘들다.
3. 상당수의 사용자는 이 페이지에서 취약점 정보를 찾지 않는다.
4. 취약점 정보가 발표되었을 때 사용자들이 어디서 이 정보를 볼 수 있는지 알 수 없다.

5. 참조

경제 산업성, 제품 안전부, 소비자 제품 리콜 안내서, 2002년 5월, 47페이지
http://www.meti.go.jp/policy/consumer/seian/contents/recall/handbook.pdf (일본어)

배경

최근 몇 년, 일본의 소프트웨어와 웹 어플리케이션의 취약점 발견 횟수가 급격히 증가하였고, 무단접근과 바이러스로 인해 정보가 유실되거나 개인정보가 노출되는 사고가 발생하였다.

취약점을 처리하는 정책을 세우기 위하여, 경제산업성의 지시로 "소프트웨어 취약점 처리 표준"과 "정보 보호 조기 통제 파트너쉽 가이드라인"을 작성하였다. 두 문서는 취약점과 관련된 당사자들에게 추천하는 취약점 처리 방법을 설명하기 위하여 만들어졌다.

이 문서는 "정보 보호 조기 통제 파트너쉽 가이드라인"의 부록 5번이다. 이 문서는 소프트웨어 개발자를 대상으로 하며 또한 실행할 수 있는 정책을 제시함으로써 취약점을 적합한 방식으로 공개하도록 장려하고자 한다.

우리는 소프트웨어 개발자들이 취약점을 공개하며 사용자들에게 필요한 정보를 제공할 때 이 문서들을 참조하길 권장한다.

이 문서는 제한 없이 배포할 수 있으며 아래의 링크에서 받을 수 있다.

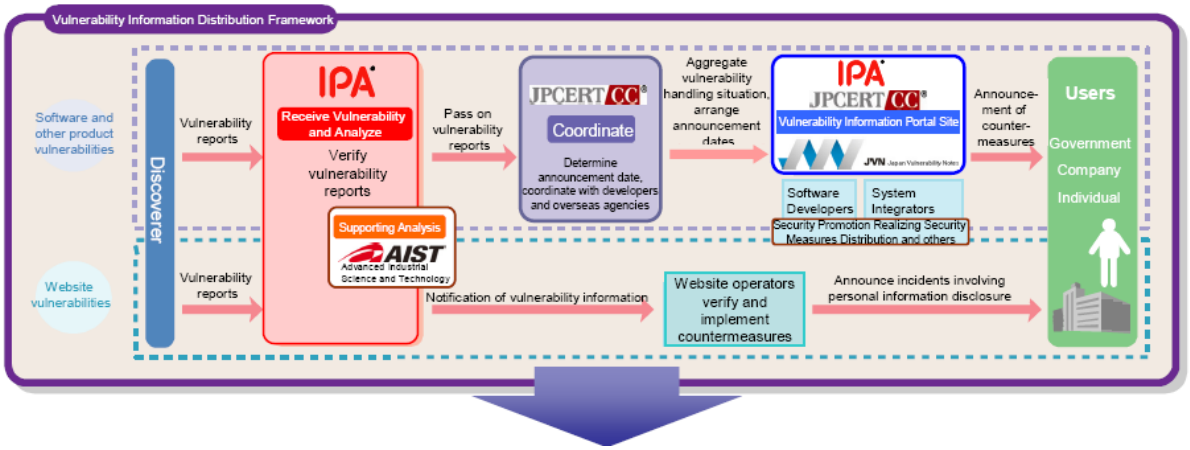
http://www.ipa.go.jp/security/english/third.html (영어)

http://www.jpcert.or.jp/english/vh/guidelines.html (영어)

http://www.ipa.go.jp/security/ciadr/partnership_guide.html (일본어)

http://www.jpcert.or.jp/vh/#guideline (일본어)

취약점 관련 정보 처리 구조 =정보 보호 조기 통제 파트너쉽=



기대 효과 1. 웹사이트 운영자와 제품 개발자로부터 입수된 취약점 해결책 홍보

2. 취약점 정보가 공유되지 않는 것을 방지

3. 중요 정보 시스템 및 개인정보와 같은 중요 정보 손실 방지

연락처

Security Center, Information-Technology Promotion Agency, Japan （IPA）
2-28-8 Honkomagome, Bunkyo-ku, Tokyo 113-6591, Japan
http://www.ipa.go.jp/security/ TEL: +81-(0)3-5978-7527 FAX: +81-(0)3-5978-7518
Japan Computer Emergency Response Team Coordination Center （JPCERT/CC）
Hirose Bldg. 11F, 3-17 kanda-nishikicho Chiyoda-ku, Tokyo 101-0054, Japan
http://www.jpcert.or.jp/ TEL : +81-(0)3-3518-4600 FAX : +81-(0)3-3518-4602

소프트웨어 개발자를 위한 취약점 정보 공개 가이드라인

정보 보호 조기 통제 파트너쉽 가이드라인 부록 5

발간일 : 2007년 5월 30일 1쇄

2008년 4월 4일 3쇄, 2008년 7월 29일(영어판)

편집자 : 정보 시스템 취약점 정보 처리 스터디 그룹

담당기관 : 일본 정보 기술 진흥원