컴퓨터 사용자를 위한 월간 정보보호 인식 뉴스레터

OUCH!

이달 호 주제..

- **하트블리드란?**
- **대응방법**
- **피싱/스미싱 공격 주의**

하트블리드- 대응방법

개요

4월 7일(월), OpenSSL이라는 굉장히 많이 사용되는SSL 프로토콜 프로그램에서 심각한 취약점이 발견되었다. SSL은 인터넷에서 사용되는 중요한 보안 프로토콜이다. SSL은 온라인 통신 암호화뿐만 아니라, 온라인 쇼핑 및 뱅킹할 때 합법적인 웹사이트를 검증해주는 기능을 한다. 이번 특별 판 뉴스레터에서는 이 취약점이 무엇인지 그리고 우리를 보호할 수 있는 방법을 알려준다.

객원 편집자

제이크 윌리엄스(@MalwareJake; malwarejake.blogspot.com)는 CSR그룹 컴퓨터 보안 컨설턴트에서 수석과학자이다. 제이크는 메모리 포렌식(FOR526) 및 악성코드 역공학(FOR610) 과정의 공동 저자이다.

하트블리드란?

해커가 하트블리드 취약점을 이용해서 웹 서버에 접속하여 패스워드 등 인증정보 등 민감한 정보를 수집할 수 있다. 만약에 공격자들이 이러한 정보를 수집할 수 있다면, 이를 이용하여 동일한 ID와 패스워드를 사용하는 계정에 로그인할 수 있다. 이 취약점은 과거2년 동안 존재하였지만 4월 7일이 되어서야 발견되고 공개되었다. 하트블리드는 윈도 및 맥 컴퓨터에는 영향이 없으며, 우리가 사용하는 페이스북, 지메일 등 인터넷의 웹 사이트에 주로 영향을 미친다. 이 문제가 복잡한 이유는 인터넷의 모든 웹 사이트에 영향을 미치는 것이 아니지만, 대부분의 사이트에 영향을 준다는 것이다. 우리들이 사용하는 웹 사이트가 취약한 지 확인하려면 아래의 Lastpass 사이트에서 점검 도구를 이용하면 된다.
https://lastpass.com/heartbleed/.

대응방안

우리를 보호하기 위해 취할 수 있는 여러 가지 단계가 있다. 이러한 단계는 하트블리드 취약점으로부터 보호할 수 있을 뿐만 아니라, 미래에 다른 공격도 보호할 수 있다.

- 먼저 사용하고 있는 웹 사이트의 패스워드를 변경해야 한다. 그리고 먼저 가장 중요한 웹 사이트부터 변경해야 한다. 만약에 사용하는 웹 사이트는 취약한 지 모른다면, 어쨌든 패스워드를 변경하는 것이 좋다. 이번 기회에 패스워드를 업데이트하고 온라인 보안을 강화해야 한다.
- 패스워드를 변경할 때, 강력하고 추측하기 어려운 것으로 변경해야 한다. 추가로 만약에 웹사이트에서 2단계 인증기능을 지원한다면 이를 사용해야 한다. 2단계 인증기능은 온라인 계정을 더 안전하게 만들 수 있다.
- 온라인 계정마다 서로 다른 패스워드를 사용해야 한다. 이렇게 하는 경우 웹사이트 한 곳이 해킹되더라도, 다른 사이트의 계정은 안전하다. 패스워드를 전부 기억하는 것이 어려울 수 있다. 이런 경우 패스워드를

하트블리드- 대응방법

안전하게 저장하는 패스워드 관리프로그램을 사용할 것을 권고한다. 패스워드 관리프로그램은 온라인 활동을 간편하게 관리할 수 있을 뿐만 아니라, 더욱 안전하게 만들 수 있는 최고의 도구이다.

- 이메일 프로그램도 주의를 기울어야 한다. 아웃룩, 애플 메일과 같은 이메일 프로그램은 메일 서버로 접속 시 SSL을 사용하고 있다면, 마찬가지로 패스워드를 변경해야 한다.

추가적인 단계에 대해서 좀더 많은 정보를 원하면, 뉴스레터 끝 부분의 참고자료 부분을 확인하기 바란다.

하트블리드 취약점으로부터 우리를 보호하는 가장 좋은 방법은 중요한 계정의 패스워드를 변경하고, 온라인 계정마다 서로 다르고, 강력한 패스워드를 만드는 것입니다.

피싱/스미싱 공격 주의

불행히도 나쁜 사람들이 이러한 기회를 이용하고 있다. 범죄자들은 하트블리드가 뉴스에서 많이 나오고 있으며 많은 사람들이 읽고 있다는 것을 알고 있다. 그래서 사이버 범죄자들은 온라인 뱅킹 등 우리가 사용하고 있는 합법적인 웹 사이트로나 회사로부터 오는 것처럼 보이는 가짜 이메일 또는 사기성 문자 메시지를 발송한다. 또한 보안회사인 것으로 가장해서 하트블리드를 점검할 수 있는 무료 도구라고 하며 안내한다.

이러한 기술(일반적인 피싱 또는 스미싱이라고 함)은 새로운 것이 아니다. 공격자들은 사람들을 속여서 악성 웹 사이트로 가도록 하는 링크를 클릭하도록 하거나, 악성 앱을 다운로드 하도록 하거나, 감염된 첨부 파일을 열도록 한다. 만약에 이러한 공격에 당하면, 컴퓨터나 스마트폰이 감염될 수 있다. 대신 패스워드를 변경하고자 한다면 브라우저에서 직접 웹 사이트의 주소(URL이라고 함)를 타이핑해서 방문하여 패스워드를 변경하는 것이 좋다. 이렇게 하면 합법적인 웹 사이트로 연결할 수 있다.

Burimet

취약한 웹사이트:	https://lastpass.com/heartbleed/
OUCH! 패스워드:	http://www.securingthehuman.org/ouch/2013#may2013
OUCH! 패스워드 관리프로그램:	http://www.securingthehuman.org/ouch/2013#october2013
OUCH! 2단계 인증:	http://www.securingthehuman.org/ouch/2013#august2013
OUCH! 피싱:	http://www.securingthehuman.org/ouch/2013#february2013
상세 기술:	https://www.sans.org/webcasts/openssl-heartbleed-vulnerability-98105

편집위원회 : Bill Wyman, Walt Scrivens, Phil Hoffman, Lance Spitzner, 번역:진수희(ITL Inc.)