2017.09

소프트웨어 업데이트

과연 신뢰해야 하나?

코드엔진 Talk #1

www.CodeEngn.com

CodeEngn

목 차

소프트웨어 업데이트 과연 신뢰해야 하나?

코드엔진 Talk

코드엔진 Talk는 정보보안에 관련된 특정 주제에 대해 코드엔진 운영진들이 모여 채팅형식으로 대화한 내용들을 문제점, 대응책, 실무사례, 사고사례 등을 이해하기 쉽게 집필한 무료 온라인 잡지입니다.

주제 선정은 페이스북 또는 이메일을 통해 의견을 받거나 최신 이슈를 선정하여 비정기적으로 Talk를 진행 할 예정입니다.

*** 본 지에 언급된 내용은 운영진 개인의 의견으로 소속된 단체나 집단을 대표하지 않고, 집필한 시점에서의 의견으로 사실과 다를 수 있습니다.**
*** 코드엔진 Talk는 배포 시 출처를 반드시 명시하여야 합니다.**

문의사항

http://codeengn.com/contact

업데이트에 대한 문제점은?

볼트101

소프트웨어의 업데이트는 과연 신뢰해야 하나?

최근 넷사랑의 xshell, xftp 등 업데이트 서버에서 변조된 파일이 배포 되었고 해당 프로그램을 사용하는 사람들은 대부분 회사 또는 집에서 서버를 관리하는 사람들일 텐데 공격자는 서버 접속정보와 계정들을 노렸을 것 같다. 변조된 파일이 배포된 이유는 아직 공식입장이 없어서 홈페이지 해킹이나 컴파일 단계에서 추가 되었을 수도 있고 추측만 있을 뿐이다

프로그램의 업데이트 확인은 넷사랑 프로그램 처럼 7일마다 주기적으로 확인 하거나 프로그램을 실행할 때를 기준으로 삼을 때도 있기 때문에 소프트웨어 마다 다르긴 함

Lonnia

소프트웨어 업데이트 신뢰여부는 .. 어떤 소프트웨어인지에 따라 신뢰 여부가 달라지지 않나 생각됩니다

Jenny

소프트웨어사에서 개발을 할 때 외부 인터넷을 차단하여 운영한 뒤 테스트를 확실하게 하고 업데이트 권고를 해야 할 것 같다는 생각을 하게 되네요

결국 소프트웨어 업데이트가 신뢰성을 잃어버린건 사실인거 같아요. 아무리 믿을만한 회사라 해도 그 회사가 완벽하게 보안이 검증되었을까? 라는 생각을 하게 되는것 같습니다

Cirrus

일부 대기업을 제외하면 소프트웨어 업데이트에 대한 검증을 수행하기가 쉽지 않은 것이 현실인 것 같아요.

보안성 검토 프로세스가 잘 정립되어 있는 곳도 테스트 환경과 테스트 그룹에 적용해보고, 이상이 없으면 운영 환경에 반영하게 되는데요.

담당자분들께서 직접 바이너리를 뜯어 보안성검토를 할만한 여건이 되지는 않지요.

볼트101

소프트웨어 업데이트의 분류로 보면 업무용, 사무용(AntiVirus 포함), 운영체제 업데이트로 나눠 볼 수 있는데 지금까지 사례로 봤을 때 운영체제와 백신 업데이트에서는 부팅 불가, 서비스 장애까지 있었는데.. 과연 일반사용자, 직장인들이 운영체제에

설치되는 모든 소프트웨어에 대해 하루하루 업데이트를 위해 시간을 쏟아야 하는 의문이 듬

Cirrus

정리하면 결국 벤더를 신뢰하고 패치 할 수밖에 없는 상황인데, 이에 대해서 별도로 가져가야 할 업데이트 절차가 있을지요?

볼트101

윈도우 업데이트는 이력관리가 잘돼서 업데이트를 개별적으로 선택해서 할 수는 있는데... 과연 소프트웨어 하나하나 신경써서 하는 사람이 과연 몇이나 되고 신경 써서 했는데 오히려 업데이트서버 해킹에 의해 악성코드에 감염이 되는게 현실인것 같다

Cirrus

그마저도 조직에서 관리하는 단말은 PMS나 WSUS, AD 등 솔루션을 이용해 강제 업데이트를 적용해버려서..
기존 설치된 소프트웨어와 충돌이 일어나는 경우도 다반사랍니다.. ㅠㅠ

업데이트 문제점과 현재 대응책은?

볼트101

업데이트의 목적은 소프트웨어의 안전성, 기능 개선에 있지만 다른 시각으로 보면 내가 원하지 않는 기능이 추가되거나 원하는 기능이 삭제되는 경우도 있어서 매번 업데이트를 해야 하는지 고민이 됨

Cirrus

그럴땐 어떻게 해야하나요?

볼트101

사용자 입장에서 이전 설치 파일을 따로 보관해 놓는 방법밖에는 없을거 같고 버전 업데이트 없이 쓰거나 아니면 그냥 무시하고 업데이트 하면서 써야될 수 밖에 없음

업데이트, 패치 등의 목적이 버그나 취약점 등을 확인하고 이로인한 위험을 막기 위한 조치이기 때문에 필수적으로 진행되어야 하는 내용이지만,

Bono	종종 발생하는 업데이트 서버의 관리 문제나, 업데이트 내용에 의해 새로운 위협등의 문제들로 이런 주제로 토의를 하게 되는 것 같네요
 Cirrus	조직의 보안정책을 따르지 않을경우 또는 벤더의 업데이트를 따르지 않아서 발생하는 문제에 대해서는 개인이 책임을 져야 하는 상황이 올까봐 그냥.. 편하게 업데이트를 누르긴 합니다^^
 Jenny	맞아여 ㅋㅋ 업데이트안했을때 어떤 불이익이 생기진 않을까라는 걱정이 생기는거같아요 ㅜㅜ ㅋㅋㅋㅋ
 볼트101	근데 업데이트를 꼬박꼬박 하게되면 그 중 업데이트 서버가 해킹된거면 악성코드에 감염되는일이 발생함...

Jenny

저도 그래서 그냥 업데이트가 있다라는 알림이 뜨면 맘 편히 업데이트를 누르곤하져...그리고 저희 조직 정책상 한글이나 윈도우를 꾸준히 업데이트를 꼬박꼬박 안 하면 안 되는지라..ㅜㅜ

한글에서는 업데이트 서버가 해킹되지 않기를 바라며 항상 꼬박꼬박 업데이트를 누르곤 한답니다 ....ㅋㅋㅋ

볼트101

그래서 대부분의 기업 내부 보안정책을 보면 업데이트(OS, 백신 등)는 바로 적용하지 않고 몇일 뒤에 적용하고 있기는 함

csucom

네.. 큰 기업일 수록 라이브 업데이트가 아닌 자체 PMS를 운영하여, 해당 패치에 대한 검증 후 배포하는 형태를 선호하는 듯 합니다. 그렇지만 말씀하신 대로 비용(인력과 시간 포함)이 이슈일 듯 합니다.

별도 검증 후 패치 배포를 선호하는 이유는 당연한 이야기겠지만 직원 수가 많을수록 문제발생시 파급효과 및 사후조치가 힘이 들 수 있으니까요

Bono

앞에서 말씀하신 것처럼 PMS와 같은 시스템을 사용하는 환경에서는 이를 통해 내부 시스템 및 사용자들이 사용하는 소프트웨어에 대한 자산 인지 수행 후, 신규 업데이트 발생 시 적용 여부를 검토 및 적용하게 되는데,
검토과정에서 해당 업데이트가 발생한 취약점의 원인과 업데이트 간 발생할 수 있는 문제, 업데이트 후 해결되는 문제 등을 검토하는 과정 또한 정확하게 이루어지고 있는지 확인해봐야 할 과제라고 생각이 드네요
검토하는 과정이 이루어지지 않으면 원칙적으로 업데이트 수행이 보류되도록 수행한다고 해도, 그 와중에 발생할 수 있는 보안 위협을 어떻게 대비하고 있어야 하는지의 문제 등을 정확하게 검토할 수 있어야 하는데.. 그렇게 잘 대응하고 있는 사례가 있는지 궁금하기도 하구요 ㅎㅎ

더욱 안전한 업데이트가 되기 위해서 필요하다고 생각되는 것은 문제 발생 시 사후 조치로 수행될 수 있는 소프트웨어 롤백, 서비스 장애시 대처방안, 문제 여부에 따른 피해 확산 방지조치 등의 대처방안이 함께 구성되어 운영되어야 한다고 생각됩니다~!

효과적인 업데이트 정책은?

csucom

말씀하신 사례처럼 예전에 모 유명 포털사이트의 경우에도 DBA 담당자가 알집 업데이트로 인해 PC가 악성코드에 감염되고 이를 통해 DB의 개인정보가 유출된 사례가 있기 때문에 무조건 업데이트를 믿고 가기에는 리스크가 있는 것 같습니다.

기본적으로 업데이트를 했을 때 이로 인한 악성코드 감염 여부를 쉽게 알 수가 없기 때문에 위험한 건데요.

1차적으로 업체 측에서 업데이트 서버에 대한 관리를 물론 잘해야겠지만

만약 그게 잘 안되서 업데이트 서버가 털리면 기본적으로 사용자는 이를 믿고 갈 수 밖에 없기 때문에 하루이틀 업데이트를 늦추더라도 근본적으로 이를 막기란 쉽지 않을 것 같습니다.

그렇다면 만에 하나 걸렸더라도 피해가 적도록 하거나 이를 감지하고 처리하는 형태의 접근이 필요할 듯 합니다.

이를테면 운영서버 관련 정보는 개인PC에 저장하지 말아야 하고 또한 운영서버로의 접근은 개인PC에서 절대 하지 않도록 해야 할 듯 합니다.

그리고 주기적인 의심 프로세스나 네트웍 트래픽 감지 등의 절차도 필요할 듯 하구요.

극단적인 방법으로는 일반 응용프로그램이나 웹서핑 등은 샌드박스나 가상머신을 활용하는 것도 방법일 듯 합니다.

Thomas

소프트웨어 업데이트로 인한 악성코드나 기타 위협을 막기 위한 최선의 방법은 업데이트를 안 하는 것이죠. 하지만 현실적으로 각종 버그나, 제품 취약점으로 인한 위협이 더 크기 때문에 저는 오늘도 업데이트를 합니다ㅎㅎ 이번 넷사랑 사태는 최초 업데이트 이후 약 3주 뒤에 패치 파일이 나왔어요. 대부분의 사용자가 감염 되었겠죠.....

다행히도 추가 페이로드까지 실행되지 않은 상태에서 발견된 것은 아주 운이 좋았다고 할 수 있죠. 만약 시스템 파괴나 랜섬웨어를 다운받는 코드가 있었다면 엄청난 사태가 발생했을지도 모릅니다. 카스퍼스키가 아니었다면.. 백도어가 최종 페이로드를 동작시킬 때까지 아무도 알아차리지 못했을 테니까요.

저는 업데이트 서버 관리도 중요하지만, 카스퍼스키처럼 빠르게 탐지하는 부분이 중요하다고 생각해요. 제2의 넷사랑 사태가 발생하지 않으리라는 보장도 없고, 카스퍼스키만 믿고 있을 순 없으니 우리도 탐지 능력을 키워야겠죠. 보안 전문가들의 몫이 아닌가 싶습니다.

일반 사용자 입장에서는 앱*크 같은 안티랜섬 제품으로 랜섬웨어 감염을 차단하고, V*Lite 같은 백신으로 사후 방역을 맡기는 것이 최선이 아닐까 생각합니다.

컴수진

최근의 이슈를 통해 알려지고 있는 위험성을 감내하고라도 업데이트를 해야하냐? 말아야하냐라고 묻는다면 저는 해야한다라고 생각해요.

왜냐면 업데이트를 통해 해결되는 각종 버그라던지 취약점 패치, 기능 업그레이드의 장점이 그 비율에 있어서 훨씬 많다고 생각되니까요.

다만, 최근 이러한 사태들을 본다면 일괄 업뎃 서버를 이용한 배포가 아닌 좀 더 강화된 업데이트 정책을 기업에서부터 만들 필요가 있을거같아요. 소소한 유틸이나 프로그램까지 적용되기엔 무리가 있을 수 있지만 일정 유저 수 이상 혹은 문제

	발생시 파급력이 큰 솔루션이나 SW 의 경우에는 이야기 나왔던 것처럼 일정 기간을 두고.. 일괄이 아닌 업데이트 확대나 혹은 안정 버전(안정성이 검증된 패치) 사용에 대한 옵션 제공 또는 선택적으로 업데이트를 적용하는 기능이 있으면 좋지 않을까 싶군요. 이렇게 해도 문제가 백프로 해결되진 않을 수 있겠지만... 최대한 줄일 수 있지 않을까 하는 생각입니다.
 Bono	작은 규모의 회사나 보안 팀이 운영되지 않는 환경은 Service Provider에서 제공하는 업데이트를 그대로 수용하여 사용할 수 밖에 없고 이에 따라 발생하는 피해를 고스란히 전달받게 될 수도 있기 때문에 이런 환경에서의 대처 방안은 사용자의 보안 인식 강화 외에... 다른 방안이 있을지 의견이자 질문을 함께 던져봅니다
 민들장군	저는 효과적인 소프트웨어 업데이트 정책(대책)을 3개 주제로 나누어서 생각해봅니다.

정부 : S/W기업에 대한 법과 제도 마련

- 사용자가 많은 S/W를 제작하는 S/W기업에 대한 당근과 채찍 전략이 필요합니다. 즉, 관리 잘 하면 연구개발비 지원 등의 혜택을 주고, 사고 발생시에는 과징금/과태료 부과하는 것이지요.

S/W기업 : 자체 보안관리

- 알아서 잘 관리해야지요. 자기가 만든 자식이니 ㅡ.ㅡ;;;

보안회사 : 많은 기업이 도입한 S/W에 대한 취약점 진단

- S/W기업이나 S/W사용자들이 수행하기 어려운 문제이니 공익적 목적으로 설립된 기관들이 유명한 S/W에 대한 취약점 진단을 실시합니다.

정리하면 정부는 법과 제도를 만들고, S/W기업,
보안전문기관은 S/W의 취약점이 있는지 double check한다는 것입니다.

자동 업데이트 사고 사례는?

Jenny

이렇게 업데이트에 대한 얘기를 하고있는 도중에 한시간 전에 이런기사가 났네요

"파워포인트만 열어도 털린다" MS오피스 취약점 또 발견

http://news1.kr/articles/?3086278

볼트101

그냥 업데이트 했을 뿐인데 랜섬웨어에 감염되면 앞이 안보일거 같은데.. 자동 업데이트는 하지 말라고 해도 문제고 해도 문제고 애매하네.. ;;

Jenny

그러니까요..업데이트를 함부로 하지말아라 라고 얘기하고싶지만 이렇게 업데이트를 하지않을 경우 랜섬웨어에 감염되는 경우가 생기니...ㅜㅜ

볼트101

자동 업데이트 사고사례는 어떤게 있는지 찾아봅시다

볼트101

[긴급] 국내 SW개발사 대상 설치파일변조 침해사고 발생

http://www.dailysecu.com/?mod=news&act=articleView&idxno=23268

[긴급] 국내 SW개발사 대상 설치파일변조 침해사고 발생,

데일리시큐

http://www.dailysecu.com/?mod=news&act=articleView&idxno=23268

PC최적화 SW '씨클리너', 한 달 가까이 악성코드와 함께 배포,

디지털타임스

http://www.dt.co.kr/contents.html?article_no=2017091902109960041001

Bono

2014년 8월 MS업데이트 오류에 의한 롤백 권고

http://www.kbench.com/?q=node/137868

2016년 맥 소프트웨어 업데이트 시스템 취약점 발견

http://macnews.tistory.com/4127

2016년 업데이트 시스템 취약점을 통한 공격 사례

http://www.etnews.com/20160614000155

2017년 4월 광고 프로그램 업데이트 서버 해킹 사건

http://www.boannews.com/media/view.asp?idx=54339

2017.09

소프트웨어 업데이트과연 신뢰해야 하나?

코드엔진 Talk #1

www.CodeEngn.com

문의사항

www.codeengn.com/contact

CodeEngn