WNDRVR

보안 위협으로부터 리눅스 시스템 보호하기

보안 위협으로부터 리눅스 시스템 보호하기

중요한 시스템일수록 윈드리버에서 실행하십시오

개요서

오픈 소스 리눅스는 임베디드 시스템 및 장치를 개발하는 개발자 사이에서 인기가 많다. 그러나 배포되는 상호 연결된 임베디드 시스템 장치들의 수가 계속해서 증가하면서 리눅스 소프트웨어의 취약점이 그 어느 때보다 널리 확산되고 있다. 취약점을 식별하고 필요한 업데이트를 수행하여 위협을 완화하는 일은 장치 개발자 및 제조업체가 전부 감당하기 어려운 경우가 많다. 본 백서는 모니터링, 평가, 통보, 치료 등 리눅스 취약점 해결을 위한 검증된 4단계 프로세스에 대해 설명한다. 또한 기업이 취약점을 내부적으로 모니터링하고 수정하는 데 따르는 비용을 따져보고, 배포된 장치 및 시스템을 지속적으로 보호할 때 숙련된 보안팀과의 협업을 선택하는 것이 왜 보다 현명한 선택일 수 있는지 설명한다.

목 차

보안이 취약한 세상

오픈 소스 리눅스 소프트웨어는 여러 가지 이유로 임베디드 시스템 개발자 사이에서 인기를 얻어왔다. 오픈 소스 리눅스는 독점 벤더의 표준으로부터 개발자들을 자유롭게 해방시켜 더 많은 유연성을 제공한다. 또한 임베디드 시스템 장치에서 자주 요구되는 상호운용성을 지원하는 등 임베디드 시스템 애플리케이션에 대한 실용적인 이점도 제공한다. 임베디드 시스템 솔루션을 실행하는 클라우드 시스템 역시 오픈 소스 리눅스 기반 운영 시스템 상에서 구축되는 경우가 갈수록 늘고 있다.

그러나 오늘날과 같이 상호 연결된 세상에서 리눅스 기반 시스템 및 장치를 보호하는 것은 개발자와 장치 제조업체가 직면한 가장 긴급하고 난처한 과제 중 하나가 됐다. “일단 팔면 끝”식으로 장치를 배포하던 시절은 이미 지나갔다. 근래 만들어지는 사실상 모든 장치는 무언가와의 상호 연결을 염두에 두고 설계되기 때문에 보안 취약점이 발생할 가능성이 높아진다. 연결된 장치는 모든 보고된 공격에 더 취약할 가능성이 높은 것이 현실이다.

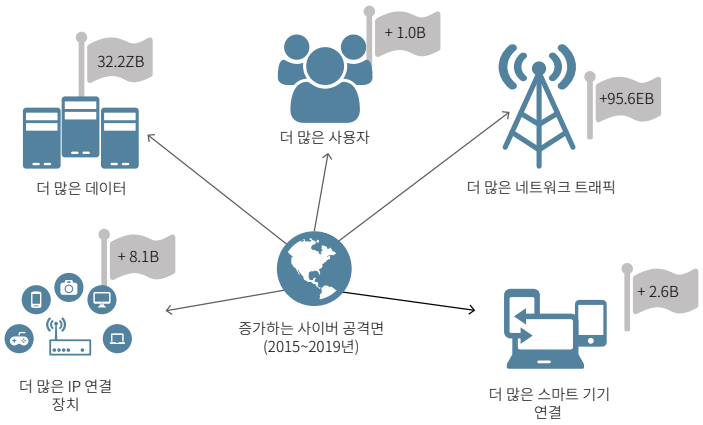


그림 1. 연결된 장치가 많을수록 데이터도 많아지고 그만큼 리스크도 커진다

임베디드 시스템이 급성장하면서 상호 연결된 장치들도 기하급수적으로 증가하고 있다. 이러한 장치, 연결, 데이터 볼륨, 네트워크 트래픽, 사용자의 급증은 그에 비례해서 더 넓어진 공격면에서의 사이버위협의 증가로 이어지고 있다. 이에 장치 제조업체와 임베디드 시스템 애플리케이션 개발자는 설계의 완전 초기 단계부터 강력한 보안 기능을 내장하기 위한 정교한 방식을 채택하고 있다.

이러한 변화는 긍정적인 동시에 필수적이다. 그러나 이것만으로는 충분하지 않다. 위협은 계속해서 진화하고 있다. 임베디드 시스템 운영자는 장치의 유효 수명 내내 보안을 유지하기 위한 방법을 필요로 한다.

제조업체는 시스템 수준 강화에서 더 나아가 새로운 취약점 패치의 민첩한 통합에 초점을 맞춰 자사의 보안 전략을 재고할 필요가 있다. 지속적으로 업데이트되지 않는 시스템은 내장된 보안이 아무리 강력하더라도 새로운 위협이 등장할 때 취약점을 노출할 위험이 생긴다.

우리가 사용하는 노트북을 예로 들어보자. 과거에는 비밀번호만 있으면 노트북을 보호할 수 있었고 외부의 가장 큰 위협이래야 고작 감염된 플로피 디스크가 전부였다. 그러나 인터넷에 연결하는 순간 노트북은 공격자들의 표적이 되며, 이러한 공격은 주로 노트북 내 설치된 애플리케이션을 통해 이루어진다. 물론 새로 발견된 소프트웨어 취약점으로부터 컴퓨터를 보호하기 위해 앱 제공자는 주나 월 단위로 업데이트 알림 또는 자동 업데이트를 제공할 것이다.

리눅스를 실행하는 모든 임베디드 시스템 장치도 이와 동일한 수준의 지속적인 보호가 필요하다. 문제는 어떻게 하면 체계적이고 확장 가능하고 경제적인 방식으로 이를 달성할 수 있는가이다.

틈에 주의하라

시스템 내 취약점을 수정하기에 앞서 취약점이 무엇이고 어디에 있는지를 파악해야 한다. 그러나 임베디드 시스템의 확장과 함께 보안 취약점이 급증하면서 이러한 프로세스도 갈수록 까다로워지고 있다.

CVE(Common Vulnerabilities and Exposures)는 업계에서 일반적으로 받아들여지는, 취약점 식별, 수정 및 보고에 관한 업계 표준이다.

취약점 정보는 CVE 식별자를 통해 적합한 보안 패치 또는 보호 기술과 연관지어질 수 있으며, 이는 오픈 소스 소프트웨어 분야에서는 특히 필수적이다.

취약점 공개는 소프트웨어 벤더, 보안 벤더, 독립적인 연구자, 커뮤니티 메일링 리스트, 미국 컴퓨터 비상 대응팀(US-CERT)과 같은 정부 기관 등 다양한 소스로부터 제공될 수 있다. 그러나 CVE 데이터베이스는 임베디드 시스템 분야에서 기인하는 취약점의 양과 규모를 따라잡아야 하는 어려움에 직면해 있다.

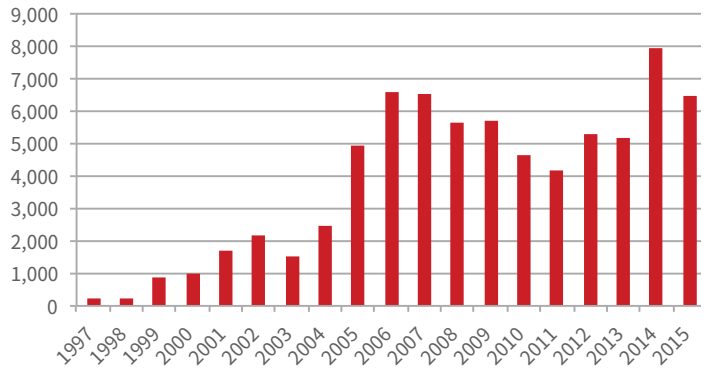
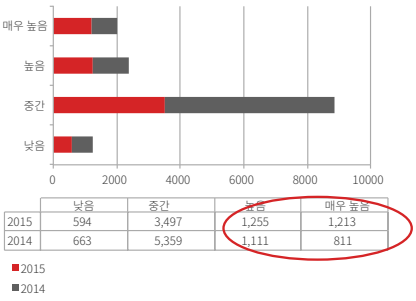


그림 2. 전체 CVE 수의 증가 추이

지난 10년간 CVE 건수는 매해 수천 건이 보고되는 등 앞선 10년 대비 폭발적인 증가세를 보였다. 뿐만 아니라 그 위험도도 증가하고 있다. CVSS(Common Vulnerability Severity Scoring) 시스템에 따르면 위험도가 높거나 매우 높은 CVE 건수는 2014년 대비 2015년에 25% 가까이 증가했다 . 미국 국립표준기술연구소(NIST)에 따르면 전체 외부 공격의 80%는 패치되지 않거나 잘못 구성된 시스템의 알려진 취약점을 이용한다. 한편, 맥아피 랩스(McAfee Labs)는 2016년 발표한 위협 예측 보고서(Threats Predictions)에서 최근 다수의 "제로데이" 공격(취약점을 벤더가 알아차리기 전에 이용하는 공격)이 오픈 소스 소프트웨어의 취약점을 노리고 있다고 보고했다.

2014~2015년 추이



	낮음	중간	높음	매우 높음
2015	594	3,497	1,255	1,213
2014	663	5,359	1,111	811

2015년 위험도 스코어별 취약점

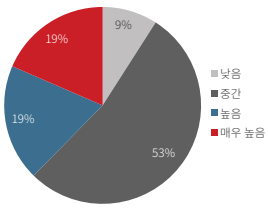


그림 3. 위험도 스코어 추이(2014~2015년)

오픈 소스 소프트웨어 사용은 사실 보안 측면에서 상당한 이점을 제공한다. 위협을 지속적으로 완화하려면 어떠한 취약점이 식별되는 즉시 장치상의 소프트웨어를 업데이트할 수 있어야 한다. 오픈 소스 커뮤니티는 규모가 크기 때문에 취약점 정보도 수많은 연구자, US-CERT와 같은 정부 기관 및 전용 메일링 리스트 등을 통해 빠르게 표면화된다. 그 결과 배포된 장치에서 오픈 소스를 사용하는 사용자들은 신속한 조치를 통해 잠재적 리스크를 낮출 수 있다.

어떠한 시스템이 충분한 시간과 자원을 가진 끈질긴 공격자로부터의 외부 위협에 대해 100% 안전할 수 있다고 생각하는 것은 비현실적이다. 그러나 조치를 취하면 해커가 하는 작업을 극도로 어렵게 만들어 침입 가능성을 크게 줄일 수는 있다.

핵심 4단계

배포된 시스템에서 지속적으로 위협을 완화하기 위해서는 모니터링, 평가, 통보 및 치료의 4단계 접근법이 필요하다.

모니터링

보안 전략에 있어서 모니터링은 "감시 카메라"라고 할 수 있다. 자물쇠로 굳게 잠긴 두 집이 있는데 그 중 하나는 보안 카메라가 있다고 가정해 보자. 당연히 보안 카메라가 있는 집이 침입에 더 잘 대비된 집이다. 사이버 보안에 있어서 이러한 "카메라"는 US-CERT, NIST, CVE 데이터베이스, 다양한 보안 벤더, 비공개 메일링 리스트, 리눅스 취약점을 찾는 커뮤니티와 같이 취약점 경보를 제공하는 조직에 의해 운영된다.

문제는 이러한 수십 군데의 조직들이 발행하는 경보엔 일정 정도의 추측이 개입될 수밖에 없다는 점이다. 따라서 어떤 조직이 정확하고 실행 가능한 정보를 제공하는지 파악하는 것이 대단히 중요하다.

평가

경보나 보안 보고서를 수신한 시스템 운영자 또는 소프트웨어 파트너는 자신의 장치들이 취약한지 여부와 취약하다면 어느 정도 취약한지를 판단해야 한다. 일반적으로 취약점은 높음, 중간, 낮음 또는 없음으로 분류되며 예상되는 위험도, 공격 난이도, 회피 가능성 등을 근거로 우선순위가 정해진다.

평가를 수행하려면 정확히 어떤 패키지와 어떤 버전이 취약한지 알아야 하고 시스템의 정확한 구성도 파악하고 있어야 한다. 취약한 제품에 대해서는, 패치를 찾기 위한 "시계"가 해당 취약점이 노출된 순간부터 작동을 시작한다.

통보

취약점 평가가 완료되면 해당 이슈, 취약점 여부 및 치료 실행 계획을 영향을 받은 사용자에게 통보해야 한다. 이 단계에서는 통보가 영향을 받은 모든 당사자에게 적시에 효율적으로 전달되도록 올바른 툴과 방법론을 적용할 필요가 있다.

치료

치료의 시기와 방법은 대개 우선순위를 기반으로 정해진다. 위험도가 높다고 판단되는 취약점은 즉각적인 "핫 픽스"가 필요할 수 있는 반면 위험도가 낮은 취약점은 정기 소프트웨어 업데이트를 통해 해결할 수도 있다.

관건은 효과적인 패치를 보안 채널을 통해 신속히 최종 사용자에게 배포할 수 있는 능력을 갖추는 것이다.

보호 비용

이 4단계 프로세스는 얼핏 들어도 할 일이 많아 보이고 실제로도 그렇다. 이 프로세스를 수행하려면 상당한 인력, 시간, 노력이 투입되어야 한다는 점은 부인할 수 없는 사실이다. 지름길은 없고 대응 속도가 관건이다. 이상적인 해결책은 모든 잠재적 취약점을 다룰 전담 보안 대응팀이다.

내부에 전담 보안팀을 구성할 경우 비용이 얼마나 들까? 매해 8,000~10,000건의 CVE가 발견되는 것을 고려할 때, 이것들을 일일이 조사하고 해결하기 위해서는 기업마다 고도로 숙련된 엔지니어 4~5명으로 구성된 팀이 필요할 것으로 보인다. 필수 경력과 기술을 갖춘 인력의 평균 연봉을 10만 달러로 잡을 경우 인건비만 한 해 50만 달러가 필요하다.

대부분의 장치 제조업체와 임베디드 시스템 운영자는 이러한 전문화된 분야를 자사의 핵심 역량이나 예산에 포함된 것으로 인식하지 않을 가능성이 높다. 이에 대한 경제적 대안은 이러한 업무를 상용 리눅스 벤더의 전담 보안 대응팀에 외주로 맡기는 것이다. 이는 취약점 발표 후 몇 시간 내에(경우에 따라서는 업스트림 패치보다 수주 또는 수개월 전에) 시기적절한 보호를 제공하기 위한 검증된 전략이다.

올바른 소프트웨어 파트너라면 취약점이 발견될 때 해당 취약점에 대한 최신 정보를 확보하기 위해 자사의 자체 모니터링 및 조사 역량 외에도 리눅스 커뮤니티나 경보 조직 내 필요한 연계를 유지하고 있을 것이다. 뿐만 아니라 제공업체가 다수 고객에 대해 보안 대응 서비스를 확장/축소할 수 있기 때문에 이러한 중요한 업무를 외주로 맡기는 것이 내부에서 관리하려고 애쓰는 것보다 비용이 훨씬 더 적게 든다.

윈드리버 리눅스 보안 대응 프로세스

임베디드 애플리케이션용 상용 리눅스 소프트웨어 분야의 선도 기업인 윈드리버(Wind River®)는 장치 제조업체와 이들의 고객이 시스템의 전체 유효 수명에 걸쳐 지속적인 위협 완화를 유지하는 데 필요한 자원을 제공해 왔다. 윈드리버 리눅스 보안 대응팀은 Wind River Linux, Yocto Linux의 보안 취약점 식별, 모니터링, 해결 및 대응을 담당한다. 이 팀은 앞서 설명한 4단계 프로세스를 수행하고 취약점의 우선순위에 따라 목표 대응 시간을 설정하는 윈드리버 보안 대응 정책을 준수한다.

윈드리버 보안 대응팀은 Wind River Linux, Yocto Linux 에 영향을 미치는 잠재적 이슈와 관련하여 cve.mitre.org에서 CVE 데이터베이스를 지속적으로 모니터링한다. 여기에는 NIST나 US-CERT와 같은 미국 정부 기관 및 조직과 공개 및 비공개 보안 메일링 리스트로부터의 구체적인 보안 통보가 포함된다. 윈드리버는 새로운 보안 위협이 등장할 때마다 이러한 각 조직으로부터 이메일 경보를 수신한다. 경보에는 커뮤니티에서 확인된 취약점과 잠재적 취약점이 모두 포함되며, 팀은 이러한 모든 취약점을 검토한다.

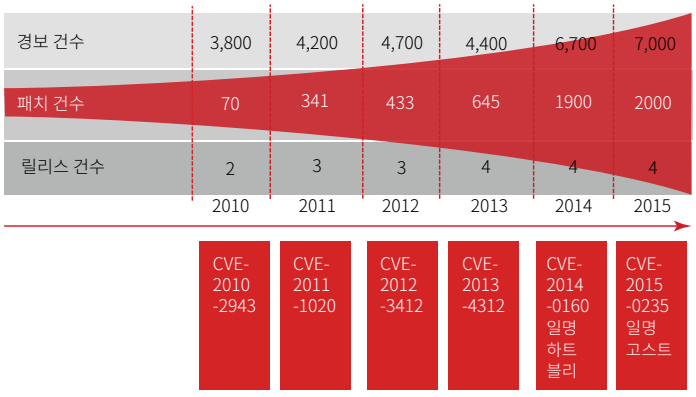


그림 4. 제품 릴리스 및 통합 패치 건수

보안팀은 관련 포럼의 회원 가입 및 참여를 통해 아직 발표되지 않은 리눅스 취약점을 확인할 수 있는데, 이를 통해 윈드리버 및 커뮤니티가 함께 취약점을 해소하고 취약점 발표 시점과 일치하는 상호 합의된 시간에 패치를 발행하도록 할 수 있다. 그 결과 보안 업데이트를 지속적으로 제공할 수 있을 뿐만 아니라 가장 심각한 취약점 중 일부를 당일에 종결할 수도 있다.

보안 대응팀은 Wind River Linux, Yocto Linux 이후 출시될 서비스 팩과 주요 릴리스에 모든 패치를 적용하여 모든 릴리스에 알려진 보안 취약점이 없도록 한다.

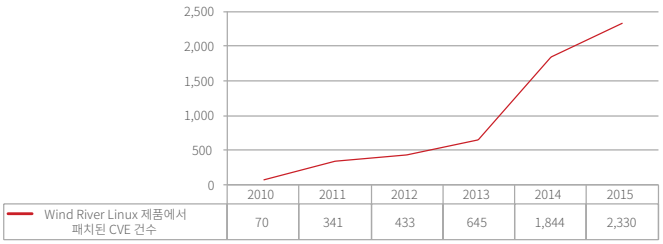


그림 5. 윈드리버 보안 대응 타임라인

결론

오늘날의 상호 연결된 세상에서 보안 취약점은 피할 수 없는 현실이며 임베디드 시스템 애플리케이션의 확산으로 그 수도 빠르게 증가하고 있다. 보안 취약점을 관리하고 위협을 완화하는 것은 최종 사용자 보호를 위해 반드시 필요하지만 대부분의 임베디드 시스템 솔루션 개발자, 장치 제조업체 및 시스템 운영자의 업무 범위를 벗어나는 수준의 노력이 요구된다. 다행스럽게도 오픈 소스 커뮤니티는 리눅스 소프트웨어에 영향을 미치는 취약점을 찾는 데 있어서 조금도 방심하지 않는다. 이러한 커뮤니티에서 적극적으로 활동하는 소프트웨어 파트너와 함께 취약점의 모니터링, 평가, 고객 통보 및 패치를 위한 검증된 프로세스를 통해 제조업체와 개발자는 배포된 임베디드 시스템의 유효 수명 내내 사이버 위협으로부터 자사의 고객을 효과적으로 보호할 수 있다.