공공분야 운용 정보보호제품 · 네트워크 장비

취약점 대응체계

2022. 3. 11

NIS

공공분야 정보보호시스템 · 네트워크 장비 취약점 대응 체계

개요

국가정보원은 「전자정부법」 제56조, 「사이버안보업무규정」 제9조 등 관련 법령에 따라 국가 · 공공기관의 정보보호시스템 및 네트워크 장비 등(이하, 'IT보안제품')에 대한 도입 · 운용 정책을 작성, 배포하고 있습니다.

이의 일환으로 국가정보원은 각급기관이 운용중인 IT보안제품의 취약점을 노린 국가배후 해킹조직 등의 사이버위협에 신속한 대응을 지원하고 피해 제품(장비)에 의한 위협 전파를 예방하기 위해 IT보안제품 취약점 대응체계를 수립하였습니다.

IT보안제품의 안전성 유지를 위한 역할

– 국가정보원의 역할

IT보안제품 취약점 대응체계는 국가정보원 · 운용기관 · 개발업체간 유기적인 협력과 정보공유를 통해 유지됩니다.

〈 IT보안제품 취약점 대응체계 〉

국가정보원은 국가 · 공공기관의 안전한 IT보안제품 운용을 지원하기 위해 도입 및 운용 정책을 작성 · 배포하며, 운용기관의 자율적 취약점 보안조치를 최대한 지원하기 위해 국가배후 해킹조직 등에 의한 취약점 악용 공격 확인시 정보공유시스템(NCTI)을 통해 지속 전파하고 있습니다.

또한, 개발업체의 신속한 보완패치 개발 · 배포를 독려하고 각급기관이 취약점이 제거된 제품을 적시 도입할 수 있도록 사전인증 제도('보안기능 시험제도' · 'CC인증' 제도 등)의 사후관리 절차와 연계, 취약점이 제거된 버전의 검증필 제품목록 우선 등재 등 도입 지원 프로그램도 마련하였습니다.

– 운용기관의 역할

운용기관은 IT보안제품의 보안 · 유지관리의 주체로서, 국가정보원 · 개발업체와 긴밀한 협조아래 자율적으로, 운용중인 IT보안제품을 수시 점검하면서 공개되거나 국가정보원이 지목하여 개선을 요청한 취약점의 제거 등 유지보수 조치를 수행합니다.

– 개발업체의 역할

개발업체는 공공분야에 납품된 IT보안제품의 보안기능을 유지하기 위해 발견되거나 공개된 취약점에 대한 보완패치를 개발 · 배포합니다.

IT보안제품 취약점 대응 체계

– 취약점 대응 단계

IT보안제품 취약점 대응체계는 운용기관의 자율적 취약점 대응 기조아래 사이버안보 책임기관인 국가정보원의 지원을 바탕으로 운영됩니다.

국가정보원 등 유관기관의 효율적인 취약점 대응을 위해 △취약점 심각도 △제품 · 업체의 신뢰성 등 기술적 · 관리적 요소를 기준으로 4단계로 구분된 대응 기준이 적용됩니다.

〈 취약점 대응 단계 〉

지속관심	보완권고	즉시보완	연동배제
1단계(자율 조치)	2단계(자율 조치)	3단계(필수 조치)	4단계(필수 조치)

각급기관은 개발업체 등과 협조, 도입한 IT보안제품에 대해 1 · 2단계 조치를 자율이행하고 국가정보원의 요청이 있을 경우, 3단계 또는 4단계 조치를 수행합니다.

– 1 · 2단계(지속관심 · 보완권고) 단계

❶ 판단 기준

구분	기준
1단계(지속관심)	△기술적 기준 o CVSS(3.1) 0.1~3.9 해당 취약점 △관리적 기준 : 없음
2단계(보완권고)	△기술적 기준 o 제품 운용환경 · 비보안 구성요소의 취약점 o 운용 안정성에 영향을 주는 취약점 o CVSS(3.1) 4.0~6.9 해당 취약점 중에서 제품 설정에 따라 보안기능에 영향을 줄 수 있는 취약점 △관리적 기준 : 없음

❷ 조치 사항

개발업체는 제품의 안전성을 유지하기 위해 △취약점 보완패치 개발 · 배포 △운용기관 대상 취약점 개선버전 설치 등의 활동을 수행합니다. 국가정보원은 1 · 2단계 과정에 배포되는 취약점 제거 버전의 사전인증 반영을 권고합니다.

운용기관은 개발업체와 협조, 운용중인 IT보안제품의 취약점을 상시 보완합니다. 국가정보원은 취약점의 심각도가 낮더라도 해당 취약점의 제거를 권고할 수 있습니다.

– 3단계(즉시보완) 단계

❶ 판단 기준

구분	기준
3단계(즉시보완)	△기술적 기준 o 백도어 또는 보안기능의 무력화 · 우회 취약점 o 사이버안보 위해 해킹조직의 공격에 악용된 취약점 o CVSS(3.1) 7.0~10.0 해당 취약점 중에서 즉시 보완이 필요한 취약점

구분	기준
3단계(즉시보완)	△관리적 기준 o 개발업체의 소스코드 유출 o 개발업체가 ‘보완권고’ 단계의 취약점 개선과정에서 부실 · 허위정보를 제공 o 취약점 개선이 지나치게 지체되어 사이버위협의 가중이 예상되는 경우 o ‘즉시보완’ 조치만이 임박하거나 진행중인 사이버위협을 해소할 수 있는 경우

❷ 조치 사항

국가정보원은 개발업체에 취약점 등에 대한 보완을 요청하는 한편, 운용기관에 대해 취약한 버전의 즉시 제거 및 개발업체가 제공한 개선된 버전의 설치를 요청합니다.

개발업체는 국가정보원의 요청에 따라 취약점 제거 등 제품을 개선한 보완패치를 개발, 운용 기관에 배포하며 보완패치 버전을 사전인증에 반영해야 합니다.

운용기관은 국가정보원이 ‘즉시보완’을 요청한 버전을 신속하게 삭제하고 개발업체로부터 지적된 사항이 보완된 버전을 받아 설치합니다. 이때 해당 제품(장비)의 피해 여부에 따라 설치 전, 초기화[1]가 요청될 수 있습니다.

– 4단계(연동배제) 단계

❶ 판단 기준

구분	기준
4단계(연동배제)	△기술적 기준 : 3단계와 동일 △관리적 기준 o 사이버안보 위해 해킹조직이 제품 개발 · 배포 과정에 연계 o 개발업체 · 제품 신뢰성의 회복 불가능한 상실 o 개발업체가 ‘즉시보완’ 단계 대응과정에서 부실 · 허위정보 제공 또는 백도어 · 취약점 등의 개선 거부 o ‘연동배제’ 조치만이 임박하거나 진행중인 사이버위협을 해소할 수 있는 경우

1) 제품이 설치될 H/W(서버 등)의 저장장치를 포맷한 후, 운영체제 재설치

❷ 조치 사항

국가정보원은 △제품 개발 · 배포과정에 사이버안보 위해 해킹조직 연계 △개발업체의 백도어 제거 · 취약점 개선 거부 △개발업체 · 제품 신뢰성의 회복 불가능한 상실 등 4단계에 해당하는 제품에 대해 연동배제 조치를 숏 국가 · 공공기관에 요청합니다.

운용기관은 국가정보원의 '연동배제' 요청이 있을 경우, 해당 제품을 전산망에서 분리한 후 대체제품 긴급도입 등의 조치를 단계적으로 이행합니다.

긴급 도입하는 대체제품은 해당 제품과 동일한 유형이어야 하지만 긴급성을 고려하여 사전인증요건(보안기능 확인서 · CC인증 등) 생략[1]이 허용됩니다.

이에 따라 운용기관은 대체제품 긴급 도입시 사전인증요건과 무관하게 자체 선정하여 도입할 수 있습니다. 사전인증요건을 생략하고 도입한 경우, 도입 후 국가정보원에 보안적합성 검증을 신청하여 전자정부법 제56조에 규정된 사항을 만족할 수 있습니다.

끝.

1) 예를 들어 긴급 도입하는 방화벽 제품은 보안기능 확인서 또는 CC인증을 받지 않아도 도입이 가능