KISA 한국인터넷진흥원	보도 자료	다시 도약하는 대한민국 함께 잘사는 국민의 나라
2023. 3. 30.(목) [배포시점]부터 보도 가능합니다.		

담당부서	취약점분석팀 이창용 팀장(전화: 02-405-5172, 전자우편: chylee@kisa.or.kr)	
참고자료	사진 있음 □ 사진 없음 ■	총 2매

KISA, 금융보안인증 소프트웨어 긴급 보안패치 권고

한국인터넷진흥원(KISA, 원장 이원태)은 과학기술정보통신부(장관 이종호)와 함께 많은 국민들이 이용하고 있는 금융보안인증 소프트웨어(S/W)에서 해킹사고를 유발하는 보안취약점이 발견되어 해당 S/W를 사용하여 서비스를 제공 중인 기업·기관에게 보안 패치를 신속히 적용할 것을 당부한다고 2023. 3. 30.(목) 밝혔다.

해당 금융보안인증 S/W는 금융기관 및 쇼핑몰 등 다수 홈페이지에서 사용자 인증서 처리를 위해 사용하는 S/W이다. 이는 사용자가 홈페이지에 접속하면 자동 설치되는 형태이므로 전자금융 서비스를 사용하는 상당수의 국민이 이용 중이나, 본인이 이용 중인 사실을 인지하지 못할 수 있다.

문제가 된 보안취약점은 해커가 원격에서 사용자 PC에 악성코드를 전파하고 감염시킬 수 있어 위험도가 높다. KISA는 최근 국정원·경찰청과 협력하여 해킹사고 조사 및 분석 수행 중 해당 취약점을 확인하고, 제조사와 함께 보안패치에 대한 검증을 완료하여 배포 중이다.

서비스 제공 기업·기관이 보안패치를 적용해야 사용자 PC에서도 취약점이 제거되는 방식으로 동작하므로, 해킹 등 피해를 예방하기 위해 기업·기관의 신속한 보안 패치 적용이 반드시 필요하다.

KISA는 신속한 대응을 위해 보호나라 누리집*을 통해 보안패치 적용 권고를 보안 공지하였으며, 유관기관들과도 적극 협력하여 조속히 보안 패치 적용이 완료될 수 있도록 노력할 예정이다.

* 보호나라 누리집 : www.boho.or.kr

또한, KISA는 향후에도 발생할 수 있는 위협에 대한 예방을 위해 금융보안을 포함한 다양한 S/W 제조사 및 서비스 제공 기업들에게 취약점 악용에 따른 해킹 피해 등 위험성을 설명하고, KISA에서 운영 중인 '보안취약점 신고포상제' 참여 등 기업 스스로가 취약점을 발굴하고 조치할 수 있도록 유도하여 보안취약점으로 인한 리스크를 지속적으로 관리하겠다는 방침이다.

KISA 최광희 사이버침해대응본부장은 "금융보안인증 S/W는 국내 대다수 국민이 사용하는 S/W인 만큼 신속한 취약점 조치가 필요하며, 앞으로도 유관기관과의 적극적인 협력을 통해 취약점을 발굴하고 제거함으로써 사이버 공격에 선제적으로 대응할 수 있도록 하겠다"고 강조했다.