드림시큐리티社 보안인증S/W(매직라인) 취약점 조치 권고

2023. 6. 28

❶ 개 요

- 국가사이버위기관리단은 北 해킹조직이 드림시큐리티社 보안인증S/W(MagicLine) 취약점을 해킹에 악용중인 사실을 확인하였습니다.

- 同 취약점에 대한 패치가 이미 개발되어 배포(3.22~)중이지만 이를 적용되지 않은 사용자 PC를 대상으로 해킹이 지속 발생하고 있는 상황입니다.

  * 3月 국가사이버안보센터, KISA(보호나라) 홈페이지에 보안권고문 게재

- 이와 관련, 지난 3월 이니텍社 INISAFE 취약점도 해킹에 악용된 바 있는 등 최근 국민 대다수 PC에 설치된 보안인증S/W의 취약점이 北 해커의 악성코드 유포 경로로 연이어 악용되고 있습니다.

- 피해 예방을 위해 同 S/W의 취약버전(1.0.0.26 이하) 설치 여부 점검 및 삭제를 권고하오니 조속히 이행하여 주시기 바랍니다.

❷ 영향받는 제품 및 버전

제품명	취약점	영향 버전	해결 버전
MagicLine 4.0	버퍼 오버플로우	1.0.0.1 ~ 1.0.0.26	1.0.0.27 이상

❸ 해결 방안

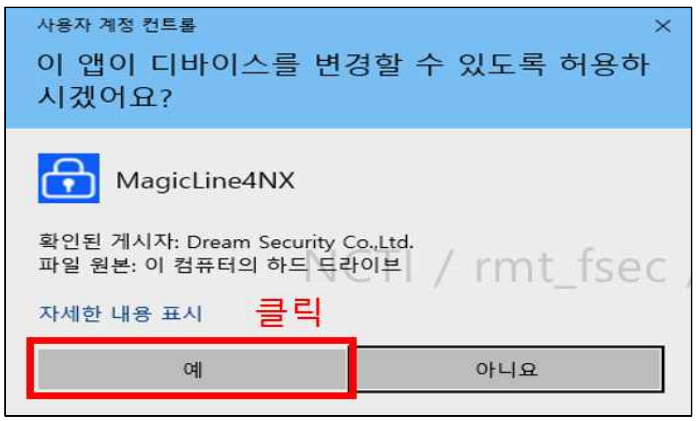
- MagicLine4NX 취약버전이 설치되어 있는 경우 삭제 조치

① 취약버전 삭제 전용도구 이용

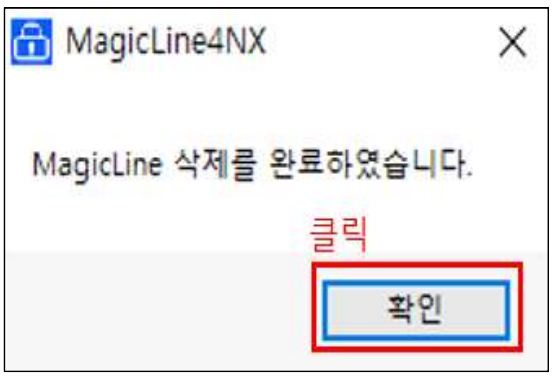
- 드림시큐리티社 홈페이지의 팝업 공지內 삭제도구 다운로드 링크 클릭

  * 또는 https://www.dreamsecurity.com/download/MagicLineNX_Uninstall.exe 접속

- 삭제도구 실행후 권한상승 허용 요청 "예" 클릭

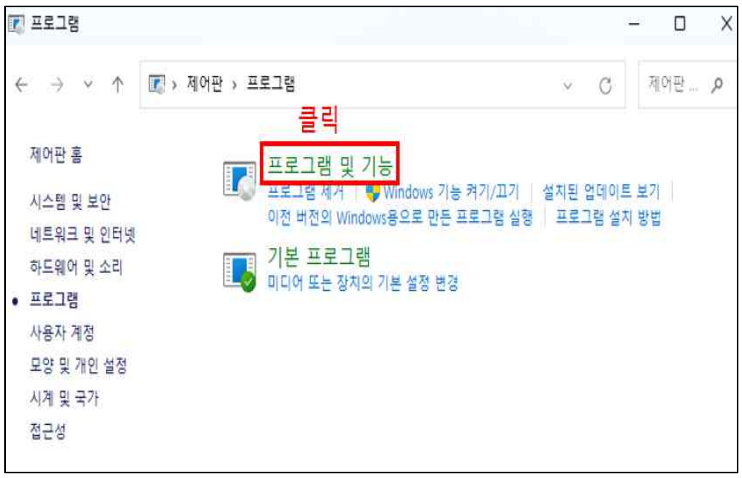


- 확인 클릭



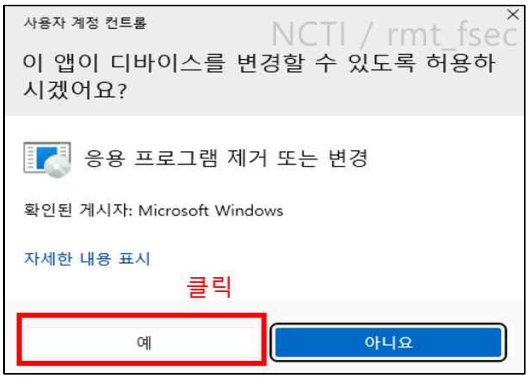
② 윈도우 제어판에서 직접 삭제

- [제어판] — [프로그램] — [프로그램 및 기능]



- MagicLine4NX 버전(1.0.0.26 이하) 확인 및 해당 프로그램 더블클릭

- '응용 프로그램 제거 또는 변경' 창에서 "예" 클릭



※ 삭제도구 이용방법 등 기타 문의 : 드림시큐리티社 (02-2233-5533). 끝.