안랩과 국가사이버안보센터(NCSC), 합동 보고서 배포 및 Microsoft 브라우저 0-DAY 발견 (CVE-2024-38178)

asec.ahnlab.com/ko/83876/

2024년 10월 15일

안랩 ASEC(AhnLab SEcurity intelligence Center) 분석팀과 국가사이버안보센터(NCSC, National Cyber Security Center, 이하 'NCSC') 합동분석협의체에서 Microsoft Internet Explorer(이하 'IE') 브라우저의 새로운 제로데이를 발견하고, 해당 취약점을 이용한 공격을 상세 분석하였다. 본 게시글을 통해 ASEC과 NCSC 합동분석협의체에서 함께 분석하고 대응한 내용을 담은 합동 분석 보고서('**Operation Code on Toast by TA-RedAnt**')를 공개한다.

이번 오퍼레이션의 배후는 북한의 해킹 조직인 **TA-RedAnt**이다. (별칭: RedEyes, ScarCruft, Group123, APT37 등) 이들은 과거 북한 관련 인물들을 대상으로 해킹 메일, 모바일 앱(APK), IE 취약점 등을 이용해 공격한 사례가 있다.

이 오퍼레이션은 IE의 0-day 취약점을 활용해 최근 다양한 무료 소프트웨어에서 함께 설치되는 특정 '토스트(Toast)' 광고 실행 프로그램을 악용한 것이 특징이다.
※토스트(Toast)란? PC화면 하단(주로 우측 하단)에서 솟아오르는 형태로 나타나는 팝업 알림

많은 토스트 광고 프로그램은 광고를 띄울 때 콘텐츠를 다운로드 후 주로 'WebView'라는 기능을 사용해 렌더링을 수행한다. 그러나 이 'WebView'는 브라우저에 기반하여 동작하기 때문에 만약 프로그램 제작자가 IE 기반의 WebView를 사용하여 코드를 작성했다면 IE 취약점이 해당 프로그램에서도 동작할 수 있다. 따라서 공격자는 이미 지원이 종료된 취약한 IE 브라우저의 엔진(jscript9.dll)을 사용하고 있는 토스트 광고 프로그램을 최초 침투 벡터로 악용하였다. Microsoft는 2022년 6월 IE 지원을 종료했으나, 이번 사례와 같이 여전히 IE를 사용하고 있는 일부 윈도우 어플리케이션을 노린 공격이 꾸준히 발견되고 있어 조직 및 사용자의 각별한 주의 및 보안 패치 업데이트가 필요하다.

공격자는 먼저 광고 프로그램이 광고를 다운(제공)받기 위해 연결하는 국내 광고 대행사의 서버를 공격하였으며, 이후 해당 서버의 광고 콘텐츠 관련 스크립트에 취약점 코드를 삽입했다. 이 취약점은 광고 프로그램이 콘텐츠를 다운로드 후 렌더링하는 과정에서 발현된다. 따라서 이번 공격은 사용자의 아무런 상호작용 없이 이뤄질 수 있는 제로클릭(Zero-Click) 공격이다.

해당 취약점은 IE의 자바스크립트 엔진(jscript9.dll)으로 최적화 과정 중 데이터 타입을 잘못 해석해 Type Confusion이 발생함으로써 취약 발현이 가능해진다. 공격자는 이 취약점을 악용해 토스트 광고 프로그램이 설치된 PC에 악성코드 감염을 유도했다. 감염 이후에는 원격 명령 등 다양한 악성행위를 수행할 수 있다.

안랩과 NCSC는 해당 취약점을 즉시 마이크로소프트에 신고했다. 마이크로소프트는 8월 13일(미국 현지 시각 기준) 정기 패치에서 해당 취약점에 대해 공식 CVE 코드(CVE-2024-38178, CVSS 7.5)를 발급하고 관련 패치도 완료했다(https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38178).

자세한 내용은 첨부된 보고서를 참조 바란다.

전체 : (전체본)공개보고서-OperationCodeonToast.pdf
요약 : (요약본)공개보고서-OperationCodeonToast.pdf

NCSC 보안권고문 링크 : https://www.ncsc.go.kr:4018/main/cop/bbs/selectBoardArticle.do?bbsId=SecurityAdvice_main&nttId=164037

AhnLab TIP를 구독하시면 연관 IOC 및 상세 분석 정보를 추가적으로 확인하실 수 있습니다. 자세한 내용은 아래 배너를 클릭하여 확인해보세요.