**MS 인터넷 익스플로러 보안 취약점 업데이트 권고**

**출처 : 인터넷침해대응센터**
**작성일 : 2020.02.12**

□ 개요
o MS社의 인터넷 익스플로러에서 패치가 적용되지 않은 시스템의 경우 랜섬웨어 등 악성코드에 감염될 수 있으므로 패치 권고

□ 설명
o 인터넷 익스플로러에서 스크립팅 엔진이 메모리에 있는 개체를 처리할 때 메모리 충돌로 인해 발생하는 원격 코드 실행 취약점(CVE-2020-0674) [1]

□ 영향 받는 제품

| 소프트웨어 명 | 영향받는 버전 |
|---|---|
| 인터넷 익스플로러 | 9, 10, 11 |

□ 해결 방안
o 최신 업데이트(2020.2.12.일 공개) 진행
- https://portal.msrc.microsoft.com/ko-KR/security-guidance/advisory/CVE-2020-0674 페이지의 "다운로드" 항목에서 사용중인 OS에 맞는 버전 설치 진행

o 윈도우7, 서버2008 등 기술지원이 종료되어 패치 적용이 어려운 경우, 아래의 임시 방안 적용
- 명령 프롬프트 창에서 하단의 명령어 실행(JScript.dll 접근 제한 설정)
(32비트 운영체제)

```
takeown /f %windir%₩system32₩jscript.dll
cacls %windir%₩system32₩jscript.dll /E /P everyone:N
```

(64비트 운영체제)

```
takeown /f %windir%₩syswow64₩jscript.dll
cacls %windir%₩syswow64₩jscript.dll /E /P everyone:N
takeown /f %windir%₩system32₩jscript.dll
cacls %windir%₩system32₩jscript.dll /E /P everyone:N
```

- 설정 복구 방법
(32비트 운영체제)

```
cacls %windir%₩system32₩jscript.dll /E /R everyone
```

(64비트 운영체제)

```
cacls %windir%₩system32₩jscript.dll /E /R everyone
cacls %windir%₩syswow64₩jscript.dll /E /R everyone
```

o 크롬, 엣지, 사파리 등 최신 패치가 제공되는 브라우저 사용 권장

Eyeon Security
Information security company
주소 : 서울특별시 서초구 서초대로 255 고덕빌딩 2층 [06595]
전화 : 02-2105-4400 (영업문의 1, 보안관제문의 2, 기술문의 3)
팩스 : 02-2105-4456
영업문의 : sales@eosec.co.kr, 보안관제 및 기술문의 : tech@eosec.co.kr
COPYRIGHTS © 아이온시큐리티 ALL RIGHTS RESERVED.

**MS** 인터넷 익스플로러 보안 취약점 업데이트 권고

**출처 : 인터넷침해대응센터**
**작성일 : 2020.02.12**

□ 기타 문의사항
o 한국인터넷진흥원 사이버민원센터 : 국번 없이 118

주소 : 서울특별시 서초구 서초대로 255 고덕빌딩 2층 [06595]
전화 : 02-2105-4400 (영업문의 1, 보안관제문의 2, 기술문의 3)
팩스 : 02-2105-4456
영업문의 : sales@eosec.co.kr, 보안관제 및 기술문의 : tech@eosec.co.kr
COPYRIGHTS © 아이온시큐리티 ALL RIGHTS RESERVED.