Adobe 제품군 보안 업데이트 권고

출처 : 인터넷침해대응센터
작성일 : 2019.04.11

□ 개요

o Adobe社는 자사 제품군의 취약점을 해결한 보안 업데이트 발표 [1]
o 낮은 버전을 사용중인 시스템은 악성코드 감염에 취약하므로 해결방안에 따라 최신버전으로 업데이트 권고

□ 설명

o Adobe Bridge CC에서 힙 오버플로우와 메모리의 경계값을 벗어난 쓰기로 발생하는 원격코드 실행 취약점(CVE-2019-7130, 7132) [2]
o Adobe InDesign에서 하이퍼링크 처리과정이 미흡하여 발생하는 원격코드 실행 취약점(CVE-2019-7107) [3]
o Adobe XD CC에서 경로 탐색으로 인해 발생하는 원격코드 실행 취약점(CVE-2019-7105, 7106) [4]
o Adobe Shockwave player에서 메모리 충돌로 인해 발생하는 임의코드 실행 취약점(CVE-2019-7098 외 6건) [5]
o Adobe Flash player에서 use-after-free로 인해 발생하는 임의코드 실행 취약점(CVE-2019-7096) [6]

□ 영향을 받는 제품

소프트웨어 명		동작 환경	영향 받는 버전
Adobe Bridge CC		윈도우즈, 맥OS	9.0.2 버전
Adobe InDesign		맥OS	14.0.1 및 이전버전
Adobe XD CC			16.0 및 이전 버전
Adobe Shockwave player		윈도우즈	12.3.4.204 및 이전 버전
Adobe Flash Player	Desktop Runtime	윈도우즈, 맥OS, 리눅스	32.0.0.156 및 이전 버전
	Google Chrome	윈도우즈, 맥OS, 리눅스, Chrome OS	
	Microsoft Edge/IE11	윈도우즈 8.1/10	

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

Adobe 제품군 보안 업데이트 권고

출처 : 인터넷침해대응센터
작성일 : 2019.04.11

□ 해결 방안

- 최신 버전으로 업데이트 진행

소프트웨어 명		동작 환경	최신 버전
Adobe Bridge CC		윈도우즈, 맥OS	9.0.3 버전
Adobe InDesign		맥OS	14.0.2 버전
Adobe XD CC			17.0.12 버전
Adobe Shockwave player		윈도우즈	12.3.5.205 버전
Adobe Flash Player	Desktop Runtime	윈도우즈, 맥OS	32.0.0.171 버전
	Google Chrome	윈도우즈, 맥OS, 리눅스, Chrome OS	
	Microsoft Edge/IE11	윈도우즈 8.1/10	
	Desktop Runtime	리눅스	

□ 기타 문의사항

o 한국인터넷진흥원 인터넷침해대응센터: 국번없이 118

[참고사이트]

[1] https://helpx.adobe.com/security.html
[2] https://helpx.adobe.com/security/products/bridge/apsb19-25.html
[3] https://helpx.adobe.com/security/products/indesign/apsb19-23.html
[4] https://helpx.adobe.com/security/products/xd/apsb19-22.html
[5] https://helpx.adobe.com/security/products/shockwave/apsb19-20.html
[6] https://helpx.adobe.com/security/products/flash-player/apsb19-19.htm

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