MS 9월 보안 위협에 따른 정기 보안 업데이트 권고

출처 : 인터넷침해대응센터
작성일 : 2019.09.11

□ 9월 보안 업데이트 개요(총 15종)
o 등급 : 긴급(Critical) 10 종, 중요(Important) 5 종
o 발표일 : 2019.9.11.(수)
o 업데이트 내용

제품군	중요도	영향	KB번호
Windows 10, Server 2019, Server 2016, Edge	긴급	원격코드실행	4516044 등 8개
Windows 8.1, Server 2012 R2	긴급	원격코드실행	4516067 등 2개
Windows Server 2012	긴급	원격코드실행	4516055 등 2개
Windows RT 8.1	긴급	원격코드실행	4516067
Windows 7, Server 2008 R2	긴급	원격코드실행	4516065 등 2개
Windows Server 2008	긴급	원격코드실행	4516026 등 2개
Internet Explorer	긴급	원격코드실행	4516065 등 15개
ChakraCore	긴급	원격코드실행	-
Office	중요	원격코드실행	4475574 등 6개
Visual Studio	중요	권한상승	4513696
SharePoint Server, SharePoint Enterprise Server	긴급	원격코드실행	4484098 등 10개
Lync	중요	정보노출	4515509
Exchange Server	중요	서비스거부	4515832
.NET Core	중요	권한상승	4514604 등 15개
Adobe Flash Player	긴급	원격코드실행	4516115

o 참고사이트
- 한글 : https://portal.msrc.microsoft.com/ko-kr/security-guidance
- 영문 : https://portal.msrc.microsoft.com/en-us/security-guidance

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

1. Windows 10, Server 2019, Server 2016, Edge 보안 업데이트

□ 설명

o 공격자가 특수하게 제작된 악성 응용 프로그램을 실행할 경우, 원격코드실행을 허용하는 취약점

o 관련취약점 :
- 원격코드실행 취약점(CVE-2019-0787,CVE-2019-0788,CVE-2019-1138,CVE-2019-1217,CVE-2019-1237,CVE-2019-1240,CVE-2019-1241,CVE-2019-1242,CVE-2019-1243,CVE-2019-1247,CVE-2019-1248,CVE-2019-1249,CVE-2019-1250,CVE-2019-1280,CVE-2019-1290,CVE-2019-1291,CVE-2019-1298,CVE-2019-1300)
- 권한상승 취약점(CVE-2019-1214,CVE-2019-1215,CVE-2019-1232,CVE-2019-1235,CVE-2019-1253,CVE-2019-1256,CVE-2019-1267,CVE-2019-1268,CVE-2019-1269,CVE-2019-1270,CVE-2019-1271,CVE-2019-1272,CVE-2019-1277,CVE-2019-1278,CVE-2019-1285,CVE-2019-1287,CVE-2019-1289)
- 서비스거부 취약점(CVE-2019-0928,CVE-2019-1292)
- 보안기능 우회 취약점(CVE-2019-1220,CVE-2019-1264)
- 정보노출 취약점(CVE-2019-1216,CVE-2019-1219,CVE-2019-1244,CVE-2019-1245,CVE-2019-1251,CVE-2019-1252,CVE-2019-1274,CVE-2019-1282,CVE-2019-1286,CVE-2019-1299)
- DID 취약점(CVE-2019-1273)

o 영향 : 원격코드실행

o 중요도 : 긴급

o 관련 KB번호
- 4516044, 4516070, 4516068, 4516066, 4516058, 4512578, 4515384, 4475589

□ 해결책
o 영향 받는 소프트웨어를 이용하는 경우 마이크로소프트사의 보안 패치 적용

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

2. Windows 8.1, Server 2012 R2 보안 업데이트

□ 설명

o 공격자가 특수하게 제작된 악성 응용 프로그램을 실행할 경우, 원격코드실행을 허용하는 취약점

o 관련취약점 :
- 원격코드실행 취약점(CVE-2019-0787,CVE-2019-0788,CVE-2019-1240,CVE-2019-1242,CVE-2019-1243,CVE-2019-1246,CVE-2019-1247,CVE-2019-1248,CVE-2019-1249,CVE-2019-1250,CVE-2019-1280,CVE-2019-1290,CVE-2019-1291)
- 권한상승 취약점(CVE-2019-1214,CVE-2019-1215,CVE-2019-1235,CVE-2019-1267,CVE-2019-1268,CVE-2019-1269,CVE-2019-1271,CVE-2019-1285,CVE-2019-1287)
- 정보노출 취약점(CVE-2019-1216,CVE-2019-1219,CVE-2019-1244,CVE-2019-1245,CVE-2019-1252,CVE-2019-1274,CVE-2019-1282,CVE-2019-1286,CVE-2019-1293)

o 영향 : 원격코드실행

o 중요도 : 긴급

o 관련 KB번호
- 4516067, 4516064

□ 해결책
o 영향 받는 소프트웨어를 이용하는 경우 마이크로소프트사의 보안 패치 적용

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

3. Windows Server 2012 보안 업데이트

□ 설명

o 공격자가 특수하게 제작된 악성 응용 프로그램을 실행할 경우, 원격코드실행을 허용하는 취약점

o 관련취약점 :
- 원격코드실행 취약점(CVE-2019-1240,CVE-2019-1242,CVE-2019-1243,CVE-2019-1248,CVE-2019-1249,CVE-2019-1250,CVE-2019-1280)
- 권한상승 취약점(CVE-2019-1214,CVE-2019-1215,CVE-2019-1235,CVE-2019-1268,CVE-2019-1271,CVE-2019-1285,CVE-2019-1287)
- 정보노출 취약점(CVE-2019-1216,CVE-2019-1219,CVE-2019-1244,CVE-2019-1245,CVE-2019-1252,CVE-2019-1274,CVE-2019-1282,CVE-2019-1286)

o 영향 : 원격코드실행

o 중요도 : 긴급

o 관련 KB번호
- 4516055, 4516062

□ 해결책
o 영향 받는 소프트웨어를 이용하는 경우 마이크로소프트사의 보안 패치 적용

4. Windows RT 8.1 보안 업데이트

□ 설명

o 공격자가 특수하게 제작된 악성 응용 프로그램을 실행할 경우, 원격코드실행을 허용하는 취약점

o 관련취약점 :
- 원격코드실행 취약점(CVE-2019-0787,CVE-2019-0788,CVE-2019-1242,CVE-2019-1243,CVE-2019-1247,CVE-2019-1248,CVE-2019-1249,CVE-2019-1250,CVE-2019-1280,CVE-2019-1290,CVE-2019-1291)
- 권한상승 취약점(CVE-2019-1214,CVE-2019-1215,CVE-2019-1235,CVE-2019-1268,CVE-2019-1269,CVE-2019-1271,CVE-2019-1285,CVE-2019-1287)
- 정보노출 취약점(CVE-2019-1216,CVE-2019-1219,CVE-2019-1244,CVE-2019-1245,CVE-2019-1252,CVE-2019-1274,CVE-2019-1282,CVE-2019-1286)

o 영향 : 원격코드실행

o 중요도 : 긴급

o 관련 KB번호
- 4516067

□ 해결책
o 영향 받는 소프트웨어를 이용하는 경우 마이크로소프트사의 보안 패치 적용

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

5. Windows 7, Server 2008 R2 보안 업데이트

□ 설명

o 공격자가 특수하게 제작된 악성 응용 프로그램을 실행할 경우, 원격코드실행을 허용하는 취약점

o 관련취약점 :
- 원격코드실행 취약점(CVE-2019-0787,CVE-2019-1240,CVE-2019-1242,CVE-2019-1243,CVE-2019-1246,CVE-2019-1247,CVE-2019-1248,CVE-2019-1249,CVE-2019-1250,CVE-2019-1280,CVE-2019-1290,CVE-2019-1291)
- 권한상승 취약점(CVE-2019-1214,CVE-2019-1215,CVE-2019-1235,CVE-2019-1267,CVE-2019-1268,CVE-2019-1271,CVE-2019-1284,CVE-2019-1285)
- 정보노출 취약점(CVE-2019-1216,CVE-2019-1219,CVE-2019-1244,CVE-2019-1245,CVE-2019-1252,CVE-2019-1274,CVE-2019-1282,CVE-2019-1283,CVE-2019-1286,CVE-2019-1293)

o 영향 : 원격코드실행

o 중요도 : 긴급

o 관련 KB번호
- 4516065, 4516033

□ 해결책
o 영향 받는 소프트웨어를 이용하는 경우 마이크로소프트사의 보안 패치 적용

6. Windows Server 2008 보안 업데이트

□ 설명

o 공격자가 특수하게 제작된 악성 응용 프로그램을 실행할 경우, 원격코드실행을 허용하는 취약점

o 관련취약점 :
- 원격코드실행 취약점(CVE-2019-1240,CVE-2019-1242,CVE-2019-1243,CVE-2019-1246,CVE-2019-1248,CVE-2019-1249,CVE-2019-1250,CVE-2019-1280,CVE-2019-1291)
- 권한상승 취약점(CVE-2019-1214,CVE-2019-1215,CVE-2019-1235,CVE-2019-1268,CVE-2019-1271,CVE-2019-1284,CVE-2019-1285)
- 정보노출 취약점(CVE-2019-1219,CVE-2019-1244,CVE-2019-1245,CVE-2019-1252,CVE-2019-1274,CVE-2019-1282,CVE-2019-1286)

o 영향 : 원격코드실행

o 중요도 : 긴급

o 관련 KB번호
- 4516026, 4516051

□ 해결책
o 영향 받는 소프트웨어를 이용하는 경우 마이크로소프트사의 보안 패치 적용

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

7. Internet Explorer 보안 업데이트

□ 설명

o 이용자가 특수하게 제작된 악성 웹 페이지를 열람할 경우, 원격코드실행을 허용하는 취약점

o 관련취약점 :
- 원격코드실행 취약점(CVE-2019-1208,CVE-2019-1221,CVE-2019-1236)
- 보안기능 우회 취약점(CVE-2019-1220)

o 영향 : 원격코드실행

o 중요도 : 긴급

o 관련 KB번호
- 4516065, 4516046, 4516067, 4516046, 4516044, 4516070, 4516068, 4516066, 4516058, 4512578, 4515384, 4516055, 4516046, 4516026, 4516046

□ 해결책
o 영향 받는 소프트웨어를 이용하는 경우 마이크로소프트사의 보안 패치 적용

8. ChakraCore 보안 업데이트

□ 설명

o 이용자가 특수하게 제작된 악성 웹 페이지를 열람할 경우, 원격코드실행을 허용하는 취약점
※ ChakraCore : Edge의 자바스크립트 엔진, Cloud, 게임엔진, IoT 등에서도 사용

o 관련취약점 :
- 원격코드실행 취약점(CVE-2019-1138,CVE-2019-1217,CVE-2019-1237,CVE-2019-1298)

o 영향 : 원격코드실행

o 중요도 : 긴급

□ 해결책
o 영향 받는 소프트웨어를 이용하는 경우 마이크로소프트사의 보안 패치 적용

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

9. Office 보안 업데이트

□ 설명

o 이용자가 특수하게 제작된 악성 문서를 열람할 경우, 원격코드실행을 허용하는 취약점

o 관련취약점 :
- 원격코드실행 취약점(CVE-2019-1297)
- 보안기능 우회 취약점(CVE-2019-1264)
- 정보노출 취약점(CVE-2019-1263)

o 영향 : 원격코드실행

o 중요도 : 중요

o 관련 KB번호
- 4475574, 4475579, 4475566, 4475607, 4475583, 4464566

□ 해결책
o 영향 받는 소프트웨어를 이용하는 경우 마이크로소프트사의 보안 패치 적용

10. Visual Studio 보안 업데이트

□ 설명

o 공격자가 프로그램 버그(실행 처리 구문의 허점 등)을 악용하여 보호되는 자원들에 임의로 접근하는 권한상승 취약점

o 관련취약점 :
- 권한상승 취약점(CVE-2019-1232)

o 영향 : 권한상승

o 중요도 : 중요

o 관련 KB번호
- 4513696

□ 해결책
o 영향 받는 소프트웨어를 이용하는 경우 마이크로소프트사의 보안 패치 적용

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

11. SharePoint Server, SharePoint Enterprise Server 보안 업데이트

□ 설명

o 이용자가 특수하게 제작된 악성 문서를 열람할 경우, 원격코드실행을 허용하는 취약점

o 관련취약점 :
- 원격코드실행 취약점(CVE-2019-1257,CVE-2019-1296)
- 권한상승 취약점(CVE-2019-1260)
- DID 취약점(CVE-2019-1259,CVE-2019-1261,CVE-2019-1262)

o 영향 : 원격코드실행

o 중요도 : 긴급

o 관련 KB번호
- 4484098, 4475590, 4475605, 4475596, 4484098, 4484099, 4475590, 4475594, 4475596, 4464557

□ 해결책
o 영향 받는 소프트웨어를 이용하는 경우 마이크로소프트사의 보안 패치 적용

12. Lync 보안 업데이트

□ 설명

o 공격자가 프로그램의 미흡한 설계(적절한 검증 부재)를 악용하여 제한된 자원에 접근가능한 정보노출 취약점

o 관련취약점 :
- 정보노출 취약점(CVE-2019-1209)

o 영향 : 정보노출

o 중요도 : 중요

o 관련 KB번호
- 4515509

□ 해결책
o 영향 받는 소프트웨어를 이용하는 경우 마이크로소프트사의 보안 패치 적용

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

13. Exchange Server 보안 업데이트

□ 설명
o 공격자가 시스템의 자원을 고갈시켜 발생하는 서비스거부 취약점

o 관련취약점 :
- 서비스거부 취약점(CVE-2019-1233)
- DID 취약점(CVE-2019-1266)

o 영향 : 서비스거부

o 중요도 : 중요

o 관련 KB번호
- 4515832

□ 해결책
o 영향 받는 소프트웨어를 이용하는 경우 마이크로소프트사의 보안 패치 적용

14. .NET Core 보안 업데이트

□ 설명

o 공격자가 프로그램 버그(실행 처리 구문의 허점 등)을 악용하여 보호되는 자원들에 임의로 접근하는 권한상승 취약점

o 관련취약점 :
- 권한상승 취약점(CVE-2019-1142)

o 영향 : 권한상승

o 중요도 : 중요

o 관련 KB번호
- 4514604, 4514599, 4514603, 4514598, 4516044, 4516070, 4516068, 4516066, 4516058, 4514354, 4514355, 4514356, 4514357, 4514601, 4514359

□ 해결책
o 영향 받는 소프트웨어를 이용하는 경우 마이크로소프트사의 보안 패치 적용

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

15. Adobe Flash Player 보안 업데이트

□ 설명
o 지원되는 모든 버전의 Windows 8.1, Windows Server 2012, Windows Server 2012 R2, Windows RT 8.1, Windows 10 및 Windows Server 2016에 설치된 Adobe Flash Player의 취약점을 해결

o 관련취약점 :
- Adobe 보안 업데이트 APSB19-46 설명된 취약점

o 영향 : 원격코드실행

o 중요도 : 긴급

o 관련 KB번호
- 4516115

□ 해결책
o 영향 받는 소프트웨어를 이용하는 경우 마이크로소프트사의 보안 패치 적용

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