MS 2월 보안 위협에 따른 정기 보안 업데이트 권고

출처 : 인터넷침해대응센터
작성일 : 2019.02.13

□ 2월 보안 업데이트 개요(총 16종)
o 등급 : 긴급(Critical) 10 종, 중요(Important) 6 종
o 발표일 : 2019.2.13.(수)
o 업데이트 내용

제품군	중요도	영향	KB번호
Windows 10, Server 2019, Server 2016, Edge	긴급	원격코드실행	4487026 등 6개
Windows 8.1, Server 2012 R2	긴급	원격코드실행	4487000 등 2개
Windows Server 2012	긴급	원격코드실행	4487025 등 2개
Windows RT 8.1	긴급	원격코드실행	4487000
Windows 7, Server 2008 R2	긴급	원격코드실행	4486563 등 2개
Windows Server 2008	긴급	원격코드실행	4487023 등 2개
Internet Explorer	긴급	원격코드실행	4486563 등 14개
ChakraCore	긴급	원격코드실행	-
Office	중요	원격코드실행	4092465 등 14개
Visual Studio	중요	원격코드실행	-
SharePoint Server, SharePoint Enterprise Server	긴급	원격코드실행	4461630 등 5개
Skype	중요	스푸핑	3061064
Exchange Server	중요	권한상승	4345836 등 4개
.NET Core	중요	원격코드실행	4483458 등 28개
Team Foundation Server	중요	정보노출	-
Adobe Flash Player	긴급	원격코드실행	4487038

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

MS 2월 보안 위협에 따른 정기 보안 업데이트 권고

출처 : 인터넷침해대응센터
작성일 : 2019.02.13

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-2019-0590,CVE-2019-0591,CVE-2019-0593,CVE-2019-0595,CVE-2019-0596,CVE-2019-0597,CVE-2019-0598,CVE-2019-0599,CVE-2019-0605,CVE-2019-0607,CVE-2019-0610,CVE-2019-0618,CVE-2019-0625,CVE-2019-0626,CVE-2019-0630,CVE-2019-0633,CVE-2019-0634,CVE-2019-0640,CVE-2019-0642,CVE-2019-0644,CVE-2019-0645,CVE-2019-0650,CVE-2019-0651,CVE-2019-0652,CVE-2019-0655,CVE-2019-0662)
- 권한상승 취약점(CVE-2019-0623,CVE-2019-0649,CVE-2019-0656,CVE-2019-0659)
- 보안기능 우회 취약점(CVE-2019-0627,CVE-2019-0631,CVE-2019-0632,CVE-2019-0637,CVE-2019-0641)
- 정보노출 취약점(CVE-2019-0601,CVE-2019-0602,CVE-2019-0615,CVE-2019-0616,CVE-2019-0619,CVE-2019-0628,CVE-2019-0635,CVE-2019-0636,CVE-2019-0643,CVE-2019-0648,CVE-2019-0658,CVE-2019-0660)
- 스푸핑 취약점(CVE-2019-0654)

o 영향 : 원격코드실행

o 중요도 : 긴급

o 관련 KB번호
- 4487026, 4487018, 4487020, 4486996, 4487017, 4487044

□ 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

MS 2월 보안 위협에 따른 정기 보안 업데이트 권고

출처 : 인터넷침해대응센터
작성일 : 2019.02.13

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-2019-0595,CVE-2019-0596,CVE-2019-0597,CVE-2019-0598,CVE-2019-0599,CVE-2019-0618,CVE-2019-0625,CVE-2019-0626,CVE-2019-0630,CVE-2019-0633,CVE-2019-0662)
- 권한상승 취약점(CVE-2019-0656)
- 정보노출 취약점(CVE-2019-0602,CVE-2019-0615,CVE-2019-0619,CVE-2019-0628,CVE-2019-0635,CVE-2019-0636,CVE-2019-0660,CVE-2019-0664)

o 영향 : 원격코드실행

o 중요도 : 긴급

o 관련 KB번호
- 4487000, 4487028

□ 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

MS 2월 보안 위협에 따른 정기 보안 업데이트 권고

출처 : 인터넷침해대응센터
작성일 : 2019.02.13

3. Windows Server 2012 보안 업데이트

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

o 관련취약점 :
- 원격코드실행 취약점(CVE-2019-0595,CVE-2019-0596,CVE-2019-0597,CVE-2019-0598,CVE-2019-0599,CVE-2019-0618,CVE-2019-0625,CVE-2019-0626,CVE-2019-0630,CVE-2019-0633,CVE-2019-0662)
- 정보노출 취약점(CVE-2019-0602,CVE-2019-0615,CVE-2019-0619,CVE-2019-0628,CVE-2019-0635,CVE-2019-0660,CVE-2019-0661,CVE-2019-0664)

o 영향 : 원격코드실행

o 중요도 : 긴급

o 관련 KB번호
- 4487025, 4486993

□ 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

MS 2월 보안 위협에 따른 정기 보안 업데이트 권고

출처 : 인터넷침해대응센터
작성일 : 2019.02.13

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-2019-0595,CVE-2019-0596,CVE-2019-0597,CVE-2019-0598,CVE-2019-0618,CVE-2019-0625,CVE-2019-0626,CVE-2019-0630,CVE-2019-0633,CVE-2019-0662)
- 권한상승 취약점(CVE-2019-0656)
- 정보노출 취약점(CVE-2019-0602,CVE-2019-0615,CVE-2019-0619,CVE-2019-0628,CVE-2019-0636,CVE-2019-0660,CVE-2019-0664)

o 영향 : 원격코드실행

o 중요도 : 긴급

o 관련 KB번호
- 4487000

□ 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

MS 2월 보안 위협에 따른 정기 보안 업데이트 권고

출처 : 인터넷침해대응센터
작성일 : 2019.02.13

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-2019-0595,CVE-2019-0596,CVE-2019-0597,CVE-2019-0598,CVE-2019-0599,CVE-2019-0618,CVE-2019-0625,CVE-2019-0626,CVE-2019-0630,CVE-2019-0662)
- 정보노출 취약점(CVE-2019-0602,CVE-2019-0615,CVE-2019-0619,CVE-2019-0628,CVE-2019-0635,CVE-2019-0636,CVE-2019-0660,CVE-2019-0661,CVE-2019-0664)

o 영향 : 원격코드실행

o 중요도 : 긴급

o 관련 KB번호
- 4486563, 4486564

□ 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

MS 2월 보안 위협에 따른 정기 보안 업데이트 권고

출처 : 인터넷침해대응센터
작성일 : 2019.02.13

6. Windows Server 2008 보안 업데이트

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

o 관련취약점 :
- 원격코드실행 취약점(CVE-2019-0595,CVE-2019-0596,CVE-2019-0597,CVE-2019-0598,CVE-2019-0599,CVE-2019-0618,CVE-2019-0625,CVE-2019-0626,CVE-2019-0630,CVE-2019-0662)
- 정보노출 취약점(CVE-2019-0602,CVE-2019-0615,CVE-2019-0619,CVE-2019-0628,CVE-2019-0635,CVE-2019-0636,CVE-2019-0660,CVE-2019-0661,CVE-2019-0664)

o 영향 : 원격코드실행

o 중요도 : 긴급

o 관련 KB번호
- 4487023, 4487019

□ 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

MS 2월 보안 위협에 따른 정기 보안 업데이트 권고

출처 : 인터넷침해대응센터
작성일 : 2019.02.13

7. Internet Explorer 보안 업데이트

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

o 관련취약점 :
- 원격코드실행 취약점(CVE-2019-0606)
- 정보노출 취약점(CVE-2019-0676)
- 스푸핑 취약점(CVE-2019-0654)

o 영향 : 원격코드실행

o 중요도 : 긴급

o 관련 KB번호
- 4486563, 4486474, 4487000, 4486474, 4487026, 4487018, 4487020, 4486996, 4487017, 4487044, 4487025, 4486474, 4487023, 4486474

□ 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

MS 2월 보안 위협에 따른 정기 보안 업데이트 권고

출처 : 인터넷침해대응센터
작성일 : 2019.02.13

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-2019-0590,CVE-2019-0591,CVE-2019-0593,CVE-2019-0605,CVE-2019-0607,CVE-2019-0610,CVE-2019-0640,CVE-2019-0642,CVE-2019-0644,CVE-2019-0651,CVE-2019-0652,CVE-2019-0655)
- 권한상승 취약점(CVE-2019-0649)
- 정보노출 취약점(CVE-2019-0658)

o 영향 : 원격코드실행

o 중요도 : 긴급

□ 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

MS 2월 보안 위협에 따른 정기 보안 업데이트 권고

출처 : 인터넷침해대응센터
작성일 : 2019.02.13

9. Office 보안 업데이트

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

o 관련취약점 :
- 원격코드실행 취약점(CVE-2019-0671,CVE-2019-0672,CVE-2019-0673,CVE-2019-0674,CVE-2019-0675)
- 보안기능 우회 취약점(CVE-2019-0540,CVE-2019-0669)

o 영향 : 원격코드실행

o 중요도 : 중요

o 관련 KB번호
- 4092465, 4462138, 4462146, 4462174, 4462154, 4461607, 4462186, 4462115, 4461597, 4462177, 4461608, 4018300, 4018294, 4018313

□ 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

MS 2월 보안 위협에 따른 정기 보안 업데이트 권고

출처 : 인터넷침해대응센터
작성일 : 2019.02.13

10. Visual Studio 보안 업데이트

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

o 관련취약점 :
- 원격코드실행 취약점(CVE-2019-0613,CVE-2019-0728)
- 스푸핑 취약점(CVE-2019-0657)

o 영향 : 원격코드실행

o 중요도 : 중요

□ 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

MS 2월 보안 위협에 따른 정기 보안 업데이트 권고

출처 : 인터넷침해대응센터
작성일 : 2019.02.13

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-2019-0594,CVE-2019-0604)
- 권한상승 취약점(CVE-2019-0668)
- 스푸핑 취약점(CVE-2019-0670)

o 영향 : 원격코드실행

o 중요도 : 긴급

o 관련 KB번호
- 4461630, 4462143, 4462155, 4462171, 4462139

□ 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

MS 2월 보안 위협에 따른 정기 보안 업데이트 권고

출처 : 인터넷침해대응센터
작성일 : 2019.02.13

12. Skype 보안 업데이트

□ 설명
o 보안 강화 업데이트

o 관련취약점 :
- 스푸핑 취약점(CVE-2019-0624)

o 영향 : 스푸핑

o 중요도 : 중요

o 관련 KB번호
- 3061064

□ 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

MS 2월 보안 위협에 따른 정기 보안 업데이트 권고

출처 : 인터넷침해대응센터
작성일 : 2019.02.13

13. Exchange Server 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-2019-0686,CVE-2019-0724)

o 영향 : 권한상승

o 중요도 : 중요

o 관련 KB번호
- 4345836, 4471391, 4471392, 4487052

□ 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

MS 2월 보안 위협에 따른 정기 보안 업데이트 권고

출처 : 인터넷침해대응센터
작성일 : 2019.02.13

14. .NET Core 보안 업데이트

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

o 관련취약점 :
- 원격코드실행 취약점(CVE-2019-0613)
- 스푸핑 취약점(CVE-2019-0657)

o 영향 : 원격코드실행

o 중요도 : 중요

o 관련 KB번호
- 4483458, 4483483, 4483459, 4483484, 4483456, 4483481, 4487026, 4487018, 4487020, 4486996, 4487017, 4483452, 4483455, 4483474, 4483453, 4483472, 4483454, 4483473, 4483451, 4483470, 4483457, 4483482, 4483450, 4483469, 4483449, 4483468, 4483451, 4483474

□ 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

MS 2월 보안 위협에 따른 정기 보안 업데이트 권고

출처 : 인터넷침해대응센터
작성일 : 2019.02.13

15. Team Foundation Server 보안 업데이트

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

o 관련취약점 :
- 정보노출 취약점(CVE-2019-0647)
- 스푸핑 취약점(CVE-2019-0646,CVE-2019-0742,CVE-2019-0743)

o 영향 : 정보노출

o 중요도 : 중요

□ 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

MS 2월 보안 위협에 따른 정기 보안 업데이트 권고

출처 : 인터넷침해대응센터
작성일 : 2019.02.13

16. 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 APSB19-08 설명된 취약점

o 영향 : 원격코드실행

o 중요도 : 긴급

o 관련 KB번호
- 4487038

□ 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