MS 4월 보안 위협에 따른 정기 보안 업데이트 권고

출처 : 인터넷침해대응센터
작성일 : 2019.04.10

□ 4월 보안 업데이트 개요(총 13종)
o 등급 : 긴급(Critical) 9 종, 중요(Important) 4 종
o 발표일 : 2019.4.10.(수)
o 업데이트 내용

제품군	중요도	영향	KB번호
Windows 10, Server 2019, Server 2016, Edge	긴급	원격코드실행	4493470 등 6개
Windows 8.1, Server 2012 R2	긴급	원격코드실행	4493446 등 2개
Windows Server 2012	긴급	원격코드실행	4493451 등 2개
Windows RT 8.1	긴급	원격코드실행	4493446
Windows 7, Server 2008 R2	긴급	원격코드실행	4493472 등 2개
Windows Server 2008	긴급	원격코드실행	4493471 등 2개
Internet Explorer	긴급	원격코드실행	4493472 등 14개
ChakraCore	긴급	원격코드실행	-
Office	중요	원격코드실행	4464504 등 5개
SharePoint Server, SharePoint Enterprise Server	중요	DID	4464515 등 6개
Exchange Server	중요	DID	4487563
Team Foundation Server	중요	DID	-
Adobe Flash Player	긴급	원격코드실행	4493478

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 4월 보안 위협에 따른 정기 보안 업데이트 권고

출처 : 인터넷침해대응센터
작성일 : 2019.04.10

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-2019-0739,CVE-2019-0786,CVE-2019-0790,CVE-2019-0792,CVE-2019-0793,CVE-2019-0794,CVE-2019-0806,CVE-2019-0810,CVE-2019-0812,CVE-2019-0829,CVE-2019-0842,CVE-2019-0845,CVE-2019-0846,CVE-2019-0847,CVE-2019-0853,CVE-2019-0856,CVE-2019-0861,CVE-2019-0877)
- 권한상승 취약점(CVE-2019-0685,CVE-2019-0730,CVE-2019-0731,CVE-2019-0735,CVE-2019-0796,CVE-2019-0803,CVE-2019-0805,CVE-2019-0841,CVE-2019-0875)
- 보안기능 우회 취약점(CVE-2019-0732)
- 정보노출 취약점(CVE-2019-0688,CVE-2019-0802,CVE-2019-0833,CVE-2019-0838,CVE-2019-0839,CVE-2019-0840,CVE-2019-0844,CVE-2019-0848,CVE-2019-0849,CVE-2019-0851)
- 스푸핑 취약점(CVE-2019-0764)
- DID 취약점(CVE-2019-0857,CVE-2019-0866,CVE-2019-0867,CVE-2019-0868,CVE-2019-0869,CVE-2019-0870,CVE-2019-0871,CVE-2019-0874)

o 영향 : 원격코드실행

o 중요도 : 긴급

o 관련 KB번호
- 4493470, 4493474, 4493441, 4493464, 4493509, 4493475

□ 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 4월 보안 위협에 따른 정기 보안 업데이트 권고

출처 : 인터넷침해대응센터
작성일 : 2019.04.10

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-2019-0790,CVE-2019-0791,CVE-2019-0792,CVE-2019-0793,CVE-2019-0794,CVE-2019-0795,CVE-2019-0842,CVE-2019-0845,CVE-2019-0846,CVE-2019-0847,CVE-2019-0853,CVE-2019-0856,CVE-2019-0877)
- 권한상승 취약점(CVE-2019-0730,CVE-2019-0731,CVE-2019-0735,CVE-2019-0803,CVE-2019-0805,CVE-2019-0859)
- 보안기능 우회 취약점(CVE-2019-0732)
- 정보노출 취약점(CVE-2019-0688,CVE-2019-0802,CVE-2019-0838,CVE-2019-0839,CVE-2019-0844,CVE-2019-0848,CVE-2019-0849,CVE-2019-0851)

o 영향 : 원격코드실행

o 중요도 : 긴급

o 관련 KB번호
- 4493446, 4493467

□ 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 4월 보안 위협에 따른 정기 보안 업데이트 권고

출처 : 인터넷침해대응센터
작성일 : 2019.04.10

3. Windows Server 2012 보안 업데이트

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

o 관련취약점 :
- 원격코드실행 취약점(CVE-2019-0790,CVE-2019-0791,CVE-2019-0793,CVE-2019-0794,CVE-2019-0842,CVE-2019-0845,CVE-2019-0846,CVE-2019-0847,CVE-2019-0853,CVE-2019-0856,CVE-2019-0877)
- 권한상승 취약점(CVE-2019-0730,CVE-2019-0731,CVE-2019-0735,CVE-2019-0803,CVE-2019-0805)
- 보안기능 우회 취약점(CVE-2019-0732)
- 정보노출 취약점(CVE-2019-0688,CVE-2019-0802,CVE-2019-0838,CVE-2019-0839,CVE-2019-0844,CVE-2019-0848,CVE-2019-0849,CVE-2019-0851)

o 영향 : 원격코드실행

o 중요도 : 긴급

o 관련 KB번호
- 4493451, 4493450

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

Eyeon Security
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 4월 보안 위협에 따른 정기 보안 업데이트 권고

출처 : 인터넷침해대응센터
작성일 : 2019.04.10

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-2019-0790,CVE-2019-0792,CVE-2019-0793,CVE-2019-0794,CVE-2019-0842,CVE-2019-0845,CVE-2019-0846,CVE-2019-0847,CVE-2019-0853,CVE-2019-0856,CVE-2019-0877)
- 권한상승 취약점(CVE-2019-0730,CVE-2019-0731,CVE-2019-0735,CVE-2019-0803,CVE-2019-0805)
- 보안기능 우회 취약점(CVE-2019-0732)
- 정보노출 취약점(CVE-2019-0688,CVE-2019-0802,CVE-2019-0838,CVE-2019-0839,CVE-2019-0844,CVE-2019-0848,CVE-2019-0849,CVE-2019-0851)

o 영향 : 원격코드실행

o 중요도 : 긴급

o 관련 KB번호
- 4493446

□ 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 4월 보안 위협에 따른 정기 보안 업데이트 권고

출처 : 인터넷침해대응센터
작성일 : 2019.04.10

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-2019-0791,CVE-2019-0793,CVE-2019-0794,CVE-2019-0795,CVE-2019-0842,CVE-2019-0845,CVE-2019-0846,CVE-2019-0847,CVE-2019-0853,CVE-2019-0856,CVE-2019-0877)
- 권한상승 취약점(CVE-2019-0730,CVE-2019-0731,CVE-2019-0735,CVE-2019-0803,CVE-2019-0805,CVE-2019-0859)
- 보안기능 우회 취약점(CVE-2019-0732)
- 정보노출 취약점(CVE-2019-0802,CVE-2019-0838,CVE-2019-0839,CVE-2019-0844,CVE-2019-0848,CVE-2019-0849,CVE-2019-0851)

o 영향 : 원격코드실행

o 중요도 : 긴급

o 관련 KB번호
- 4493472, 4493448

□ 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 4월 보안 위협에 따른 정기 보안 업데이트 권고

출처 : 인터넷침해대응센터
작성일 : 2019.04.10

6. Windows Server 2008 보안 업데이트

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

o 관련취약점 :
- 원격코드실행 취약점(CVE-2019-0791,CVE-2019-0793,CVE-2019-0794,CVE-2019-0795,CVE-2019-0842,CVE-2019-0845,CVE-2019-0846,CVE-2019-0847,CVE-2019-0853,CVE-2019-0856,CVE-2019-0877)
- 권한상승 취약점(CVE-2019-0730,CVE-2019-0731,CVE-2019-0735,CVE-2019-0803,CVE-2019-0805,CVE-2019-0859)
- 보안기능 우회 취약점(CVE-2019-0732)
- 정보노출 취약점(CVE-2019-0802,CVE-2019-0838,CVE-2019-0839,CVE-2019-0844,CVE-2019-0848,CVE-2019-0849,CVE-2019-0851)

o 영향 : 원격코드실행

o 중요도 : 긴급

o 관련 KB번호
- 4493471, 4493458

□ 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 4월 보안 위협에 따른 정기 보안 업데이트 권고

출처 : 인터넷침해대응센터
작성일 : 2019.04.10

7. Internet Explorer 보안 업데이트

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

o 관련취약점 :
- 원격코드실행 취약점(CVE-2019-0752,CVE-2019-0753,CVE-2019-0862)
- 스푸핑 취약점(CVE-2019-0764)

o 영향 : 원격코드실행

o 중요도 : 긴급

o 관련 KB번호
- 4493472, 4493435, 4493446, 4493435, 4493470, 4493475, 4493474, 4493441, 4493464, 4493509, 4493451, 4493435, 4493471, 4493435

□ 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 4월 보안 위협에 따른 정기 보안 업데이트 권고

출처 : 인터넷침해대응센터
작성일 : 2019.04.10

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-2019-0739,CVE-2019-0806,CVE-2019-0810,CVE-2019-0829,CVE-2019-0861)

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

MS 4월 보안 위협에 따른 정기 보안 업데이트 권고

출처 : 인터넷침해대응센터
작성일 : 2019.04.10

9. Office 보안 업데이트

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

o 관련취약점 :
- 원격코드실행 취약점(CVE-2019-0801,CVE-2019-0828)

o 영향 : 원격코드실행

o 중요도 : 중요

o 관련 KB번호
- 4464504, 4462242, 4462223, 4462209, 4462236

□ 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 4월 보안 위협에 따른 정기 보안 업데이트 권고

출처 : 인터넷침해대응센터
작성일 : 2019.04.10

10. SharePoint Server, SharePoint Enterprise Server 보안 업데이트

□ 설명
o 보안 강화 업데이트

o 관련취약점 :
- DID 취약점(CVE-2019-0830,CVE-2019-0831)

o 영향 : DID

o 중요도 : 중요

o 관련 KB번호
- 4464515, 4464510, 4464518, 4464525, 4464511, 4464528

□ 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 4월 보안 위협에 따른 정기 보안 업데이트 권고

출처 : 인터넷침해대응센터
작성일 : 2019.04.10

11. Exchange Server 보안 업데이트

□ 설명
o 보안 강화 업데이트

o 관련취약점 :
- DID 취약점(CVE-2019-0858)

o 영향 : DID

o 중요도 : 중요

o 관련 KB번호
- 4487563

□ 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 4월 보안 위협에 따른 정기 보안 업데이트 권고

출처 : 인터넷침해대응센터
작성일 : 2019.04.10

12. Team Foundation Server 보안 업데이트

□ 설명
o 보안 강화 업데이트

o 관련취약점 :
- DID 취약점(CVE-2019-0866,CVE-2019-0867,CVE-2019-0868,CVE-2019-0870,CVE-2019-0871)

o 영향 : DID

o 중요도 : 중요

□ 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 4월 보안 위협에 따른 정기 보안 업데이트 권고

출처 : 인터넷침해대응센터
작성일 : 2019.04.10

13. 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 APSB19-19 설명된 취약점

o 영향 : 원격코드실행

o 중요도 : 긴급

o 관련 KB번호
- 4493478

□ 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