MS 3월 보안 위협에 따른 정기 보안 업데이트 권고

출처 : 인터넷침해대응센터
작성일 : 2019.03.13

□ 3월 보안 업데이트 개요(총 15종)
o 등급 : 긴급(Critical) 8 종, 중요(Important) 5 종, 낮음(Low) 2 종
o 발표일 : 2019.3.13.(수)
o 업데이트 내용

제품군	중요도	영향	KB번호
Windows 10, Server 2019, Server 2016, Edge	긴급	원격코드실행	4487006 등 11개
Windows 8.1, Server 2012 R2	긴급	원격코드실행	4489881 등 2개
Windows Server 2012	긴급	원격코드실행	4489891 등 2개
Windows RT 8.1	긴급	원격코드실행	4489881
Windows 7, Server 2008 R2	긴급	원격코드실행	4474419 등 3개
Windows Server 2008	긴급	원격코드실행	4489880 등 2개
Internet Explorer	긴급	원격코드실행	4489878 등 14개
ChakraCore	긴급	원격코드실행	-
Office	중요	원격코드실행	4462226
Visual Studio	중요	스푸핑	-
SharePoint Server, SharePoint Enterprise Server	중요	스푸핑	4462208 등 2개
Lync	중요	DID	2809243
.NET Core	중요	스푸핑	-
Team Foundation Server	낮음	DID	-
Adobe Flash Player	낮음	DID	4489907

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 3월 보안 위협에 따른 정기 보안 업데이트 권고

출처 : 인터넷침해대응센터
작성일 : 2019.03.13

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-2019-0603,CVE-2019-0609,CVE-2019-0617,CVE-2019-0678,CVE-2019-0726,CVE-2019-0746,CVE-2019-0756,CVE-2019-0765,CVE-2019-0780,CVE-2019-0784)
- 권한상승 취약점(CVE-2019-0592,CVE-2019-0682,CVE-2019-0689,CVE-2019-0692,CVE-2019-0693,CVE-2019-0694,CVE-2019-0766,CVE-2019-0797)
- 서비스거부 취약점(CVE-2019-0690,CVE-2019-0754)
- 보안기능 우회 취약점(CVE-2019-0612,CVE-2019-0762)
- 정보노출 취약점(CVE-2019-0611,CVE-2019-0614,CVE-2019-0702,CVE-2019-0703,CVE-2019-0704,CVE-2019-0755,CVE-2019-0767,CVE-2019-0774,CVE-2019-0775,CVE-2019-0776,CVE-2019-0779,CVE-2019-0782,CVE-2019-0821)
- DID 취약점(CVE-2019-0798)

o 영향 : 원격코드실행

o 중요도 : 긴급

o 관련 KB번호
- 4487006, 4487011, 4487021, 4487029, 4489899, 4489882, 4489868, 4489872, 4489871, 4489886, 3061064

□ 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 3월 보안 위협에 따른 정기 보안 업데이트 권고

출처 : 인터넷침해대응센터
작성일 : 2019.03.13

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-2019-0603,CVE-2019-0617,CVE-2019-0756,CVE-2019-0765,CVE-2019-0784)
- 권한상승 취약점(CVE-2019-0797)
- 서비스거부 취약점(CVE-2019-0690,CVE-2019-0754)
- 정보노출 취약점(CVE-2019-0614,CVE-2019-0703,CVE-2019-0704,CVE-2019-0755,CVE-2019-0759,CVE-2019-0767,CVE-2019-0775,CVE-2019-0782,CVE-2019-0821)

o 영향 : 원격코드실행

o 중요도 : 긴급

o 관련 KB번호
- 4489881, 4489883

□ 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 3월 보안 위협에 따른 정기 보안 업데이트 권고

출처 : 인터넷침해대응센터
작성일 : 2019.03.13

3. Windows Server 2012 보안 업데이트

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

o 관련취약점 :
- 원격코드실행 취약점(CVE-2019-0603,CVE-2019-0617,CVE-2019-0756,CVE-2019-0765,CVE-2019-0784)
- 권한상승 취약점(CVE-2019-0797)
- 서비스거부 취약점(CVE-2019-0690,CVE-2019-0754)
- 정보노출 취약점(CVE-2019-0614,CVE-2019-0703,CVE-2019-0704,CVE-2019-0755,CVE-2019-0767,CVE-2019-0775,CVE-2019-0782,CVE-2019-0821)

o 영향 : 원격코드실행

o 중요도 : 긴급

o 관련 KB번호
- 4489891, 4489884

□ 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 3월 보안 위협에 따른 정기 보안 업데이트 권고

출처 : 인터넷침해대응센터
작성일 : 2019.03.13

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-2019-0603,CVE-2019-0617,CVE-2019-0756,CVE-2019-0765,CVE-2019-0784)
- 권한상승 취약점(CVE-2019-0797)
- 서비스거부 취약점(CVE-2019-0754)
- 정보노출 취약점(CVE-2019-0614,CVE-2019-0703,CVE-2019-0704,CVE-2019-0755,CVE-2019-0767,CVE-2019-0775,CVE-2019-0782,CVE-2019-0821)

o 영향 : 원격코드실행

o 중요도 : 긴급

o 관련 KB번호
- 4489881

□ 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 3월 보안 위협에 따른 정기 보안 업데이트 권고

출처 : 인터넷침해대응센터
작성일 : 2019.03.13

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-2019-0603,CVE-2019-0617,CVE-2019-0756,CVE-2019-0765,CVE-2019-0784)
- 권한상승 취약점(CVE-2019-0683,CVE-2019-0808)
- 서비스거부 취약점(CVE-2019-0690,CVE-2019-0754)
- 정보노출 취약점(CVE-2019-0614,CVE-2019-0703,CVE-2019-0704,CVE-2019-0755,CVE-2019-0759,CVE-2019-0767,CVE-2019-0775,CVE-2019-0782,CVE-2019-0821)

o 영향 : 원격코드실행

o 중요도 : 긴급

o 관련 KB번호
- 4474419, 4489878, 4489885

□ 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 3월 보안 위협에 따른 정기 보안 업데이트 권고

출처 : 인터넷침해대응센터
작성일 : 2019.03.13

6. Windows Server 2008 보안 업데이트

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

o 관련취약점 :
- 원격코드실행 취약점(CVE-2019-0603,CVE-2019-0617,CVE-2019-0756,CVE-2019-0765,CVE-2019-0784)
- 권한상승 취약점(CVE-2019-0683,CVE-2019-0808)
- 서비스거부 취약점(CVE-2019-0690,CVE-2019-0754)
- 정보노출 취약점(CVE-2019-0614,CVE-2019-0703,CVE-2019-0704,CVE-2019-0755,CVE-2019-0759,CVE-2019-0767,CVE-2019-0775,CVE-2019-0782,CVE-2019-0821)

o 영향 : 원격코드실행

o 중요도 : 긴급

o 관련 KB번호
- 4489880, 4489876

□ 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 3월 보안 위협에 따른 정기 보안 업데이트 권고

출처 : 인터넷침해대응센터
작성일 : 2019.03.13

7. Internet Explorer 보안 업데이트

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

o 관련취약점 :
- 원격코드실행 취약점(CVE-2019-0609,CVE-2019-0667,CVE-2019-0680,CVE-2019-0746,CVE-2019-0763,CVE-2019-0780,CVE-2019-0783)
- 보안기능 우회 취약점(CVE-2019-0762)

o 영향 : 원격코드실행

o 중요도 : 긴급

o 관련 KB번호
- 4489878, 4489873, 4489881, 4489873, 4489882, 4489872, 4489871, 4489886, 4489868, 4489899, 4489891, 4489873, 4489880, 4489873

□ 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 3월 보안 위협에 따른 정기 보안 업데이트 권고

출처 : 인터넷침해대응센터
작성일 : 2019.03.13

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-2019-0609,CVE-2019-0746)
- 권한상승 취약점(CVE-2019-0592)
- 정보노출 취약점(CVE-2019-0611)

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 3월 보안 위협에 따른 정기 보안 업데이트 권고

출처 : 인터넷침해대응센터
작성일 : 2019.03.13

9. Office 보안 업데이트

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

o 관련취약점 :
- 원격코드실행 취약점(CVE-2019-0748)

o 영향 : 원격코드실행

o 중요도 : 중요

o 관련 KB번호
- 4462226

□ 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 3월 보안 위협에 따른 정기 보안 업데이트 권고

출처 : 인터넷침해대응센터
작성일 : 2019.03.13

10. Visual Studio 보안 업데이트

□ 설명
o 공격자가 NW/시스템 접근에 필요한 특정값을 탈취하거나 변조를 통해 접근제어를 우회하는 취약점

o 관련취약점 :
- 스푸핑 취약점(CVE-2019-0757)

o 영향 : 스푸핑

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 3월 보안 위협에 따른 정기 보안 업데이트 권고

출처 : 인터넷침해대응센터
작성일 : 2019.03.13

11. SharePoint Server, SharePoint Enterprise Server 보안 업데이트

□ 설명
o 공격자가 NW/시스템 접근에 필요한 특정값을 탈취하거나 변조를 통해 접근제어를 우회하는 취약점

o 관련취약점 :
- 스푸핑 취약점(CVE-2019-0778)

o 영향 : 스푸핑

o 중요도 : 중요

o 관련 KB번호
- 4462208, 4462211

□ 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 3월 보안 위협에 따른 정기 보안 업데이트 권고

출처 : 인터넷침해대응센터
작성일 : 2019.03.13

12. Lync 보안 업데이트

□ 설명
o 보안 강화 업데이트

o 관련취약점 :
- DID 취약점(CVE-2019-0798)

o 영향 : DID

o 중요도 : 중요

o 관련 KB번호
- 2809243

□ 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 3월 보안 위협에 따른 정기 보안 업데이트 권고

출처 : 인터넷침해대응센터
작성일 : 2019.03.13

13. .NET Core 보안 업데이트

□ 설명
o 공격자가 NW/시스템 접근에 필요한 특정값을 탈취하거나 변조를 통해 접근제어를 우회하는 취약점

o 관련취약점 :
- 스푸핑 취약점(CVE-2019-0757)

o 영향 : 스푸핑

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 3월 보안 위협에 따른 정기 보안 업데이트 권고

출처 : 인터넷침해대응센터
작성일 : 2019.03.13

14. Team Foundation Server 보안 업데이트

□ 설명
o 보안 강화 업데이트

o 관련취약점 :
- DID 취약점(CVE-2019-0777)

o 영향 : DID

o 중요도 : 낮음

□ 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 3월 보안 위협에 따른 정기 보안 업데이트 권고

출처 : 인터넷침해대응센터
작성일 : 2019.03.13

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 APSB19-12 설명된 취약점

o 영향 : DID

o 중요도 : 낮음

o 관련 KB번호
- 4489907

□ 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