

## 보안 취약점 자료

문서 제목	MS 5월 보안 위협에 따른 정기 보안 업데이트 권고
문서 번호	A3AEGIS-20190515-01
작성 일자	2019년 05월 15일
제공 부서	(주)에이쓰리시큐리티

# 보안 취약점 자료

제 목	MS 5월 보안 위협에 따른 정기 보안 업데이트 권고																																																																		
내 용	<p>□ 5월 보안 업데이트 개요(총 15종)</p> <p>○ 등급 : 긴급(Critical) 9 종, 중요(Important) 6 종</p> <p>○ 발표일 : 2019.5.15.(수)</p> <p>○ 업데이트 내용</p> <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="width: 45%;">제품군</th> <th style="width: 10%;">중요도</th> <th style="width: 25%;">영향</th> <th style="width: 20%;">KB번호</th> </tr> </thead> <tbody> <tr> <td>Windows 10, Server 2019, Server 2016, Edge</td> <td>긴급</td> <td>원격코드실행</td> <td>4494440 등 7개</td> </tr> <tr> <td>Windows 8.1, Server 2012 R2</td> <td>긴급</td> <td>원격코드실행</td> <td>4499151 등 2개</td> </tr> <tr> <td>Windows Server 2012</td> <td>긴급</td> <td>원격코드실행</td> <td>4499171 등 2개</td> </tr> <tr> <td>Windows RT 8.1</td> <td>중요</td> <td>원격코드실행</td> <td>4499151</td> </tr> <tr> <td>Windows 7, Server 2008 R2</td> <td>긴급</td> <td>원격코드실행</td> <td>4499164 등 2개</td> </tr> <tr> <td>Windows Server 2008</td> <td>긴급</td> <td>원격코드실행</td> <td>4499149 등 2개</td> </tr> <tr> <td>Internet Explorer</td> <td>긴급</td> <td>원격코드실행</td> <td>4499167 등 15개</td> </tr> <tr> <td>ChakraCore</td> <td>긴급</td> <td>원격코드실행</td> <td>-</td> </tr> <tr> <td>Office</td> <td>긴급</td> <td>원격코드실행</td> <td>4464561 등 5개</td> </tr> <tr> <td>Visual Studio</td> <td>중요</td> <td>권한상승</td> <td>4489639</td> </tr> <tr> <td>SharePoint Server, SharePoint Enterprise Server</td> <td>중요</td> <td>원격코드실행</td> <td>4464564 등 4개</td> </tr> <tr> <td>Skype</td> <td>중요</td> <td>정보노출</td> <td>-</td> </tr> <tr> <td>ASP.NET Core, .NET Core</td> <td>중요</td> <td>서비스거부</td> <td>4499409 등 19개</td> </tr> <tr> <td>Team Foundation Server</td> <td>중요</td> <td>스푸핑</td> <td>-</td> </tr> <tr> <td>Adobe Flash Player</td> <td>긴급</td> <td>원격코드실행</td> <td>4497932</td> </tr> </tbody> </table>			제품군	중요도	영향	KB번호	Windows 10, Server 2019, Server 2016, Edge	긴급	원격코드실행	4494440 등 7개	Windows 8.1, Server 2012 R2	긴급	원격코드실행	4499151 등 2개	Windows Server 2012	긴급	원격코드실행	4499171 등 2개	Windows RT 8.1	중요	원격코드실행	4499151	Windows 7, Server 2008 R2	긴급	원격코드실행	4499164 등 2개	Windows Server 2008	긴급	원격코드실행	4499149 등 2개	Internet Explorer	긴급	원격코드실행	4499167 등 15개	ChakraCore	긴급	원격코드실행	-	Office	긴급	원격코드실행	4464561 등 5개	Visual Studio	중요	권한상승	4489639	SharePoint Server, SharePoint Enterprise Server	중요	원격코드실행	4464564 등 4개	Skype	중요	정보노출	-	ASP.NET Core, .NET Core	중요	서비스거부	4499409 등 19개	Team Foundation Server	중요	스푸핑	-	Adobe Flash Player	긴급	원격코드실행	4497932
제품군	중요도	영향	KB번호																																																																
Windows 10, Server 2019, Server 2016, Edge	긴급	원격코드실행	4494440 등 7개																																																																
Windows 8.1, Server 2012 R2	긴급	원격코드실행	4499151 등 2개																																																																
Windows Server 2012	긴급	원격코드실행	4499171 등 2개																																																																
Windows RT 8.1	중요	원격코드실행	4499151																																																																
Windows 7, Server 2008 R2	긴급	원격코드실행	4499164 등 2개																																																																
Windows Server 2008	긴급	원격코드실행	4499149 등 2개																																																																
Internet Explorer	긴급	원격코드실행	4499167 등 15개																																																																
ChakraCore	긴급	원격코드실행	-																																																																
Office	긴급	원격코드실행	4464561 등 5개																																																																
Visual Studio	중요	권한상승	4489639																																																																
SharePoint Server, SharePoint Enterprise Server	중요	원격코드실행	4464564 등 4개																																																																
Skype	중요	정보노출	-																																																																
ASP.NET Core, .NET Core	중요	서비스거부	4499409 등 19개																																																																
Team Foundation Server	중요	스푸핑	-																																																																
Adobe Flash Player	긴급	원격코드실행	4497932																																																																

# 보안 취약점 자료

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

설명

- 공격자가 특수하게 제작된 악성 응용 프로그램을 실행할 경우, 원격코드실행을 허용하는 취약점
  
- 관련취약점 :
  - 원격코드실행 취약점(CVE-2019-0884,CVE-2019-0885,CVE-2019-0889,CVE-2019-0890,CVE-2019-0891,CVE-2019-0895,CVE-2019-0896,CVE-2019-0897,CVE-2019-0898,CVE-2019-0899,CVE-2019-0900,CVE-2019-0901,CVE-2019-0912,CVE-2019-0913,CVE-2019-0914,CVE-2019-0915,CVE-2019-0916,CVE-2019-0917,CVE-2019-0923,CVE-2019-0924,CVE-2019-0925,CVE-2019-0926,CVE-2019-0927,CVE-2019-0933,CVE-2019-0937,CVE-2019-0940)
  - 권한상승 취약점(CVE-2019-0707,CVE-2019-0727,CVE-2019-0734,CVE-2019-0863,CVE-2019-0881,CVE-2019-0892,CVE-2019-0931,CVE-2019-0938,CVE-2019-0942)
  - 보안기능 우회 취약점(CVE-2019-0733)
  - 정보노출 취약점(ADV190013,CVE-2019-0758,CVE-2019-0882,CVE-2019-0886,CVE-2019-0961)
  - DID 취약점(CVE-2019-0872)
  
- 영향 : 원격코드실행
  
- 중요도 : 긴급
  
- 관련 KB 번호
  - 4494440, 4499154, 4499181, 4499179, 4499167, 4494441, 4497936

해결책

- 영향 받는 소프트웨어를 이용하는 경우 마이크로소프트사의 보안 패치 적용

## 2. Windows 8.1, Server 2012 R2 보안 업데이트

설명

- 공격자가 특수하게 제작된 악성 응용 프로그램을 실행할 경우, 원격코드실행을 허용하는 취약점
  
- 관련취약점 :
  - 원격코드실행 취약점(CVE-2019-0725,CVE-2019-0885,CVE-2019-0889,CVE-2019-0890,CVE-2019-0891,CVE-2019-

# 보안 취약점 자료

0895,CVE-2019-0896,CVE-2019-0897,CVE-2019-0898,CVE-2019-0899,CVE-2019-0900,CVE-2019-0901,CVE-2019-0902)

- 권한상승 취약점(CVE-2019-0707,CVE-2019-0734,CVE-2019-0863,CVE-2019-0881)
- 정보노출 취약점(ADV190013,CVE-2019-0758,CVE-2019-0882,CVE-2019-0961)

o 영향 : 원격코드실행

o 중요도 : 긴급

o 관련 KB 번호

- 4499151, 4499165

해결책

- o 영향 받는 소프트웨어를 이용하는 경우 마이크로소프트사의 보안 패치 적용

### 3. Windows Server 2012 보안 업데이트

설명

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

o 관련취약점 :

- 원격코드실행 취약점(CVE-2019-0725,CVE-2019-0885,CVE-2019-0889,CVE-2019-0890,CVE-2019-0891,CVE-2019-0895,CVE-2019-0896,CVE-2019-0897,CVE-2019-0898,CVE-2019-0899,CVE-2019-0900,CVE-2019-0901)
- 권한상승 취약점(CVE-2019-0707,CVE-2019-0734,CVE-2019-0863,CVE-2019-0881)
- 정보노출 취약점(ADV190013,CVE-2019-0758,CVE-2019-0882,CVE-2019-0961)

o 영향 : 원격코드실행

o 중요도 : 긴급

o 관련 KB 번호

- 4499171, 4499158

# 보안 취약점 자료

해결책

- 영향 받는 소프트웨어를 이용하는 경우 마이크로소프트사의 보안 패치 적용

#### 4. Windows RT 8.1 보안 업데이트

설명

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

○ 관련취약점 :

- 원격코드실행 취약점(CVE-2019-0885,CVE-2019-0890,CVE-2019-0891,CVE-2019-0895,CVE-2019-0896,CVE-2019-0897,CVE-2019-0898,CVE-2019-0899,CVE-2019-0900,CVE-2019-0901)
- 권한상승 취약점(CVE-2019-0707,CVE-2019-0734,CVE-2019-0863,CVE-2019-0881)
- 정보노출 취약점(CVE-2019-0882,CVE-2019-0961)

- 영향 : 원격코드실행

- 중요도 : 중요

○ 관련 KB 번호

- 4499151

해결책

- 영향 받는 소프트웨어를 이용하는 경우 마이크로소프트사의 보안 패치 적용

#### 5. Windows 7, Server 2008 R2 보안 업데이트

설명

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

○ 관련취약점 :

- 원격코드실행 취약점(CVE-2019-0708,CVE-2019-0725,CVE-2019-0885,CVE-2019-0889,CVE-2019-0890,CVE-2019-0891,CVE-2019-0895,CVE-2019-0896,CVE-2019-0897,CVE-2019-0898,CVE-2019-0899,CVE-2019-0900,CVE-2019-

# 보안 취약점 자료

0901,CVE-2019-0902)

- 권한상승 취약점(CVE-2019-0734,CVE-2019-0863,CVE-2019-0881)
- 정보노출 취약점(ADV190013,CVE-2019-0758,CVE-2019-0882,CVE-2019-0961)

o 영향 : 원격코드실행

o 중요도 : 긴급

o 관련 KB 번호

- 4499164, 4499175

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-2019-0708,CVE-2019-0885,CVE-2019-0889,CVE-2019-0890,CVE-2019-0891,CVE-2019-0895,CVE-2019-0896,CVE-2019-0897,CVE-2019-0898,CVE-2019-0899,CVE-2019-0900,CVE-2019-0901,CVE-2019-0902)

- 권한상승 취약점(CVE-2019-0734,CVE-2019-0881)

- 정보노출 취약점(CVE-2019-0758,CVE-2019-0882,CVE-2019-0961)

o 영향 : 원격코드실행

o 중요도 : 긴급

o 관련 KB 번호

- 4499149, 4499180

# 보안 취약점 자료

해결책

- 영향 받는 소프트웨어를 이용하는 경우 마이크로소프트사의 보안 패치 적용

## 7. Internet Explorer 보안 업데이트

설명

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

○ 관련취약점 :

- 원격코드실행 취약점(CVE-2019-0884,CVE-2019-0911,CVE-2019-0929,CVE-2019-0940)
- 보안기능 우회 취약점(CVE-2019-0995)
- 정보노출 취약점(CVE-2019-0930)

- 영향 : 원격코드실행

- 중요도 : 긴급

○ 관련 KB 번호

- 4499167, 4494441, 4497936, 4499164, 4498206, 4499151, 4498206, 4494440, 4499154, 4499181, 4499179, 4499171, 4498206, 4498206, 4499149

해결책

- 영향 받는 소프트웨어를 이용하는 경우 마이크로소프트사의 보안 패치 적용

## 8. ChakraCore 보안 업데이트

설명

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

○ 관련취약점 :

- 원격코드실행 취약점(CVE-2019-0911,CVE-2019-0912,CVE-2019-0913,CVE-2019-0914,CVE-2019-0915,CVE-2019-

# 보안 취약점 자료

0916,CVE-2019-0924,CVE-2019-0925,CVE-2019-0927,CVE-2019-0937)

- 영향 : 원격코드실행
- 중요도 : 긴급
- 해결책
- 영향 받는 소프트웨어를 이용하는 경우 마이크로소프트사의 보안 패치 적용

## 9. Office 보안 업데이트

- 설명
- 이용자가 특수하게 제작된 악성 문서를 열람할 경우, 원격코드실행을 허용하는 취약점
- 관련취약점 :
  - 원격코드실행 취약점(CVE-2019-0945,CVE-2019-0946,CVE-2019-0947,CVE-2019-0953)
- 영향 : 원격코드실행
- 중요도 : 긴급
- 관련 KB 번호
  - 4464561, 4464551, 4464567, 4464536, 4462169
- 해결책
- 영향 받는 소프트웨어를 이용하는 경우 마이크로소프트사의 보안 패치 적용

## 10. Visual Studio 보안 업데이트

- 설명
- 공격자가 프로그램 버그(실행 처리 구문의 허점 등)를 악용하여 보호되는 자원들에 임의로 접근하는 권한상승 취약점

# 보안 취약점 자료

○ 관련취약점 :

- 권한상승 취약점(CVE-2019-0727)

○ 영향 : 권한상승

○ 중요도 : 중요

○ 관련 KB 번호

- 4489639

해결책

- 영향 받는 소프트웨어를 이용하는 경우 마이크로소프트사의 보안 패치 적용

## 11. SharePoint Server, SharePoint Enterprise Server 보안 업데이트

설명

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

○ 관련취약점 :

- 원격코드실행 취약점(CVE-2019-0952)
- 권한상승 취약점(CVE-2019-0957,CVE-2019-0958)
- 정보노출 취약점(CVE-2019-0956)
- DID 취약점(CVE-2019-0949,CVE-2019-0950,CVE-2019-0951)

○ 영향 : 원격코드실행

○ 중요도 : 중요

○ 관련 KB 번호

- 4464564, 4464549, 4464573, 4464556

해결책

# 보안 취약점 자료

o 영향 받는 소프트웨어를 이용하는 경우 마이크로소프트사의 보안 패치 적용

## 12. Skype 보안 업데이트

### 설명

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

### o 관련취약점 :

- 정보노출 취약점(CVE-2019-0932)

o 영향 : 정보노출

o 중요도 : 중요

### 해결책

o 영향 받는 소프트웨어를 이용하는 경우 마이크로소프트사의 보안 패치 적용

## 13. ASP.NET Core, .NET Core 보안 업데이트

### 설명

o 공격자가 시스템의 자원을 고갈시켜 발생하는 서비스거부 취약점

### o 관련취약점 :

- 서비스거부 취약점(CVE-2019-0820,CVE-2019-0864,CVE-2019-0980,CVE-2019-0981,CVE-2019-0982)

o 영향 : 서비스거부

o 중요도 : 중요

### o 관련 KB 번호

- 4499409, 4498964, 4499167, 4499405, 4494440, 4499406, 4498961, 4499408, 4498963, 4499407, 4498962, 4495610, 4495611, 4495613, 4495616, 4495620, 4499154, 4499181, 4499179

# 보안 취약점 자료

해결책

- 영향 받는 소프트웨어를 이용하는 경우 마이크로소프트사의 보안 패치 적용

## 14. Team Foundation Server 보안 업데이트

설명

- 보안 강화 업데이트

○ 관련취약점 :

- 스푸핑 취약점(CVE-2019-0872)

- 영향 : 스푸핑

- 중요도 : 중요

해결책

- 영향 받는 소프트웨어를 이용하는 경우 마이크로소프트사의 보안 패치 적용

## 15. Adobe Flash Player 보안 업데이트

설명

○ 지원되는 모든 버전의 Windows 8.1, Windows Server 2012, Windows Server 2012 R2, Windows RT 8.1, Windows 10 및 Windows Server 2016 에 설치된 Adobe Flash Player 의 취약점을 해결

○ 관련취약점 :

- Adobe 보안 업데이트 APSB19-26 설명된 취약점

- 영향 : 원격코드실행

- 중요도 : 긴급

## 보안 취약점 자료

○ 관련 KB 번호

- 4497932

□ 해결책

○ 영향 받는 소프트웨어를 이용하는 경우 마이크로소프트사의 보안 패치 적용