SGA 솔루션즈
Microsoft Windows
업데이트 패치

2026. 06.

고유 CVE	긴급 조치 대상
245	12

SGA 에스지에이솔루션즈(주)

MS 윈도우 업데이트 패치 목차

키워드 사전

키워드	설명
Microsoft Patch Tuesday	Microsoft 가 매월 정기적으로 윈도우, 오피스, 서버 제품 등의 보안 업데이트를 배포하는 날입니다. 보통 매월 둘째 주 화요일에 진행되며, 기업에서는 이 날 공개된 패치를 기준으로 보안 조치를 계획합니다.
KB (Knowledge Base)	Microsoft 업데이트에 붙는 고유 번호로, 특정 패치나 문제 해결 내용을 구분하기 위한 식별자입니다. 예를 들어 KB5034123 처럼 표시되며, 어떤 업데이트를 설치해야 하는지 확인할 때 사용합니다.
최대 심각도	해당 보안 업데이트에 포함된 취약점 중 가장 위험도가 높은 등급을 의미합니다. 보통 Critical, Important 등으로 표시되며, 패치 우선순위를 정할 때 참고합니다.
CVE (Common Vulnerabilities and Exposures)	전 세계적으로 공개된 보안 취약점에 부여되는 고유 번호입니다. 예를 들어 CVE-2026-12345 처럼 표시되며, 특정 취약점을 정확히 식별하고 추적하는 데 사용합니다.
CISA KEV(Known Exploited Vulnerability) 카탈로그	미국 CISA 가 실제 공격에 악용된 것으로 확인된 취약점을 모아둔 목록입니다. 이 목록에 포함된 취약점은 공격에 쓰인 이력이 있기 때문에 일반 취약점보다 더 빠른 조치가 필요합니다.
CVSS (Common Vulnerability Scoring System)	보안 취약점의 위험도를 점수로 나타내는 평가 기준입니다. 보통 0.0 부터 10.0 까지의 점수로 표시되며, 점수가 높을수록 더 위험한 취약점으로 봅니다.
스푸핑 (Spoofing)	공격자가 신뢰할 수 있는 사람, 시스템, 웹사이트처럼 속여 사용자를 믿게 만드는 공격 방식입니다. 예를 들어 가짜 로그인 페이지나 위조된 이메일을 통해 계정 정보 입력을 유도할 수 있습니다.

2026 년 6 월 Microsoft Patch Tuesday 는 역대 최대 규모의 보안 업데이트로 발표되었습니다.

이번 업데이트에는 공개된 제로데이 취약점과 실제 악용이 확인된 취약점(CVE-2026-41091, CVE-2026-42897)이 포함되어 있어 각별한 주의가 필요합니다. 일반 및 서버 목록에 포함된 KB ID 는 본문에서 텍스트로 확인할 수 있으며, 각 KB 별 상세 링크는 '6. KB 패치 정보' 항목에서 확인하시기 바랍니다.

핵심 요약

2026 년 6 월 Microsoft 정기 보안 업데이트(Patch Tuesday)에는 **총 245 건의 고유 CVE 가 포함**되었습니다. 이 **중 최대 심각도 기준 Critical 은 65 건, Important 는 177 건이며, CVSS 9.0 이상으로 분류되는 고위험 취약점은 10 건**입니다.

이번 리포트에서는 공개된 취약점을 위험도 기준으로 다시 분류하고, 우선적으로 확인해야 할 **긴급 조치 대상 12 건을 선별**했습니다.

가장 주목할 점은 실제 악용이 확인된 취약점 2 건입니다.

CVE-2026-41091 은 Microsoft Defender 권한 상승 취약점으로, 이미 실제 공격에 악용된 정황이 확인된 제로데이 취약점입니다. 공격자가 이를 악용할 경우 로컬 권한 상승을 통해 SYSTEM 권한을 확보할 수 있어 빠른 점검과 조치가 필요합니다.

CVE-2026-42897 은 Exchange 및 Office 와 관련된 취약점으로, CISA KEV 카탈로그에 등재되었습니다. 악성 문서를 통해 침해로 이어질 수 있는 만큼, 관련 시스템과 사용자 환경을 우선적으로 확인해야 합니다. **두 취약점 모두 이번 업데이트에서 최우선 대응이 필요한 항목**입니다.

미인증 원격 코드 실행(RCE) 취약점도 다수 포함되어 있습니다.

특히 **CVE-2026-47291(HTTP.sys, CVSS 9.8), CVE-2026-45657(Windows 커널/TCP-IP, CVSS 9.8), CVE-2026-44815(DHCP 클라이언트, CVSS 9.8)**는 사용자 상호작용 없이 네트워크를 통해 공격이 가능할 수 있습니다. 따라서 인터넷에 노출된 서버, DHCP, AD 등 핵심 인프라를 우선적으로 점검하고 패치를 적용하는 것이 중요합니다. **CVE-2026-45657** 의 경우 웜 형태의 확산 가능성도 언급되는 만큼 내부 네트워크 관점의 영향도 함께 확인할 필요가 있습니다.

클라우드 영역에서는 **CVE-2026-48567(Azure HorizonDB)**이 CVSS 10.0 으로 가장 높은 점수를 기록했습니다. 다만 Microsoft 가 서비스 단에서 이미 완화 조치를 적용한 상태이므로, 관련 사용 여부와 추가 안내 사항을 함께 확인하는 것이 좋습니다.

이번 패치 배포는 총 36 건의 KB 로 정리됩니다. CERT 대응 관점에서는 다음 항목을 우선적으로 확인하는 것을 권장합니다.

1. 실제 악용이 확인된 2 건의 취약점에 대한 침해 흔적 점검
2. 인터넷 노출 웹 서버(HTTP.sys), DHCP, AD 등 핵심 인프라 우선 패치
3. Exchange EEMS 완화 기능 활성화 여부 확인
4. 패치 전 임시 완화책 적용 여부 검토

   예: HTTP.sys 의 MaxRequestBytes 레지스트리 설정 확인

보안 업데이트는 단순히 최신 패치를 적용하는 작업을 넘어, 실제 악용 가능성과 자사 운영 환경의 노출도를 함께 판단하는 과정이 중요합니다. 이번 리포트를 통해 우선 조치가 필요한 항목을 빠르게 확인하고, 주요 시스템부터 단계적으로 패치 계획을 수립하시기 바랍니다.

1. 전체 통계

항목	건수
고유 CVE 취약점 수	245
긴급 조치 대상(악용확인 OR CVSS≥9.0)	12
최대 심각도 Critical	65
최대 심각도 Important	177
최대 심각도 Moderate/Low	3
CVSS 9.0 이상	10
영향 받는 제품(SKU) 수	143
KB 패치 수	36

2. 영역(태그)별 CVE 현황

영역(태그)	CVE 건수	최고 CVSS	위험등급
Microsoft Exchange Server	8	8.8	긴급
Visual Studio Code	6	9.6	긴급
Windows 커널	4	9.8	긴급
Microsoft Malware Protection Engine	3	정보 없음	긴급
Windows DHCP 클라이언트	2	9.8	긴급
Azure Stack Edge	2	9.8	긴급
Windows TCP/IP	2	9.6	긴급
Microsoft Exchange Online	2	9.1	긴급
Windows DHCP Server	2	9.1	긴급
Azure HorizonDB	1	10.0	긴급

Nuance PowerScribe	1	9.8	긴급
Windows HTTP.sys	1	9.8	긴급
Microsoft Office SharePoint	21	8.8	높음
원격 데스크톱 클라이언트	11	8.8	높음
Windows DWM 핵심 라이브러리	11	7.8	높음
Microsoft Office Word	10	7.8	높음
Microsoft Office	9	8.4	높음
Microsoft Office Excel	8	8.2	높음
Windows 보안 부팅	8	7.9	높음
Windows 푸시 알림	8	7.8	높음
WinSock 용 Windows 보조 기능 드라이버	7	7.8	높음
Windows Kerberos	3	7.1	높음
역할: Windows Hyper-V	2	8.4	높음
Windows Hyper-V	2	8.4	높음
Windows 성능 모니터	2	8.1	높음
Universal Plug and Play(upnp.dll)	2	8.1	높음
Windows NT OS 커널	2	7.8	높음
Windows BitLocker	2	7.8	높음
Windows Win32K - GRFX	2	7.8	높음
Windows 예상 파일 시스템 필터 드라이버	2	7.8	높음
Windows 범용 디스크 형식 파일 시스템 드라이버(UDFS)	2	7.8	높음
Microsoft Azure 증명 서비스 및 디바이스 상태 증명 서비스	2	7.8	높음
.NET	2	7.8	높음
Windows RDP	2	7.5	높음

Windows 전화 통신 서비스	2	7.0	**높음**
Microsoft Azure Kubernetes Service	1	8.8	**높음**
Microsoft Dynamics 365(온-프레미스)	1	8.8	**높음**
Active Directory Domain Services	1	8.8	**높음**
Windows 암호화 서비스	1	8.4	**높음**
GitHub Copilot 및 Visual Studio Code	1	8.4	**높음**
Linux MANA 드라이버	1	8.2	**높음**
Windows 배포 서비스	1	8.1	**높음**
Android 용 Microsoft Teams	1	8.1	**높음**
Microsoft Live Share Canvas SDK	1	8.0	**높음**
Windows 부팅 관리자	1	7.9	**높음**
Windows 커널 모드 드라이버	1	7.8	**높음**
Windows SDK	1	7.8	**높음**
Microsoft Kinect	1	7.8	**높음**
Windows UEFI	1	7.8	**높음**
Windows 핫패치 모니터링 서비스	1	7.8	**높음**
Microsoft 그래픽 구성 요소	1	7.8	**높음**
Windows NTFS	1	7.8	**높음**
Windows 공용 로그 파일 시스템 드라이버	1	7.8	**높음**
Winlogon	1	7.8	**높음**
Windows Bluetooth 서비스	1	7.8	**높음**
Windows Media	1	7.8	**높음**
Windows Narrator Braille	1	7.8	**높음**
Windows 인터넷(wininet.dll)	1	7.8	**높음**
Windows Collaborative Translation Framework	1	7.8	**높음**

Windows 관리자 보호	1	7.8	**높음**
Windows 프로그램 호환성 관리자 서비스	1	7.8	**높음**
Microsoft PowerToys	1	7.8	**높음**
Microsoft Copilot	1	7.7	**높음**
HTTP/2	1	7.5	**높음**
ASP.NET Core	1	7.5	**높음**
Android 용 Office	1	7.1	**높음**
Microsoft Office 간편 실행	1	7.0	**높음**
UI 자동화 관리자(uiamanager.dll)	1	7.0	**높음**
함수 검색 서비스(fdwsd.dll)	1	7.0	**높음**
Windows 저장소	1	7.0	**높음**
Windows Bluetooth 포트 드라이버	1	7.0	**높음**
Microsoft Windows DNS	1	7.0	**높음**
Windows Shell	2	6.5	**보통**
Windows 애플리케이션 ID(AppID) 하위 시스템	2	5.5	**보통**
Microsoft Graph	1	6.5	**보통**
Copilot Chat(Microsoft Edge)	1	6.5	**보통**
M365 Copilot	1	6.5	**보통**
Microsoft UxTheme 라이브러리(uxtheme.dll)	1	5.5	**보통**
Windows 네트워크 컨트롤러(NC) 호스트 에이전트	1	5.5	**보통**
엔드포인트용 Microsoft Defender	1	5.5	**보통**
Windows MOTW(Mark of the Web)	1	5.4	**보통**
Microsoft Office Project	1	4.6	**보통**
Microsoft Bing	1	4.3	**보통**
Microsoft Edge (Chromium)	5	정보 없음	정보 없음

Microsoft	5	정보 없음	정보 없음
Microsoft PC Manager	3	정보 없음	정보 없음
Windows	3	정보 없음	정보 없음
Microsoft SharePoint Enterprise Server	2	정보 없음	정보 없음
Microsoft Entra ID	2	정보 없음	정보 없음
Dynamics	1	정보 없음	정보 없음
Azure Synapse	1	정보 없음	정보 없음
Microsoft Dynamics	1	정보 없음	정보 없음
Azure Active Directory	1	정보 없음	정보 없음
Azure AI Bot Service	1	정보 없음	정보 없음
Microsoft Cost Management	1	정보 없음	정보 없음
GitHub Copilot Chat	1	정보 없음	정보 없음
Microsoft Global Secure Access (GSA)	1	정보 없음	정보 없음
Microsoft Planetary Computer Pro (GeoCatalog)	1	정보 없음	정보 없음
Azure Stack HCI	1	정보 없음	정보 없음
Azure Resource Manager	1	정보 없음	정보 없음
Azure Virtual Network Gateway	1	정보 없음	정보 없음
Azure Privileged Identity Management (PIM)	1	정보 없음	정보 없음
Microsoft Power Pages	1	정보 없음	정보 없음
Azure Orbital Spatio	1	정보 없음	정보 없음
Windows Admin Center in Azure Portal	1	정보 없음	정보 없음
Microsoft Defender Antimalware Platform	1	정보 없음	정보 없음
Azure Local	1	정보 없음	정보 없음
Microsoft Authenticator	1	정보 없음	정보 없음

3. 긴급 조치 목록 (악용 확인 + CVSS 9.0 이상)

실제 악용이 확인되었거나 CVSS 9.0 이상인 최우선 조치 대상입니다.

연번	분류	CVE	영향	CVSS	위험등급	권장조치	KB ID	비고
1	Microsoft Malware Protection Engine	CVE-2026-41091	권한 상승	정보 없음	긴급	긴급 패치 권고	정보 없음	**Microsoft Defender 권한 상승(CVSS 7.8)** - 실제 악용 확인(제로데이). 다수 연구자 크레딧으로 광범위한 인더 와일드 악용 정황. 로컬 권한 상승으로 초기 침투를 SYSTEM 장악으로 확대 가능. Defender 는 자동 업데이트되므로 대부분 자동 보호되나, 자동 업데이트 비활성/격리 환경은 최신 보안 인텔리전스로 즉시 갱신 필요. 악용 확인.
2	Microsoft Exchange Server	CVE-2026-42897	스푸핑	정보 없음	긴급	긴급 패치 권고	5094139, 5094140, 5094142, 5094144	**Microsoft Office/Word 관련 취약점** - CISA KEV(알려진 악용 취약점) 등재, 실제 악용 확인. 악성 문서 전달을 통한 침해 가능. 사용자에게 미확인 Office/Word 문서 열람 주의 공지 및 즉시 패치 권장. 악용 확인.
3	Azure HorizonDB	CVE-2026-48567	권한 상승	10.0	긴급	긴급 패치 권고	정보 없음	**Azure HorizonDB 인증 우회(스푸핑) 취약점(CVSS 10.0, 최대 심각도)** - 미인증 원격 공격자가 인증을 우회하여 네트워크에서 권한 상승 가능. Scope:Changed 로

								관리 ID·서비스 주체를 통해 연결된 다른 Azure 리소스로의 측면 이동 위험. Microsoft 가 서비스 측에서 이미 완화 완료하여 사용자 조치는 원칙적으로 불필요하나, HorizonDB 접근 로그 감사 및 자격 증명 교체 권장. 공개 PoC 없음.
4	Nuance PowerScribe	CVE-2026-26142	원격 코드 실행	9.8	**긴급**	긴급 패치 권고	정보 없음	**Nuance PowerScribe 360(4.0/4.0.1) 취약점(CVSS 9.8)** - AV:N/AC:L/PR:N/UI:N 미인증 원격 공격자가 낮은 난이도로 침해 가능. 의료 음성인식 워크플로 시스템으로 네트워크 격리 및 즉시 패치 권장. 악용 가능성 낮음.
5	Windows DHCP 클라이언트	CVE-2026-44815	원격 코드 실행	9.8	**긴급**	긴급 패치 권고	5093998, 5094041, 5094042, 5094122, 5094123, 5094125, 5094126, 5094127, 5094128, 5095051	**Windows DHCP 클라이언트 서비스 원격 코드 실행(CVSS 9.8)** - 스택 기반 버퍼 오버플로로 미인증 원격 공격자가 사용자 상호작용 없이 코드 실행. 공격자가 네트워크상 악성 DHCP 서버를 운영하여 조작된 응답을 전송하는 방식. DhcpGetOriginalSubnetMask API 호출이 조건이므로 패치 전 완화책으로 해당 API 사용 애플리케이션을 점검·제한 권장. 악용 가능성 낮음.

6	Windows 커널	CVE-2026-45657	원격 코드 실행	9.8	긴급	긴급 패치 권고	5093998, 5094125, 5094126, 5094128, 5095051	**Windows 커널 원격 코드 실행(CVSS 9.8)** - 커널의 TCP/IP 처리 결함으로 미인증 원격 공격자가 사용자 상호작용 없이 SYSTEM 권한으로 코드 실행 가능(웜 확산 가능성 지적됨). Microsoft 평가는 '악용 가능성 낮음'이나 패치 역분석을 통한 익스플로잇 개발 가능성이 높아 신속 배포 권장.
7	Windows HTTP.sys	CVE-2026-47291	원격 코드 실행	9.8	긴급	긴급 패치 권고	5093998, 5094041, 5094042, 5094122, 5094123, 5094125, 5094126, 5094127, 5094128, 5095051	**Windows HTTP.sys 원격 코드 실행(CVSS 9.8)** - 정수 오버플로 및 힙 기반 버퍼 오버플로로 미인증 원격 공격자가 사용자 상호작용 없이 코드 실행. 기본 MaxRequestBytes 레지스트리 값을 사용하는 시스템은 영향받지 않음. 패치 전 완화책으로 레지스트리 값 확인(고시된 PowerShell 스크립트 활용). Microsoft 평가 '악용 가능성 높음'으로 인터넷 노출 웹 서비스 최우선 조치.
8	Azure Stack Edge	CVE-2026-47643	원격 코드 실행	9.8	긴급	긴급 패치 권고	정보 없음	**Azure Stack Edge 취약점(CVSS 9.8)** - 미인증 원격 공격자에 의한 높은 영향의 침해 가능. 엣지 어플라이언스 특성상 온-프레미스 관리 인터페이스 노출을 최소화하고 즉시 패치 권장. 악용 가능성 낮음.

9	Windows TCP/IP	CVE-2026-42904	권한 상승	9.6	긴급	긴급 패치 권고	5093998, 5094125, 5094126, 5094127, 5094128, 5095051	**Windows 10(21H2 등) 취약점(CVSS 9.6)** - 광범위한 클라이언트 SKU 에 영향. 미인증/저권한 공격자에 의한 고영향 침해 가능성으로 신속 패치 권장. 악용 가능성 낮음.
10	Visual Studio Code	CVE-2026-47281	권한 상승	9.6	긴급	긴급 패치 권고	정보 없음	**Visual Studio Code 취약점(CVSS 9.6)** - 개발자 엔드포인트 대상 고위험 취약점으로 확장·작업영역 신뢰 처리 관련. 최신 버전으로 즉시 업데이트 권장. 악용 가능성 낮음.
11	Windows DHCP Server	CVE-2026-45602	변조	9.1	긴급	긴급 패치 권고	5093998, 5094041, 5094042, 5094122, 5094123, 5094125, 5094126, 5094127, 5094128, 5095051	**Windows 10(1607 등) 취약점(CVSS 9.1)** - 레거시 포함 다수 Windows 빌드에 영향. 신속 패치 권장. 악용 가능성 낮음.
12	Microsoft Exchange Online	CVE-2026-48579	정보 유출	9.1	긴급	긴급 패치 권고	정보 없음	**Microsoft Exchange Online 권한 상승(CVSS 9.1)** - 클라우드 서비스 측 취약점으로 Microsoft 가 서비스 측 조치. 테넌트 접근 로그 및 권한 부여 이벤트 감사 권장. 악용 가능성 낮음.

4. 일반 사용자 관련 전체 목록 (188 건)

연번	분류	CVE	영향	CVSS	위험등급	권장조치	KB ID	비고
1	원격 데스크톱 클라이언트	CVE-2026-42985	원격 코드 실행	8.8	**높음**	우선 패치 권고	5093998, 5094041, 5094042, 5094122, 5094123, 5094125, 5094126, 5094127, 5094128, 5095051	원격 코드 실행 / 악용 가능성 높음 / 우선 패치 권고
2	Microsoft Office SharePoint	CVE-2026-45484	권한 상승	8.8	**높음**	우선 패치 권고	5002873, 5002874, 5002880	권한 상승 / 악용 가능성 낮음 / 우선 패치 권고
3	원격 데스크톱 클라이언트	CVE-2026-47289	원격 코드 실행	8.8	**높음**	우선 패치 권고	5093998, 5094041, 5094042, 5094122, 5094123, 5094125, 5094126, 5094127, 5094128, 5095051	원격 코드 실행 / 악용 가능성 낮음 / 우선 패치 권고

4	원격 데스크톱 클라이언트	CVE-2026-47653	원격 코드 실행	8.8	**높음**	우선 패치 권고	5093998, 5094041, 5094042, 5094122, 5094123, 5094125, 5094126, 5094127, 5094128, 5095051	원격 코드 실행 / 악용 불가능 / 우선 패치 권고
5	Windows 암호화 서비스	CVE-2026-44810	권한 상승	8.4	**높음**	우선 패치 권고	5093998, 5094125, 5094126, 5094128, 5095051	권한 상승 / 악용 가능성 낮음 / 우선 패치 권고
6	Microsoft Office	CVE-2026-45456	원격 코드 실행	8.4	**높음**	우선 패치 권고	5002873, 5002874, 5002876, 5002879, 5002880, 5002881	원격 코드 실행 / 악용 가능성 낮음 / 우선 패치 권고
7	Microsoft Office	CVE-2026-45458	원격 코드 실행	8.4	**높음**	우선 패치 권고	5002873, 5002874, 5002876, 5002879, 5002880, 5002881	원격 코드 실행 / 악용 가능성 낮음 / 우선 패치 권고
8	Microsoft Office	CVE-2026-45461	원격 코드 실행	8.4	**높음**	우선 패치 권고	5002878	원격 코드 실행 / 악용 가능성 낮음 / 우선 패치 권고

9	Microsoft Office	CVE-2026-45463	원격 코드 실행	8.4	**높음**	우선 패치 권고	5002878	원격 코드 실행 / 악용 가능성 낮음 / 우선 패치 권고
10	Microsoft Office	CVE-2026-45472	원격 코드 실행	8.4	**높음**	우선 패치 권고	5002878	원격 코드 실행 / 악용 가능성 낮음 / 우선 패치 권고
11	Microsoft Office	CVE-2026-45474	원격 코드 실행	8.4	**높음**	우선 패치 권고	5002878	원격 코드 실행 / 악용 가능성 낮음 / 우선 패치 권고
12	Windows Hyper-V	CVE-2026-45607	원격 코드 실행	8.4	**높음**	우선 패치 권고	5093998, 5094122, 5094123, 5094125, 5094126, 5094127, 5094128, 5095051	원격 코드 실행 / 악용 가능성 낮음 / 우선 패치 권고
13	역할: Windows Hyper-V	CVE-2026-45641	원격 코드 실행	8.4	**높음**	우선 패치 권고	5093998, 5094125, 5094126, 5094127, 5094128, 5095051	원격 코드 실행 / 악용 가능성 낮음 / 우선 패치 권고
14	Microsoft Office	CVE-2026-47635	원격 코드 실행	8.4	**높음**	우선 패치 권고	-	원격 코드 실행 / 악용 가능성 낮음 / 우선 패치 권고

15	Microsoft Office Excel	CVE-2026-44822	정보 유출	8.2	**높음**	우선 패치 권고	5002875, 5002877	정보 유출 / 악용 불가능 / 우선 패치 권고
16	Linux MANA 드라이버	CVE-2026-45476	권한 상승	8.2	**높음**	우선 패치 권고	-	권한 상승 / 악용 가능성 낮음 / 우선 패치 권고
17	Windows Hyper-V	CVE-2026-47652	원격 코드 실행	8.2	**높음**	우선 패치 권고	5093998, 5094125, 5094126, 5094128, 5095051	원격 코드 실행 / 악용 가능성 낮음 / 우선 패치 권고
18	Android 용 Microsoft Teams	CVE-2026-42835	정보 유출	8.1	**높음**	우선 패치 권고	-	정보 유출 / 악용 가능성 낮음 / 우선 패치 권고
19	Windows 성능 모니터	CVE-2026-42974	원격 코드 실행	8.1	**높음**	우선 패치 권고	5093998, 5094125, 5094126, 5094128, 5095051	원격 코드 실행 / 악용 가능성 낮음 / 우선 패치 권고
20	Windows 성능 모니터	CVE-2026-42981	원격 코드 실행	8.1	**높음**	우선 패치 권고	5093998, 5094125, 5094126, 5094128, 5095051	원격 코드 실행 / 악용 가능성 낮음 / 우선 패치 권고

21	Universal Plug and Play(upnp.dll)	CVE-2026-45599	원격 코드 실행	8.1	**높음**	우선 패치 권고	5093998, 5094041, 5094042, 5094122, 5094123, 5094125, 5094126, 5094127, 5094128, 5095051	원격 코드 실행 / 악용 가능성 낮음 / 우선 패치 권고
22	Universal Plug and Play(upnp.dll)	CVE-2026-45635	원격 코드 실행	8.1	**높음**	우선 패치 권고	5093998, 5094041, 5094042, 5094122, 5094123, 5094125, 5094126, 5094127, 5094128, 5095051	원격 코드 실행 / 악용 가능성 낮음 / 우선 패치 권고
23	Microsoft Live Share Canvas SDK	CVE-2026-45644	권한 상승	8.0	**높음**	우선 패치 권고	-	권한 상승 / 악용 가능성 낮음 / 우선 패치 권고
24	Microsoft Office SharePoint	CVE-2026-47298	원격 코드 실행	8.0	**높음**	우선 패치 권고	5002873, 5002874, 5002880	원격 코드 실행 / 악용 가능성 높음 / 우선 패치 권고

25	Windows 보안 부팅	CVE-2026-45588	보안 기능 우회	7.9	**높음**	우선 패치 권고	5093998, 5094041, 5094042, 5094122, 5094123, 5094125, 5094126, 5094127, 5094128, 5095051	보안 기능 우회 / 악용 가능성 낮음 / 우선 패치 권고
26	Windows 보안 부팅	CVE-2026-45654	보안 기능 우회	7.9	**높음**	우선 패치 권고	5094125, 5094126, 5095051	보안 기능 우회 / 악용 가능성 낮음 / 우선 패치 권고
27	Windows 부팅 관리자	CVE-2026-47656	보안 기능 우회	7.9	**높음**	우선 패치 권고	5093998, 5094041, 5094042, 5094122, 5094123, 5094125, 5094126, 5094127, 5094128, 5095051	보안 기능 우회 / 악용 가능성 낮음 / 우선 패치 권고
28	Windows 보안 부팅	CVE-2026-48568	보안 기능 우회	7.9	**높음**	우선 패치 권고	5093998, 5094041, 5094042, 5094122, 5094123, 5094125, 5094126, 5094127, 5094128, 5095051	보안 기능 우회 / 악용 가능성 낮음 / 우선 패치 권고

29	Windows 보안 부팅	CVE-2026-48570	보안 기능 우회	7.9	**높음**	우선 패치 권고	5093998, 5094041, 5094042, 5094122, 5094123, 5094125, 5094126, 5094127, 5094128, 5095051	보안 기능 우회 / 악용 가능성 낮음 / 우선 패치 권고
30	Windows 보안 부팅	CVE-2026-48573	보안 기능 우회	7.9	**높음**	우선 패치 권고	5093998, 5094041, 5094042, 5094122, 5094123, 5094125, 5094126, 5094127, 5094128, 5095051	보안 기능 우회 / 악용 가능성 낮음 / 우선 패치 권고
31	Windows 보안 부팅	CVE-2026-48575	보안 기능 우회	7.9	**높음**	우선 패치 권고	5093998, 5094041, 5094042, 5094122, 5094123, 5094125, 5094126, 5094127, 5094128, 5095051	보안 기능 우회 / 악용 가능성 낮음 / 우선 패치 권고

32	Windows 보안 부팅	CVE-2026-48576	보안 기능 우회	7.9	**높음**	우선 패치 권고	5093998, 5094041, 5094042, 5094122, 5094123, 5094125, 5094126, 5094127, 5094128, 5095051	보안 기능 우회 / 악용 가능성 낮음 / 우선 패치 권고
33	Windows 보안 부팅	CVE-2026-48578	권한 상승	7.9	**높음**	우선 패치 권고	5093998, 5094041, 5094042, 5094122, 5094123, 5094125, 5094126, 5094127, 5094128, 5095051	권한 상승 / 악용 가능성 낮음 / 우선 패치 권고
34	Windows 범용 디스크 형식 파일 시스템 드라이버(UDFS)	CVE-2026-40404	권한 상승	7.8	**높음**	우선 패치 권고	5093998, 5094041, 5094042, 5094122, 5094123, 5094125, 5094126, 5094127, 5094128, 5095051	권한 상승 / 악용 가능성 낮음 / 우선 패치 권고

35	Windows 범용 디스크 형식 파일 시스템 드라이버(UDFS)	CVE-2026-40409	권한 상승	7.8	**높음**	우선 패치 권고	5093998, 5094041, 5094042, 5094122, 5094123, 5094125, 5094126, 5094127, 5094128, 5095051	권한 상승 / 악용 가능성 낮음 / 우선 패치 권고
36	Microsoft Kinect	CVE-2026-41092	권한 상승	7.8	**높음**	우선 패치 권고	5093998, 5094041, 5094042, 5094122, 5094123, 5094125, 5094126, 5094127, 5094128, 5095051	권한 상승 / 악용 가능성 낮음 / 우선 패치 권고
37	Windows 예상 파일 시스템 필터 드라이버	CVE-2026-42828	권한 상승	7.8	**높음**	우선 패치 권고	5093998, 5094123, 5094125, 5094126, 5094127, 5094128, 5095051	권한 상승 / 악용 가능성 낮음 / 우선 패치 권고
38	Windows 관리자 보호	CVE-2026-42829	보안 기능 우회	7.8	**높음**	우선 패치 권고	5094126, 5095051	보안 기능 우회 / 악용 가능성 낮음 / 우선 패치 권고

39	Windows 예상 파일 시스템 필터 드라이버	CVE-2026-42837	권한 상승	7.8	**높음**	우선 패치 권고	5093998, 5094123, 5094125, 5094126, 5094127, 5094128, 5095051	권한 상승 / 악용 가능성 낮음 / 우선 패치 권고
40	Microsoft PowerToys	CVE-2026-42902	권한 상승	7.8	**높음**	우선 패치 권고	-	권한 상승 / 악용 가능성 낮음 / 우선 패치 권고
41	Windows DWM 핵심 라이브러리	CVE-2026-42905	권한 상승	7.8	**높음**	우선 패치 권고	5093998, 5094041, 5094042, 5094122, 5094123, 5094125, 5094126, 5094127, 5094128, 5095051	권한 상승 / 악용 가능성 높음 / 우선 패치 권고
42	Windows 핫패치 모니터링 서비스	CVE-2026-42910	권한 상승	7.8	**높음**	우선 패치 권고	5094125, 5094126, 5095051	권한 상승 / 악용 가능성 낮음 / 우선 패치 권고
43	Windows NT OS 커널	CVE-2026-42916	권한 상승	7.8	**높음**	우선 패치 권고	5093998, 5094041, 5094042, 5094122, 5094123, 5094125, 5094126, 5094127, 5094128, 5095051	권한 상승 / 악용 가능성 낮음 / 우선 패치 권고

44	Windows 푸시 알림	CVE-2026-42977	권한 상승	7.8	**높음**	우선 패치 권고	5093998, 5094123, 5094125, 5094126, 5094127, 5094128, 5095051	권한 상승 / 악용 불가능 / 우선 패치 권고
45	Windows 푸시 알림	CVE-2026-42978	권한 상승	7.8	**높음**	우선 패치 권고	5093998, 5094123, 5094125, 5094126, 5094127, 5094128, 5095051	권한 상승 / 악용 불가능 / 우선 패치 권고
46	Windows 푸시 알림	CVE-2026-42979	권한 상승	7.8	**높음**	우선 패치 권고	5093998, 5094123, 5094125, 5094126, 5094127, 5094128, 5095051	권한 상승 / 악용 불가능 / 우선 패치 권고
47	Windows NT OS 커널	CVE-2026-42980	권한 상승	7.8	**높음**	우선 패치 권고	5093998, 5094041, 5094042, 5094122, 5094123, 5094125, 5094126, 5094127, 5094128, 5095051	권한 상승 / 악용 가능성 높음 / 우선 패치 권고

48	Windows DWM 핵심 라이브러리	CVE-2026-42983	권한 상승	7.8	**높음**	우선 패치 권고	5093998, 5094123, 5094125, 5094126, 5094127, 5094128, 5095051	권한 상승 / 악용 가능성 낮음 / 우선 패치 권고
49	Microsoft 그래픽 구성 요소	CVE-2026-42986	권한 상승	7.8	**높음**	우선 패치 권고	5093998, 5094041, 5094042, 5094122, 5094123, 5094125, 5094126, 5094127, 5094128, 5095051	권한 상승 / 악용 가능성 높음 / 우선 패치 권고
50	Winlogon	CVE-2026-42989	권한 상승	7.8	**높음**	우선 패치 권고	5093998, 5094041, 5094042, 5094122, 5094123, 5094125, 5094126, 5094127, 5094128, 5095051	권한 상승 / 악용 가능성 높음 / 우선 패치 권고
51	Windows 푸시 알림	CVE-2026-42991	권한 상승	7.8	**높음**	우선 패치 권고	5093998, 5094123, 5094125, 5094126, 5094127, 5094128, 5095051	권한 상승 / 악용 불가능 / 우선 패치 권고

52	Windows DWM 핵심 라이브러리	CVE-2026-44802	권한 상승	7.8	**높음**	우선 패치 권고	5093998, 5094123, 5094125, 5094126, 5094127, 5094128, 5095051	권한 상승 / 악용 가능성 낮음 / 우선 패치 권고
53	Windows Win32K - GRFX	CVE-2026-44803	원격 코드 실행	7.8	**높음**	우선 패치 권고	5093998, 5094041, 5094042, 5094122, 5094123, 5094125, 5094126, 5094127, 5094128, 5095051	원격 코드 실행 / 악용 가능성 높음 / 우선 패치 권고
54	Windows DWM 핵심 라이브러리	CVE-2026-44804	권한 상승	7.8	**높음**	우선 패치 권고	5095051	권한 상승 / 악용 가능성 낮음 / 우선 패치 권고
55	Windows DWM 핵심 라이브러리	CVE-2026-44807	권한 상승	7.8	**높음**	우선 패치 권고	5095051	권한 상승 / 악용 가능성 낮음 / 우선 패치 권고
56	Windows DWM 핵심 라이브러리	CVE-2026-44808	권한 상승	7.8	**높음**	우선 패치 권고	5095051	권한 상승 / 악용 가능성 낮음 / 우선 패치 권고
57	Windows 공용 로그 파일 시스템 드라이버	CVE-2026-44809	권한 상승	7.8	**높음**	우선 패치 권고	5094125, 5094126, 5095051	권한 상승 / 악용 불가능 / 우선 패치 권고

58	Windows DWM 핵심 라이브러리	CVE-2026-44811	권한 상승	7.8	**높음**	우선 패치 권고	5095051	권한 상승 / 악용 가능성 낮음 / 우선 패치 권고
59	Windows Win32K - GRFX	CVE-2026-44812	원격 코드 실행	7.8	**높음**	우선 패치 권고	5093998, 5094041, 5094042, 5094122, 5094123, 5094125, 5094126, 5094127, 5094128, 5095051	원격 코드 실행 / 악용 가능성 높음 / 우선 패치 권고
60	Windows DWM 핵심 라이브러리	CVE-2026-44813	권한 상승	7.8	**높음**	우선 패치 권고	5095051	권한 상승 / 악용 가능성 낮음 / 우선 패치 권고
61	Microsoft Office Excel	CVE-2026-44817	원격 코드 실행	7.8	**높음**	우선 패치 권고	5002875, 5002877	원격 코드 실행 / 악용 불가능 / 우선 패치 권고
62	Microsoft Office Word	CVE-2026-44819	원격 코드 실행	7.8	**높음**	우선 패치 권고	5002873, 5002874, 5002876, 5002878, 5002880, 5002881	원격 코드 실행 / 악용 가능성 낮음 / 우선 패치 권고
63	Microsoft Office Excel	CVE-2026-44820	원격 코드 실행	7.8	**높음**	우선 패치 권고	5002875, 5002877	원격 코드 실행 / 악용 가능성 낮음 / 우선 패치 권고

64	Microsoft Office Excel	CVE-2026-44823	원격 코드 실행	7.8	**높음**	우선 패치 권고	5002875, 5002877	원격 코드 실행 / 악용 가능성 낮음 / 우선 패치 권고
65	Microsoft Office Word	CVE-2026-44824	원격 코드 실행	7.8	**높음**	우선 패치 권고	5002873, 5002874, 5002876, 5002878, 5002880, 5002881	원격 코드 실행 / 악용 가능성 낮음 / 우선 패치 권고
66	Microsoft Office Word	CVE-2026-45457	원격 코드 실행	7.8	**높음**	우선 패치 권고	-	원격 코드 실행 / 악용 가능성 낮음 / 우선 패치 권고
67	Microsoft Office Excel	CVE-2026-45469	원격 코드 실행	7.8	**높음**	우선 패치 권고	5002875, 5002877	원격 코드 실행 / 악용 가능성 낮음 / 우선 패치 권고
68	Microsoft Office Word	CVE-2026-45471	원격 코드 실행	7.8	**높음**	우선 패치 권고	5002873, 5002874, 5002876, 5002879, 5002880, 5002881	원격 코드 실행 / 악용 가능성 낮음 / 우선 패치 권고
69	Microsoft Office Word	CVE-2026-45475	원격 코드 실행	7.8	**높음**	우선 패치 권고	5002873, 5002874, 5002876, 5002878, 5002880, 5002881	원격 코드 실행 / 악용 가능성 낮음 / 우선 패치 권고

70	Microsoft Office Word	CVE-2026-45486	원격 코드 실행	7.8	**높음**	우선 패치 권고	-	원격 코드 실행 / 악용 가능성 낮음 / 우선 패치 권고
71	Windows 프로그램 호환성 관리자 서비스	CVE-2026-45487	권한 상승	7.8	**높음**	우선 패치 권고	5093998, 5094125, 5094126, 5094127, 5094128, 5095051	권한 상승 / 악용 불가능 / 우선 패치 권고
72	.NET	CVE-2026-45490	권한 상승	7.8	**높음**	우선 패치 권고	5097148, 5097149, 5097150	권한 상승 / 악용 가능성 낮음 / 우선 패치 권고
73	Windows Collaborative Translation Framework	CVE-2026-45586	권한 상승	7.8	**높음**	우선 패치 권고	5093998, 5094041, 5094042, 5094122, 5094123, 5094125, 5094126, 5094127, 5094128, 5095051	권한 상승 / 악용 가능성 높음 / 우선 패치 권고
74	Windows 인터넷(wininet.dll)	CVE-2026-45592	권한 상승	7.8	**높음**	우선 패치 권고	5093998, 5094006, 5094041, 5094122, 5094123, 5094125, 5094126, 5094127, 5094128, 5095051	권한 상승 / 악용 불가능 / 우선 패치 권고

75	Windows SDK	CVE-2026-45593	권한 상승	7.8	**높음**	우선 패치 권고	5093998, 5094123, 5094125, 5094126, 5094127, 5094128, 5095051	권한 상승 / 악용 가능성 낮음 / 우선 패치 권고
76	Windows 커널 모드 드라이버	CVE-2026-45600	권한 상승	7.8	**높음**	우선 패치 권고	5094125, 5094126, 5095051	권한 상승 / 악용 불가능 / 우선 패치 권고
77	Windows Bluetooth 서비스	CVE-2026-45605	권한 상승	7.8	**높음**	우선 패치 권고	5093998, 5094122, 5094123, 5094125, 5094126, 5094127, 5094128, 5095051	권한 상승 / 악용 가능성 낮음 / 우선 패치 권고
78	Windows NTFS	CVE-2026-45636	원격 코드 실행	7.8	**높음**	우선 패치 권고	5093998, 5094041, 5094042, 5094122, 5094123, 5094125, 5094126, 5094127, 5094128, 5095051	원격 코드 실행 / 악용 가능성 낮음 / 우선 패치 권고

79	Windows DWM 핵심 라이브러리	CVE-2026-45637	권한 상승	7.8	**높음**	우선 패치 권고	5093998, 5094123, 5094125, 5094126, 5094127, 5094128, 5095051	권한 상승 / 악용 가능성 낮음 / 우선 패치 권고
80	WinSock 용 Windows 보조 기능 드라이버	CVE-2026-45638	권한 상승	7.8	**높음**	우선 패치 권고	5093998, 5094041, 5094042, 5094122, 5094123, 5094125, 5094126, 5094127, 5094128, 5095051	권한 상승 / 악용 가능성 낮음 / 우선 패치 권고
81	Microsoft Office Word	CVE-2026-45643	원격 코드 실행	7.8	**높음**	우선 패치 권고	-	원격 코드 실행 / 악용 가능성 낮음 / 우선 패치 권고
82	Microsoft Office	CVE-2026-45645	원격 코드 실행	7.8	**높음**	우선 패치 권고	5002852	원격 코드 실행 / 악용 가능성 낮음 / 우선 패치 권고

83	Windows UEFI	CVE-2026-45656	보안 기능 우회	7.8	**높음**	우선 패치 권고	5093998, 5094041, 5094042, 5094122, 5094123, 5094125, 5094126, 5094127, 5094128, 5095051	보안 기능 우회 / 악용 가능성 낮음 / 우선 패치 권고
84	Windows BitLocker	CVE-2026-45658	보안 기능 우회	7.8	**높음**	우선 패치 권고	5093998, 5094041, 5094042, 5094122, 5094123, 5094125, 5094126, 5094127, 5094128, 5095051	보안 기능 우회 / 악용 가능성 높음 / 우선 패치 권고
85	Visual Studio Code	CVE-2026-47292	권한 상승	7.8	**높음**	우선 패치 권고	-	권한 상승 / 악용 가능성 낮음 / 우선 패치 권고
86	Windows Narrator Braille	CVE-2026-48565	권한 상승	7.8	**높음**	우선 패치 권고	-	권한 상승 / 악용 가능성 낮음 / 우선 패치 권고

87	Windows Media	CVE-2026-48574	원격 코드 실행	7.8	**높음**	우선 패치 권고	5093998, 5094041, 5094042, 5094122, 5094123, 5094125, 5094126, 5094127, 5094128, 5095051	원격 코드 실행 / 악용 가능성 낮음 / 우선 패치 권고
88	Windows 커널	CVE-2026-48583	권한 상승	7.8	**높음**	우선 패치 권고	5093998, 5094122, 5094123, 5094125, 5094126, 5094127, 5094128, 5095051	권한 상승 / 악용 가능성 낮음 / 우선 패치 권고
89	Visual Studio Code	CVE-2026-40376	권한 상승	7.5	**높음**	우선 패치 권고	-	권한 상승 / 악용 가능성 낮음 / 우선 패치 권고
90	Windows RDP	CVE-2026-42908	정보 유출	7.5	**높음**	우선 패치 권고	5093998, 5094041, 5094042, 5094122, 5094123, 5094125, 5094126, 5094127, 5094128, 5095051	정보 유출 / 악용 가능성 낮음 / 우선 패치 권고

91	원격 데스크톱 클라이언트	CVE-2026-42909	원격 코드 실행	7.5	**높음**	우선 패치 권고	5093998, 5094041, 5094042, 5094122, 5094123, 5094125, 5094126, 5094127, 5094128, 5095051	원격 코드 실행 / 악용 불가능 / 우선 패치 권고
92	원격 데스크톱 클라이언트	CVE-2026-42913	원격 코드 실행	7.5	**높음**	우선 패치 권고	5093998, 5094125, 5094126, 5094128, 5095051	원격 코드 실행 / 악용 불가능 / 우선 패치 권고
93	원격 데스크톱 클라이언트	CVE-2026-42992	원격 코드 실행	7.5	**높음**	우선 패치 권고	5093998, 5094122, 5094123, 5094125, 5094126, 5094127, 5094128, 5095051	원격 코드 실행 / 악용 가능성 낮음 / 우선 패치 권고
94	원격 데스크톱 클라이언트	CVE-2026-42993	원격 코드 실행	7.5	**높음**	우선 패치 권고	5093998, 5094125, 5094126, 5094127, 5094128, 5095051	원격 코드 실행 / 악용 가능성 낮음 / 우선 패치 권고

95	원격 데스크톱 클라이언트	CVE-2026-44799	원격 코드 실행	7.5	**높음**	우선 패치 권고	5093998, 5094041, 5094042, 5094122, 5094123, 5094125, 5094126, 5094127, 5094128, 5095051	원격 코드 실행 / 악용 가능성 낮음 / 우선 패치 권고
96	원격 데스크톱 클라이언트	CVE-2026-44801	원격 코드 실행	7.5	**높음**	우선 패치 권고	5093998, 5094041, 5094042, 5094122, 5094123, 5094125, 5094126, 5094127, 5094128, 5095051	원격 코드 실행 / 악용 가능성 낮음 / 우선 패치 권고
97	ASP.NET Core	CVE-2026-45591	서비스 거부	7.5	**높음**	우선 패치 권고	5097148, 5097149, 5097150	서비스 거부 / 악용 가능성 낮음 / 우선 패치 권고
98	Windows RDP	CVE-2026-45639	정보 유출	7.5	**높음**	우선 패치 권고	5093998, 5094041, 5094042, 5094122, 5094123, 5094125, 5094126, 5094127, 5094128, 5095051	정보 유출 / 악용 가능성 낮음 / 우선 패치 권고

99	원격 데스크톱 클라이언트	CVE-2026-48563	원격 코드 실행	7.5	**높음**	우선 패치 권고	5093998, 5094123, 5094125, 5094126, 5094127, 5094128, 5095051	원격 코드 실행 / 악용 가능성 낮음 / 우선 패치 권고
100	HTTP/2	CVE-2026-49160	서비스 거부	7.5	**높음**	우선 패치 권고	5093998, 5094122, 5094123, 5094125, 5094126, 5094127, 5094128, 5095051	서비스 거부 / 악용 가능성 높음 / 우선 패치 권고
101	Microsoft Office SharePoint	CVE-2026-45481	스푸핑	7.3	**높음**	우선 패치 권고	5002873, 5002874, 5002880	스푸핑 / 악용 가능성 높음 / 우선 패치 권고
102	Microsoft Office SharePoint	CVE-2026-47634	스푸핑	7.3	**높음**	우선 패치 권고	5002873, 5002874	스푸핑 / 악용 가능성 높음 / 우선 패치 권고
103	Android 용 Office	CVE-2026-45649	스푸핑	7.1	**높음**	우선 패치 권고	-	스푸핑 / 악용 불가능 / 우선 패치 권고
104	Visual Studio Code	CVE-2026-48569	보안 기능 우회	7.1	**높음**	우선 패치 권고	-	보안 기능 우회 / 악용 가능성 낮음 / 우선 패치 권고

105	WinSock 용 Windows 보조 기능 드라이버	CVE-2026-34335	권한 상승	7.0	**높음**	우선 패치 권고	5093998, 5094041, 5094042, 5094122, 5094123, 5094125, 5094126, 5094127, 5094128, 5095051	권한 상승 / 악용 불가능 / 우선 패치 권고
106	함수 검색 서비스(fdwsd.dll)	CVE-2026-42836	권한 상승	7.0	**높음**	우선 패치 권고	5093998, 5094041, 5094042, 5094122, 5094123, 5094125, 5094126, 5094127, 5094128, 5095051	권한 상승 / 악용 가능성 낮음 / 우선 패치 권고
107	WinSock 용 Windows 보조 기능 드라이버	CVE-2026-42911	권한 상승	7.0	**높음**	우선 패치 권고	5093998, 5094041, 5094042, 5094122, 5094123, 5094125, 5094126, 5094127, 5094128, 5095051	권한 상승 / 악용 가능성 낮음 / 우선 패치 권고

108	Windows 전화 통신 서비스	CVE-2026-42912	권한 상승	7.0	**높음**	우선 패치 권고	5093998, 5094041, 5094042, 5094122, 5094123, 5094125, 5094126, 5094127, 5094128, 5095051	권한 상승 / 악용 가능성 낮음 / 우선 패치 권고
109	Windows 커널	CVE-2026-42984	권한 상승	7.0	**높음**	우선 패치 권고	5093998, 5094123, 5094125, 5094126, 5094127, 5094128, 5095051	권한 상승 / 악용 불가능 / 우선 패치 권고
110	Microsoft Office Excel	CVE-2026-44818	원격 코드 실행	7.0	**높음**	우선 패치 권고	5002875, 5002877	원격 코드 실행 / 악용 가능성 낮음 / 우선 패치 권고
111	WinSock 용 Windows 보조 기능 드라이버	CVE-2026-45596	권한 상승	7.0	**높음**	우선 패치 권고	5093998, 5094041, 5094042, 5094122, 5094123, 5094125, 5094126, 5094127, 5094128, 5095051	권한 상승 / 악용 가능성 낮음 / 우선 패치 권고

112	UI 자동화 관리자(uiamanager.dll)	CVE-2026-45597	권한 상승	7.0	**높음**	우선 패치 권고	5093998, 5094125, 5094126, 5094128, 5095051	권한 상승 / 악용 가능성 낮음 / 우선 패치 권고
113	WinSock 용 Windows 보조 기능 드라이버	CVE-2026-45598	권한 상승	7.0	**높음**	우선 패치 권고	5093998, 5094041, 5094042, 5094122, 5094123, 5094125, 5094126, 5094127, 5094128, 5095051	권한 상승 / 악용 가능성 낮음 / 우선 패치 권고
114	WinSock 용 Windows 보조 기능 드라이버	CVE-2026-45601	권한 상승	7.0	**높음**	우선 패치 권고	5093998, 5094041, 5094042, 5094122, 5094123, 5094125, 5094126, 5094127, 5094128, 5095051	권한 상승 / 악용 가능성 낮음 / 우선 패치 권고
115	WinSock 용 Windows 보조 기능 드라이버	CVE-2026-45603	권한 상승	7.0	**높음**	우선 패치 권고	5093998, 5094041, 5094042, 5094122, 5094123, 5094125, 5094126, 5094127, 5094128, 5095051	권한 상승 / 악용 가능성 낮음 / 우선 패치 권고

116	Windows Bluetooth 포트 드라이버	CVE-2026-45640	권한 상승	7.0	**높음**	우선 패치 권고	5093998, 5094125, 5094126, 5094127, 5094128, 5095051	권한 상승 / 악용 가능성 낮음 / 우선 패치 권고
117	Windows 커널	CVE-2026-45653	권한 상승	7.0	**높음**	우선 패치 권고	5093998, 5094041, 5094042, 5094122, 5094123, 5094125, 5094126, 5094127, 5094128, 5095051	권한 상승 / 악용 불가능 / 우선 패치 권고
118	Microsoft Office 간편 실행	CVE-2026-47293	권한 상승	7.0	**높음**	우선 패치 권고	-	권한 상승 / 악용 가능성 낮음 / 우선 패치 권고
119	Windows 저장소	CVE-2026-47648	권한 상승	7.0	**높음**	우선 패치 권고	5093998, 5094041, 5094042, 5094122, 5094123, 5094125, 5094126, 5094127, 5094128, 5095051	권한 상승 / 악용 불가능 / 우선 패치 권고

120	Windows DHCP 클라이언트	CVE-2026-45608	정보 유출	6.8	**보통**	조기 패치 권고	5093998, 5094041, 5094042, 5094122, 5094123, 5094125, 5094126, 5094127, 5094128, 5095051	정보 유출 / 악용 불가능 / 조기 패치 권고
121	Windows Kerberos	CVE-2026-42903	서비스 거부	6.5	**보통**	조기 패치 권고	5093998, 5094041, 5094042, 5094122, 5094123, 5094125, 5094126, 5094127, 5094128, 5095051	서비스 거부 / 악용 불가능 / 조기 패치 권고
122	Windows Shell	CVE-2026-42907	정보 유출	6.5	**보통**	조기 패치 권고	5093998, 5094123, 5094125, 5094126, 5094127, 5094128, 5095051	정보 유출 / 악용 가능성 낮음 / 조기 패치 권고
123	Microsoft Office SharePoint	CVE-2026-45454	원격 코드 실행	6.5	**보통**	조기 패치 권고	5002873, 5002874, 5002880	원격 코드 실행 / 악용 가능성 낮음 / 조기 패치 권고

124	Visual Studio Code	CVE-2026-47284	정보 유출	6.5	**보통**	조기 패치 권고	-	정보 유출 / 악용 가능성 낮음 / 조기 패치 권고
125	Visual Studio Code	CVE-2026-47287	변조	6.5	**보통**	조기 패치 권고	-	변조 / 악용 가능성 낮음 / 조기 패치 권고
126	.NET	CVE-2026-45491	변조	6.2	**보통**	조기 패치 권고	5097148, 5097149, 5097150	변조 / 악용 불가능 / 조기 패치 권고
127	Windows TCP/IP	CVE-2026-42915	서비스 거부	5.7	**보통**	조기 패치 권고	5093998, 5094125, 5094126, 5094127, 5094128, 5095051	서비스 거부 / 악용 가능성 낮음 / 조기 패치 권고
128	Windows Shell	CVE-2026-42906	정보 유출	5.5	**보통**	조기 패치 권고	5093998, 5094125, 5094126, 5094127, 5094128, 5095051	정보 유출 / 악용 가능성 낮음 / 조기 패치 권고
129	Windows 전화 통신 서비스	CVE-2026-42968	정보 유출	5.5	**보통**	조기 패치 권고	5093998, 5094041, 5094042, 5094122, 5094123, 5094125, 5094126, 5094127, 5094128, 5095051	정보 유출 / 악용 가능성 낮음 / 조기 패치 권고

130	Windows 푸시 알림	CVE-2026-42969	정보 유출	5.5	**보통**	조기 패치 권고	5093998, 5094122, 5094123, 5094125, 5094126, 5094127, 5094128, 5095051	정보 유출 / 악용 불가능 / 조기 패치 권고
131	Windows 푸시 알림	CVE-2026-42970	정보 유출	5.5	**보통**	조기 패치 권고	5093998, 5094041, 5094042, 5094122, 5094123, 5094125, 5094126, 5094127, 5094128, 5095051	정보 유출 / 악용 가능성 낮음 / 조기 패치 권고
132	Windows 푸시 알림	CVE-2026-42971	정보 유출	5.5	**보통**	조기 패치 권고	5093998, 5094122, 5094123, 5094125, 5094126, 5094127, 5094128, 5095051	정보 유출 / 악용 가능성 낮음 / 조기 패치 권고

133	역할: Windows Hyper-V	CVE-2026-42972	정보 유출	5.5	**보통**	조기 패치 권고	5093998, 5094041, 5094042, 5094122, 5094123, 5094125, 5094126, 5094127, 5094128, 5095051	정보 유출 / 악용 가능성 낮음 / 조기 패치 권고
134	Windows 푸시 알림	CVE-2026-42973	정보 유출	5.5	**보통**	조기 패치 권고	5093998, 5094122, 5094123, 5094125, 5094126, 5094127, 5094128, 5095051	정보 유출 / 악용 가능성 낮음 / 조기 패치 권고
135	Windows DWM 핵심 라이브러리	CVE-2026-44814	정보 유출	5.5	**보통**	조기 패치 권고	5095051	정보 유출 / 악용 가능성 낮음 / 조기 패치 권고
136	Microsoft Office Word	CVE-2026-44821	정보 유출	5.5	**보통**	조기 패치 권고	5002873, 5002874, 5002876, 5002878, 5002880, 5002881	정보 유출 / 악용 가능성 낮음 / 조기 패치 권고

137	Windows 애플리케이션 ID(AppID) 하위 시스템	CVE-2026-45594	정보 유출	5.5	**보통**	조기 패치 권고	5093998, 5094122, 5094123, 5094125, 5094126, 5094127, 5094128, 5095051	정보 유출 / 악용 가능성 낮음 / 조기 패치 권고
138	Windows 애플리케이션 ID(AppID) 하위 시스템	CVE-2026-45604	정보 유출	5.5	**보통**	조기 패치 권고	5093998, 5094125, 5094126, 5095051	정보 유출 / 악용 가능성 낮음 / 조기 패치 권고
139	Microsoft UxTheme 라이브러리(uxtheme.dll)	CVE-2026-45606	서비스 거부	5.5	**보통**	조기 패치 권고	5093998, 5094041, 5094042, 5094122, 5094123, 5094125, 5094126, 5094127, 5094128, 5095051	서비스 거부 / 악용 가능성 낮음 / 조기 패치 권고
140	Windows DWM 핵심 라이브러리	CVE-2026-48566	정보 유출	5.5	**보통**	조기 패치 권고	5087423, 5087539, 5089466, 5089548, 5089549	정보 유출 / 악용 가능성 낮음 / 조기 패치 권고
141	Microsoft Office SharePoint	CVE-2026-33113	스푸핑	5.4	**보통**	조기 패치 권고	5002873, 5002874, 5002880	스푸핑 / 악용 가능성 낮음 / 조기 패치 권고

142	Microsoft Office SharePoint	CVE-2026-45453	스푸핑	5.4	**보통**	조기 패치 권고	5002873, 5002874, 5002880	스푸핑 / 악용 가능성 낮음 / 조기 패치 권고
143	Microsoft Office SharePoint	CVE-2026-45464	스푸핑	5.4	**보통**	조기 패치 권고	5002873, 5002874, 5002880	스푸핑 / 악용 가능성 낮음 / 조기 패치 권고
144	Microsoft Office SharePoint	CVE-2026-45465	스푸핑	5.4	**보통**	조기 패치 권고	5002873, 5002874, 5002880	스푸핑 / 악용 가능성 낮음 / 조기 패치 권고
145	Windows MOTW(Mark of the Web)	CVE-2026-45595	보안 기능 우회	5.4	**보통**	조기 패치 권고	5093998, 5094041, 5094122, 5094123, 5094125, 5094126, 5094127, 5094128, 5095051	보안 기능 우회 / 악용 가능성 낮음 / 조기 패치 권고
146	Microsoft Office SharePoint	CVE-2026-47636	스푸핑	5.4	**보통**	조기 패치 권고	5002873, 5002874, 5002880	스푸핑 / 악용 가능성 낮음 / 조기 패치 권고
147	Microsoft Office SharePoint	CVE-2026-47639	스푸핑	5.4	**보통**	조기 패치 권고	5002873, 5002874, 5002880	스푸핑 / 악용 불가능 / 조기 패치 권고
148	Microsoft Office SharePoint	CVE-2026-48560	스푸핑	5.4	**보통**	조기 패치 권고	5002873, 5002874, 5002880	스푸핑 / 악용 가능성 낮음 / 조기 패치 권고

149	Windows Kerberos	CVE-2026-42914	서비스 거부	5.3	**보통**	조기 패치 권고	5093998, 5094041, 5094042, 5094122, 5094123, 5094125, 5094126, 5094127, 5094128, 5095051	서비스 거부 / 악용 가능성 낮음 / 조기 패치 권고
150	Windows BitLocker	CVE-2026-45655	보안 기능 우회	5.3	**보통**	조기 패치 권고	5093998, 5094041, 5094042, 5094122, 5094123, 5094125, 5094126, 5094127, 5094128, 5095051	보안 기능 우회 / 악용 가능성 낮음 / 조기 패치 권고
151	Microsoft Office	CVE-2026-45460	정보 유출	4.7	**보통**	조기 패치 권고	-	정보 유출 / 악용 불가능 / 조기 패치 권고
152	Microsoft Office SharePoint	CVE-2026-45462	스푸핑	4.6	**보통**	조기 패치 권고	5002873, 5002874, 5002880	스푸핑 / 악용 가능성 낮음 / 조기 패치 권고
153	Microsoft Office SharePoint	CVE-2026-45467	스푸핑	4.6	**보통**	조기 패치 권고	5002873, 5002874, 5002880	스푸핑 / 악용 가능성 낮음 / 조기 패치 권고

154	Microsoft Office SharePoint	CVE-2026-45468	스푸핑	4.6	**보통**	조기 패치 권고	5002873, 5002874, 5002880	스푸핑 / 악용 가능성 낮음 / 조기 패치 권고
155	Microsoft Office SharePoint	CVE-2026-45479	스푸핑	4.6	**보통**	조기 패치 권고	5002873, 5002874, 5002880	스푸핑 / 악용 가능성 낮음 / 조기 패치 권고
156	Microsoft Office Project	CVE-2026-45483	스푸핑	4.6	**보통**	조기 패치 권고	5002873, 5002874, 5002880	스푸핑 / 악용 가능성 낮음 / 조기 패치 권고
157	Microsoft Office SharePoint	CVE-2026-47637	스푸핑	4.6	**보통**	조기 패치 권고	5002873, 5002874, 5002880	스푸핑 / 악용 가능성 낮음 / 조기 패치 권고
158	Microsoft Office SharePoint	CVE-2026-47638	스푸핑	4.6	**보통**	조기 패치 권고	5002873, 5002874, 5002880	스푸핑 / 악용 가능성 낮음 / 조기 패치 권고
159	Microsoft Office SharePoint	CVE-2026-47640	스푸핑	4.6	**보통**	조기 패치 권고	5002873, 5002874, 5002880	스푸핑 / 악용 불가능 / 조기 패치 권고
160	Microsoft Office SharePoint	CVE-2026-47641	스푸핑	4.6	**보통**	조기 패치 권고	5002873, 5002874, 5002880	스푸핑 / 악용 가능성 낮음 / 조기 패치 권고
161	Microsoft Office SharePoint	CVE-2026-48562	스푸핑	4.6	**보통**	조기 패치 권고	5002873, 5002874, 5002880	스푸핑 / 악용 가능성 낮음 / 조기 패치 권고

162	Microsoft Office Excel	CVE-2026-45455	정보 유출	3.3	**낮음**	정기 업데이트 시 적용	5002875, 5002877	정보 유출 / 악용 가능성 낮음 / 정기 업데이트 시 적용
163	Microsoft Office Excel	CVE-2026-45459	보안 기능 우회	3.3	**낮음**	정기 업데이트 시 적용	-	보안 기능 우회 / 악용 가능성 낮음 / 정기 업데이트 시 적용
164	Microsoft Office Word	CVE-2026-45466	정보 유출	3.3	**낮음**	정기 업데이트 시 적용	-	정보 유출 / 악용 불가능 / 정기 업데이트 시 적용
165	Microsoft Office Word	CVE-2026-45485	정보 유출	3.3	**낮음**	정기 업데이트 시 적용	5002873, 5002874, 5002876, 5002878, 5002880, 5002881	정보 유출 / 악용 가능성 낮음 / 정기 업데이트 시 적용
166	Microsoft Power Pages	CVE-2026-23652	원격 코드 실행	정보없음	**높음(추정)**	우선 패치 권고	-	원격 코드 실행 / CVSS 정보없음(추정) / 우선 패치 권고
167	Microsoft Global Secure Access (GSA)	CVE-2026-23663	권한 상승	정보없음	**높음(추정)**	우선 패치 권고	-	권한 상승 / CVSS 정보없음(추정) / 우선 패치 권고
168	Microsoft Edge (Chromium)	CVE-2026-32208	스푸핑	정보없음	**높음(추정)**	우선 패치 권고	-	스푸핑 / CVSS 정보없음(추정) / 우선 패치 권고

169	Microsoft Entra ID	CVE-2026-33843	권한 상승	정보없음	**높음(추정)**	우선 패치 권고	-	권한 상승 / CVSS 정보없음(추정) / 우선 패치 권고
170	Microsoft Planetary Computer Pro (GeoCatalog)	CVE-2026-41104	정보 유출	정보없음	**높음(추정)**	우선 패치 권고	-	정보 유출 / CVSS 정보없음(추정) / 우선 패치 권고
171	Microsoft Authenticator	CVE-2026-41615	정보 유출	정보없음	**높음(추정)**	우선 패치 권고	-	정보 유출 / CVSS 정보없음(추정) / 우선 패치 권고
172	Microsoft Entra ID	CVE-2026-42901	권한 상승	정보없음	**높음(추정)**	우선 패치 권고	-	권한 상승 / CVSS 정보없음(추정) / 우선 패치 권고
173	Microsoft Edge (Chromium)	CVE-2026-45492	보안 기능 우회	정보없음	**낮음(추정)**	정기 업데이트 시 적용	-	보안 기능 우회 / CVSS 정보없음(추정) / 정기 업데이트 시 적용
174	Microsoft Edge (Chromium)	CVE-2026-45494	스푸핑	정보없음	**낮음(추정)**	정기 업데이트 시 적용	-	스푸핑 / CVSS 정보없음(추정) / 정기 업데이트 시 적용

175	Microsoft Edge (Chromium)	CVE-2026-45495	원격 코드 실행	정보없음	**보통(추정)**	조기 패치 권고	-	원격 코드 실행 / CVSS 정보없음(추정) / 조기 패치 권고
176	Microsoft Defender Antimalware Platform	CVE-2026-45498	서비스 거부	정보없음	**낮음(추정)**	정기 업데이트 시 적용	-	서비스 거부 / CVSS 정보없음(추정) / 정기 업데이트 시 적용
177	Microsoft Malware Protection Engine	CVE-2026-45584	원격 코드 실행	정보없음	**높음(추정)**	우선 패치 권고	-	원격 코드 실행 / CVSS 정보없음(추정) / 우선 패치 권고
178	Windows	CVE-2026-45585	보안 기능 우회	정보없음	**보통(추정)**	조기 패치 권고	5094125, 5094126, 5095051	보안 기능 우회 / CVSS 정보없음(추정) / 조기 패치 권고
179	Microsoft SharePoint Enterprise Server	CVE-2026-45659	원격 코드 실행	정보없음	**보통(추정)**	조기 패치 권고	5002863, 5002868, 5002870	원격 코드 실행 / CVSS 정보없음(추정) / 조기 패치 권고
180	Microsoft SharePoint Enterprise Server	CVE-2026-47294	원격 코드 실행	정보없음	**보통(추정)**	조기 패치 권고	5002863, 5002868, 5002870	원격 코드 실행 / CVSS 정보없음(추정) / 조기 패치 권고

181	Microsoft Cost Management	CVE-2026-47633	정보 유출	정보없음	**높음(추정)**	우선 패치 권고	-	정보 유출 / CVSS 정보없음(추정) / 우선 패치 권고
182	Microsoft PC Manager	CVE-2026-49161	보안 기능 우회	정보없음	**보통(추정)**	조기 패치 권고	-	보안 기능 우회 / CVSS 정보없음(추정) / 조기 패치 권고
183	Windows	CVE-2026-50507	보안 기능 우회	정보없음	**보통(추정)**	조기 패치 권고	5093998, 5094041, 5094122, 5094123, 5094126, 5094127, 5094128, 5095051	보안 기능 우회 / CVSS 정보없음(추정) / 조기 패치 권고
184	Windows	CVE-2026-50508	스푸핑	정보없음	**보통(추정)**	조기 패치 권고	5093998, 5094041, 5094042, 5094122, 5094127, 5094128	스푸핑 / CVSS 정보없음(추정) / 조기 패치 권고
185	Microsoft PC Manager	CVE-2026-50511	권한 상승	정보없음	**보통(추정)**	조기 패치 권고	-	권한 상승 / CVSS 정보없음(추정) / 조기 패치 권고
186	Microsoft PC Manager	CVE-2026-50512	권한 상승	정보없음	**보통(추정)**	조기 패치 권고	-	권한 상승 / CVSS 정보없음(추정) / 조기 패치 권고

187	Microsoft Edge (Chromium)	CVE-2026-50521	원격 코드 실행	정보없음	**보통(추정)**	조기 패치 권고	-	원격 코드 실행 / CVSS 정보없음(추정) / 조기 패치 권고
188	Microsoft Malware Protection Engine	CVE-2026-50656	권한 상승	정보없음	**보통(추정)**	조기 패치 권고	-	권한 상승 / CVSS 정보없음(추정) / 조기 패치 권고

5. 서버 관리자 전용 목록 (45 건)

연번	분류	CVE	영향	CVSS	위험등급	권장조치	KB ID	비고
1	Microsoft Azure Kubernetes Service	CVE-2026-32193	원격 코드 실행	8.8	**높음**	우선 패치 권고	-	원격 코드 실행 / 악용 불가능 / 우선 패치 권고
2	Microsoft Dynamics 365(온-프레미스)	CVE-2026-40371	권한 상승	8.8	**높음**	우선 패치 권고	-	권한 상승 / 악용 가능성 낮음 / 우선 패치 권고
3	Microsoft Exchange Server	CVE-2026-45504	권한 상승	8.8	**높음**	우선 패치 권고	5094139, 5094140, 5094142, 5094144	권한 상승 / 악용 불가능 / 우선 패치 권고
4	Active Directory Domain Services	CVE-2026-45648	원격 코드 실행	8.8	**높음**	우선 패치 권고	5094125, 5094128	원격 코드 실행 / 악용 불가능 / 우선 패치 권고
5	Azure Stack Edge	CVE-2026-41098	스푸핑	8.4	**높음**	우선 패치 권고	-	스푸핑 / 악용 가능성 낮음 / 우선 패치 권고

6	GitHub Copilot 및 Visual Studio Code	CVE-2026-45482	보안 기능 우회	8.4	**높음**	우선 패치 권고	-	보안 기능 우회 / 악용 가능성 낮음 / 우선 패치 권고
7	Windows 배포 서비스	CVE-2026-42987	원격 코드 실행	8.1	**높음**	우선 패치 권고	5094041, 5094042, 5094122, 5094123, 5094125, 5094128	원격 코드 실행 / 악용 가능성 낮음 / 우선 패치 권고
8	Microsoft Exchange Server	CVE-2026-45503	정보 유출	8.1	**높음**	우선 패치 권고	5094139, 5094140, 5094142, 5094144	정보 유출 / 악용 불가능 / 우선 패치 권고
9	Microsoft Exchange Server	CVE-2026-47631	스푸핑	8.1	**높음**	우선 패치 권고	5094139, 5094140, 5094142, 5094144	스푸핑 / 악용 가능성 낮음 / 우선 패치 권고
10	Microsoft Azure 증명 서비스 및 디바이스 상태 증명 서비스	CVE-2026-33828	권한 상승	7.8	**높음**	우선 패치 권고	5093998, 5094122, 5094123, 5094125, 5094126, 5094127, 5094128, 5095051	권한 상승 / 악용 불가능 / 우선 패치 권고
11	Microsoft Copilot	CVE-2026-45497	원격 코드 실행	7.7	**높음**	우선 패치 권고	-	원격 코드 실행 / 우선 패치 권고
12	Microsoft Exchange Server	CVE-2026-45583	원격 코드 실행	7.5	**높음**	우선 패치 권고	5094139, 5094140, 5094142, 5094144	원격 코드 실행 / 악용 가능성 낮음 / 우선 패치 권고

13	원격 데스크톱 클라이언트	CVE-2026-47654	원격 코드 실행	7.5	**높음**	우선 패치 권고	5094122, 5094123, 5094125, 5094128	원격 코드 실행 / 악용 불가능 / 우선 패치 권고
14	Windows Kerberos	CVE-2026-47288	원격 코드 실행	7.1	**높음**	우선 패치 권고	5094041, 5094042, 5094122, 5094123, 5094125, 5094128	원격 코드 실행 / 악용 불가능 / 우선 패치 권고
15	Microsoft Windows DNS	CVE-2026-41108	권한 상승	7.0	**높음**	우선 패치 권고	5093998, 5094041, 5094042, 5094122, 5094123, 5094125, 5094126, 5094127, 5094128, 5095051	권한 상승 / 악용 불가능 / 우선 패치 권고
16	M365 Copilot	CVE-2026-42824	정보 유출	6.5	**보통**	조기 패치 권고	-	정보 유출 / 조기 패치 권고
17	Microsoft Exchange Server	CVE-2026-45501	스푸핑	6.5	**보통**	조기 패치 권고	5094139, 5094140, 5094142, 5094144	스푸핑 / 악용 가능성 낮음 / 조기 패치 권고
18	Copilot Chat(Microsoft Edge)	CVE-2026-47644	정보 유출	6.5	**보통**	조기 패치 권고	-	정보 유출 / 악용 가능성 낮음 / 조기 패치 권고
19	Microsoft Graph	CVE-2026-47655	정보 유출	6.5	**보통**	조기 패치 권고	-	정보 유출 / 조기 패치 권고

20	Microsoft Exchange Server	CVE-2026-45500	스푸핑	6.1	**보통**	조기 패치 권고	5094139, 5094140, 5094142, 5094144	스푸핑 / 악용 가능성 낮음 / 조기 패치 권고
21	Windows 네트워크 컨트롤러(NC) 호스트 에이전트	CVE-2026-44805	서비스 거부	5.5	**보통**	조기 패치 권고	5094123, 5094125, 5094128	서비스 거부 / 악용 불가능 / 조기 패치 권고
22	Windows DHCP Server	CVE-2026-45634	정보 유출	5.5	**보통**	조기 패치 권고	5093998, 5094041, 5094042, 5094122, 5094123, 5094125, 5094126, 5094127, 5094128, 5095051	정보 유출 / 악용 불가능 / 조기 패치 권고
23	엔드포인트용 Microsoft Defender	CVE-2026-45647	권한 상승	5.5	**보통**	조기 패치 권고	-	권한 상승 / 악용 가능성 낮음 / 조기 패치 권고
24	Microsoft Exchange Server	CVE-2026-45502	정보 유출	5.0	**보통**	조기 패치 권고	5094139, 5094140, 5094142, 5094144	정보 유출 / 악용 불가능 / 조기 패치 권고
25	Microsoft Bing	CVE-2026-45650	스푸핑	4.3	**보통**	조기 패치 권고	-	스푸핑 / 악용 가능성 낮음 / 조기 패치 권고

26	Microsoft Azure 증명 서비스 및 디바이스 상태 증명 서비스	CVE-2026-45642	스푸핑	3.9	**낮음**	정기 업데이트 시 적용	5093998, 5094041, 5094042, 5094122, 5094123, 5094125, 5094126, 5094127, 5094128, 5095051	스푸핑 / 악용 가능성 낮음 / 정기 업데이트 시 적용
27	Azure Stack HCI	CVE-2026-26147	정보 유출	정보없음	**높음(추정)**	우선 패치 권고	-	정보 유출 / CVSS 정보없음(추정) / 우선 패치 권고
28	Azure AI Bot Service	CVE-2026-32174	권한 상승	정보없음	**높음(추정)**	우선 패치 권고	-	권한 상승 / CVSS 정보없음(추정) / 우선 패치 권고
29	Azure Privileged Identity Management (PIM)	CVE-2026-35430	권한 상승	정보없음	**높음(추정)**	우선 패치 권고	-	권한 상승 / CVSS 정보없음(추정) / 우선 패치 권고
30	Azure Virtual Network Gateway	CVE-2026-40411	원격 코드 실행	정보없음	**높음(추정)**	우선 패치 권고	-	원격 코드 실행 / CVSS 정보없음(추정) / 우선 패치 권고

31	Azure Orbital Spatio	CVE-2026-40412	원격 코드 실행	정보없음	**높음(추정)**	우선 패치 권고	-	원격 코드 실행 / CVSS 정보없음(추정) / 우선 패치 권고
32	Microsoft	CVE-2026-41090	변조	정보없음	**높음(추정)**	우선 패치 권고	-	변조 / CVSS 정보없음(추정) / 우선 패치 권고
33	Azure Local	CVE-2026-42822	권한 상승	정보없음	**높음(추정)**	우선 패치 권고	-	권한 상승 / CVSS 정보없음(추정) / 우선 패치 권고
34	Microsoft	CVE-2026-42827	정보 유출	정보없음	**높음(추정)**	우선 패치 권고	-	정보 유출 / CVSS 정보없음(추정) / 우선 패치 권고
35	Windows Admin Center in Azure Portal	CVE-2026-42834	권한 상승	정보없음	**보통(추정)**	조기 패치 권고	-	권한 상승 / CVSS 정보없음(추정) / 조기 패치 권고
36	Microsoft	CVE-2026-42895	변조	정보없음	**높음(추정)**	우선 패치 권고	-	변조 / CVSS 정보없음(추정) / 우선 패치 권고
37	Azure Active Directory	CVE-2026-45480	권한 상승	정보없음	**높음(추정)**	우선 패치 권고	-	권한 상승 / CVSS 정보없음(추정) / 우선 패치 권고

38	Azure Resource Manager	CVE-2026-47280	권한 상승	정보없음	**높음(추정)**	우선 패치 권고	-	권한 상승 / CVSS 정보없음(추정) / 우선 패치 권고
39	Microsoft	CVE-2026-47645	권한 상승	정보없음	**높음(추정)**	우선 패치 권고	-	권한 상승 / CVSS 정보없음(추정) / 우선 패치 권고
40	Dynamics	CVE-2026-47646	스푸핑	정보없음	**높음(추정)**	우선 패치 권고	-	스푸핑 / CVSS 정보없음(추정) / 우선 패치 권고
41	Microsoft Dynamics	CVE-2026-47647	권한 상승	정보없음	**높음(추정)**	우선 패치 권고	-	권한 상승 / CVSS 정보없음(추정) / 우선 패치 권고
42	Microsoft Exchange Online	CVE-2026-48582	권한 상승	정보없음	**높음(추정)**	우선 패치 권고	-	권한 상승 / CVSS 정보없음(추정) / 우선 패치 권고
43	Azure Synapse	CVE-2026-48584	권한 상승	정보없음	**높음(추정)**	우선 패치 권고	-	권한 상승 / CVSS 정보없음(추정) / 우선 패치 권고
44	GitHub Copilot Chat	CVE-2026-50519	정보 유출	정보없음	**보통(추정)**	조기 패치 권고	-	정보 유출 / CVSS 정보없음(추정) / 조기 패치 권고

45	Microsoft	CVE-2026-54130	정보 유출	정보없음	**높음(추정)**	우선 패치 권고	-	정보 유출 / CVSS 정보없음(추정) / 우선 패치 권고

6. KB 패치 정보 (36 건)

연번	KB ID	적용 제품	다운로드 유형	관련 CVE 수	비고
1	5095051	Windows 11 Version 26H1 for ARM64-based Systems, Windows 11 version 26H1 for x64-based Systems	Security Update	111	업데이트 안내
2	5094125	Windows Server 2025, Windows Server 2025 (Server Core installation)	Security Update	108	업데이트 안내
3	5094126	Windows 11 Version 24H2 for ARM64-based Systems, Windows 11 Version 24H2 for x64-based Systems, Windows 11 Version 25H2 for ARM64-based Systems, Windows 11 Version 25H2 for x64-based Systems, Windows Server 2025, Windows Server 2025 (Server Core installation)	Security Update	105	업데이트 안내
4	5094128	Windows Server 2022, Windows Server 2022 (Server Core installation)	Security Update	104	업데이트 안내
5	5093998	Windows 11 Version 22H2 for ARM64-based Systems, Windows 11 Version 22H2 for x64-based Systems, Windows 11 Version 23H2 for ARM64-based Systems, Windows 11 Version 23H2 for x64-based Systems	Security Update	100	업데이트 안내

6	5094127	Windows 10 Version 21H2 for 32-bit Systems, Windows 10 Version 21H2 for ARM64-based Systems, Windows 10 Version 21H2 for x64-based Systems, Windows 10 Version 22H2 for 32-bit Systems, Windows 10 Version 22H2 for ARM64-based Systems, Windows 10 Version 22H2 for x64-based Systems 외 1 종	Security Update	92	업데이트 안내
7	5094123	Windows 10 Version 1809 for 32-bit Systems, Windows 10 Version 1809 for x64-based Systems, Windows Server 2019, Windows Server 2019 (Server Core installation)	Security Update	88	업데이트 안내
8	5094122	Windows 10 Version 1607 for 32-bit Systems, Windows 10 Version 1607 for x64-based Systems, Windows Server 2016, Windows Server 2016 (Server Core installation)	Security Update	75	업데이트 안내
9	5094041	Windows Server 2012 R2, Windows Server 2012 R2 (Server Core installation)	Monthly Rollup	64	업데이트 안내
10	5094042	Windows Server 2012, Windows Server 2012 (Server Core installation)	Monthly Rollup	61	업데이트 안내
11	5002873	Microsoft SharePoint Server Subscription Edition	Security Update	30	업데이트 안내
12	5002874	Microsoft SharePoint Server 2019	Security Update	30	업데이트 안내
13	5002880	Microsoft SharePoint Enterprise Server 2016	Security Update	29	업데이트 안내
14	5002878	Microsoft Office 2016 (32-bit edition), Microsoft Office 2016 (64-bit edition)	Security Update	9	업데이트 안내
15	5094142	Microsoft Exchange Server 2019 Cumulative Update 14	Security Update	8	업데이트 안내
16	5094144	Microsoft Exchange Server 2016 Cumulative Update 23	Security Update	8	업데이트 안내

17	5002876	Microsoft SharePoint Server 2019	Security Update	8	업데이트 안내
18	5094139	Microsoft Exchange Server Subscription Edition RTM	Security Update	8	업데이트 안내
19	5094140	Microsoft Exchange Server 2019 Cumulative Update 15	Security Update	8	업데이트 안내
20	5002881	Microsoft SharePoint Enterprise Server 2016	Security Update	8	업데이트 안내
21	5002877	Microsoft Excel 2016 (32-bit edition), Microsoft Excel 2016 (64-bit edition)	Security Update	7	업데이트 안내
22	5002875	Office Online Server	Security Update	7	업데이트 안내
23	5002879	Microsoft Word 2016 (32-bit edition), Microsoft Word 2016 (64-bit edition)	Security Update	3	업데이트 안내
24	5097150	.NET 9.0 installed on Linux, .NET 9.0 installed on Mac OS, .NET 9.0 installed on Windows, ASP.NET Core 9.0	Security Update	3	업데이트 안내
25	5097149	.NET 8.0, .NET 8.0 installed on Linux, .NET 8.0 installed on Mac OS, .NET 8.0 installed on Windows, ASP.NET Core 8.0	Security Update	3	업데이트 안내
26	5097148	.NET 10.0 installed on Linux, .NET 10.0 installed on Mac OS, .NET 10.0 installed on Windows, ASP.NET Core 10.0	Security Update	3	업데이트 안내
27	5002863	Microsoft SharePoint Server Subscription Edition	Security Update	2	업데이트 안내
28	5002870	Microsoft SharePoint Server 2019	Security Update	2	업데이트 안내
29	5002868	Microsoft SharePoint Enterprise Server 2016	Security Update	2	업데이트 안내

30	5089548	Windows 11 Version 26H1 for ARM64-based Systems, Windows 11 version 26H1 for x64-based Systems	Security Update	1	업데이트 안내
31	5094006	Windows Server 2012 R2, Windows Server 2012 R2 (Server Core installation)	IE Cumulative	1	업데이트 안내
32	5087539	Windows Server 2025, Windows Server 2025 (Server Core installation)	Security Update	1	업데이트 안내
33	5087423	Windows Server 2025, Windows Server 2025 (Server Core installation)	Security Hotpatch Update	1	업데이트 안내
34	5089549	Windows 11 Version 24H2 for ARM64-based Systems, Windows 11 Version 24H2 for x64-based Systems, Windows 11 Version 25H2 for ARM64-based Systems, Windows 11 Version 25H2 for x64-based Systems	Security Update	1	업데이트 안내
35	5089466	Windows 11 Version 24H2 for ARM64-based Systems, Windows 11 Version 24H2 for x64-based Systems, Windows 11 Version 25H2 for ARM64-based Systems, Windows 11 Version 25H2 for x64-based Systems	Security Hotpatch Update	1	업데이트 안내
36	5002852	Microsoft Office 2016 (32-bit edition), Microsoft Office 2016 (64-bit edition)	Security Update	1	업데이트 안내

7. 사용자 행동 가이드

■ 일반 PC 사용자

조치 항목	상세 방법	긴급도
Windows 자동 업데이트 즉시 적용	설정 > Windows Update 에서 6 월 누적 업데이트를 즉시 설치·재부팅. 커널(CVE-2026-45657)·HTTP.sys(CVE-2026-47291)·DHCP 클라이언트(CVE-2026-44815) 미인증 원격 코드 실행 포함.	**긴급**

Microsoft Defender 최신화	실제 악용 확인된 Defender 권한 상승(CVE-2026-41091). 보통 자동 갱신되나 자동 업데이트 비활성/격리 환경은 보안 인텔리전스 수동 즉시 갱신.	**긴급**
Office/Word 문서 열람 주의	악용 확인 Office 취약점(CVE-2026-42897) 및 다수 Critical Office RCE. 미확인 문서 미리보기·열람 자제, Office 최신 빌드 갱신.	**긴급**
Microsoft Edge 업데이트	Edge(Chromium) 최신 버전 갱신(설정 > 정보). 다수 RCE 포함.	**높음**
Visual Studio Code 업데이트	개발 PC 는 VS Code(CVE-2026-47281, CVSS 9.6) 최신 버전 즉시 갱신.	**높음**
BitLocker/보안 부팅 점검	물리 접근 기반 BitLocker 우회(CVE-2026-50507)·다수 보안 부팅 우회 포함. 분실·도난 대비 디바이스 물리 보안 강화.	**높음**

■ **IT 관리자**

조치 항목	상세 방법	긴급도
Azure 클라우드 서비스 점검	서비스 측 완화된 HorizonDB(CVE-2026-48567, CVSS 10.0)·Exchange Online(CVE-2026-48579)·Stack Edge(CVE-2026-47643) 접근 로그·권한 이벤트 감사, 자격 증명 교체.	**긴급**
인터넷 노출 웹 서버 우선 패치	HTTP.sys RCE(CVE-2026-47291, 악용 가능성 높음)·HTTP/2 DoS(CVE-2026-49160) 우선 패치. 패치 전 MaxRequestBytes/MaxHeadersCount 완화책 적용.	**긴급**
DHCP/도메인 인프라 패치	DHCP 클라이언트 RCE(CVE-2026-44815)·AD RCE(CVE-2026-45648) 서버 신속 패치, 취약 API 점검.	**긴급**
Exchange Server 긴급 완화	EEMS(Emergency Mitigation Service) 활성화 확인, 6 월 보안 업데이트 긴급 적용.	**긴급**
Hyper-V/가상화 호스트 패치	Critical Hyper-V OOB read(CVE-2026-47652 등) 즉시 적용, 게스트-호스트 신뢰 경계 감사.	**높음**
RDP/원격 데스크톱 클라이언트	원격 데스크톱 클라이언트 다수 CVE(4 건 Critical) 패치, 불필요한 RDP 노출 네트워크 분할 제한.	**높음**

중앙 배포 및 모니터링	SCCM/Intune 로 패치 배포 상태 감사, DC·경계·메일/파일 서버 이상 행위 로깅 강화.	**보통**

참고 링크

- MSRC 2026 년 6 월 릴리스 노트: https://msrc.microsoft.com/update-guide/releaseNote/2026-Jun
- Microsoft Update Catalog: https://www.catalog.update.microsoft.com/
- MSRC 보안 업데이트 가이드: https://msrc.microsoft.com/update-guide/
- CISA KEV 카탈로그: https://www.cisa.gov/known-exploited-vulnerabilities-catalog