m3g YAZILIM & DANIŞMANLIK

AYLIK GÜVENLİK GÜNCELLEMESİ DEĞERLENDİRME RAPORU

Microsoft Patch Tuesday Eylül 2026

Risk sıralı zafiyet analizi, giderme ve azaltım planı

Microsoft yayın tarihi	**8 Eylül 2026 (Salı)**
MSRC bülten kimliği	**2026-Sep**
Rapor tarihi	**21 Eylül 2026**
Kapsam	**Microsoft'un yayınladığı tüm ürün aileleri**
Toplam zafiyet	**972 CVE (114 Critical)**
Aktif istismar edilen	**2 zafiyet (CISA KEV)**
Bir sonraki Patch Tuesday	**13 Ekim 2026 (Salı)**

Acil aksiyon gerektiren iki zafiyet

CVE-2026-81963 (Windows Update Stack) ve **CVE-2026-85880** (Windows ALPC) gerçek dünyada aktif olarak istismar ediliyor ve CISA KEV kataloğuna eklendi. Her ikisi de SYSTEM yetkisi kazanımına yol açıyor. Bakım penceresi beklenmeden, 48 saat içinde yamalanmalıdır.

Bu ayın yaması bir kesinti hatası getirdi

Eylül kümülatif güncellemeleri bazı ortamlarda **Remote Desktop Services kesintilerine** yol açtı. Microsoft 14 Eylül'de bant dışı (out-of-band) düzeltmeler yayınladı. Yamayı uygularken bu güncellemeleri birlikte planlayın — ayrıntı için “Bilinen Sorunlar” bölümüne bakın.

Hazırlayan: m3g Yazılım ve Danışmanlık · info@m3g.com.tr · m3g.com.tr
Bu rapor müşteriye sunum amacıyla hazırlanmıştır. İçerik, Microsoft Security Response Center ve bağımsız güvenlik araştırma kuruluşlarının kamuya açık yayınlarına dayanmaktadır.

1. Yönetici Özeti

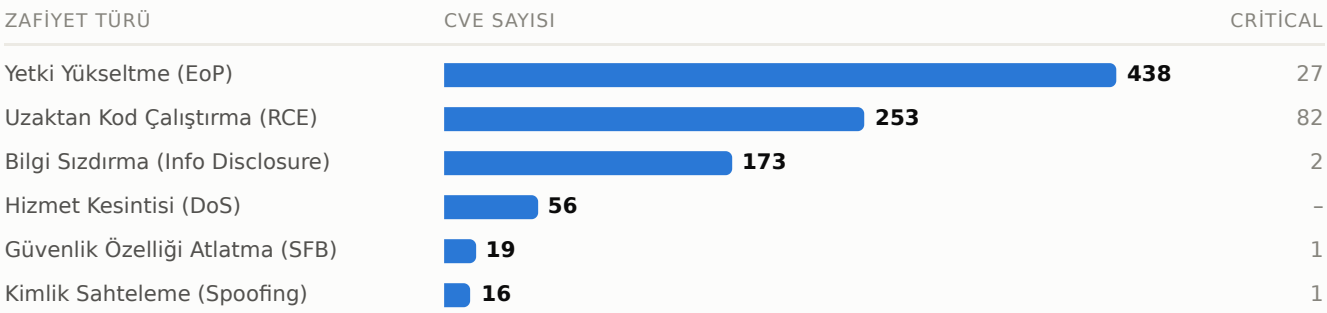
972	114	2	20	41
Toplam yeni CVE (rekor)	Critical seviye	Aktif istismar edilen	Wormable zafiyet	Raporda öncelik verilen kayıt

- **Microsoft tarihinin en büyük Patch Tuesday'i.** 972 yeni CVE kapatıldı; bu, Ağustos ayının yaklaşık iki katı. Analiz kuruluşları metodoloji farkları nedeniyle sayıyı 964 – 974 aralığında raporluyor (Chromium, Mariner ve harici CVE'lerin sayıma dahil edilip edilmemesi). Bu rapor ZDI'nin 972 yeni CVE / 114 Critical sayımını referans alır.
- **İki zafiyet gerçek dünyada aktif olarak istismar ediliyor** ve aynı gün CISA KEV kataloğuna eklendi (son giderme tarihi 22 Eylül 2026): CVE-2026-81963 ve CVE-2026-85880. İkisi de yerel yetki yükseltme; tipik kullanım, bir kod çalıştırma zafiyetiyle zincirlenerek fidye yazılımı dağıtımıdır.
- **20 adet wormable zafiyet** — kimlik doğrulaması ve kullanıcı etkileşimi gerekmeden ağ üzerinden kod çalıştırılabiliyor. Bunlar DNS, DHCP, Netlogon, Active Directory, SMB, MSMQ, NFS, RRAS, SSTP, Failover Cluster ve RMCAST bileşenlerinde. **Sunucu altyapısı bu ay istemcilerden daha yüksek risk taşıyor.**
- **Kritik tek bulgu: CVE-2026-69730 (DNS Server, CVSS 9.8).** Kimlik doğrulaması olmadan tek paketle kod çalıştırma; DNS rolü çoğu kurumda Domain Controller üzerinde çalıştığı için doğrudan domain ele geçirme riski. 2020'deki SigRed'in devamı niteliğinde değerlendiriliyor.
- **Office kullanıcıları için kullanıcı etkileşimi gerekmiyor.** Outlook Önizleme Bölmesiyle tetiklenebilen 12 Critical zafiyet var (CVE-2026-77493, CVE-2026-78509, CVE-2026-78510 dahil, hepsi CVSS 9.8). Kimlik avı kampanyalarında tek tıklama bile gerekmez.
- **Yamanın kendisi bir risk kaynağı oldu.** Eylül güncellemeleri RDS kesintilerine yol açtı; Microsoft 14 Eylül'de bant dışı düzeltmeler yayınladı. Yamayı kaldırmak bir çözüm değildir — OOB güncellemeyi uygulayın.
- **Yama kapsamı dışında kalan bir risk var.** “ShieldCrash” adlı PoC, Microsoft Defender'daki ShieldBreak (CVE-2026-69414) yamasının atlatılabildiğini gösteriyor; rapor tarihi itibarıyla yayınlanmış bir düzeltme yok.

2. Sayılar ve Dağılım

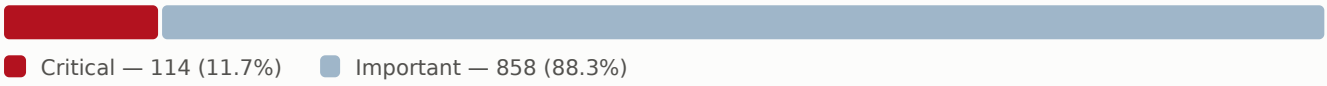
Zafiyet türüne göre dağılım

972 CVE · Kaynak: Qualys / CrowdStrike / BleepingComputer, Eylül 2026



Önem derecesine göre dağılım

Microsoft önem derecelendirmesi · Moderate ve Low seviyesinde kayıt yok



ETKİLENEN ÜRÜN AİLESİ	YAKLAŞIK HACİM
Windows bileşenleri (çekirdek OS, ağ servisleri, sürücüler)	100+ bileşen
SQL Server	60+ CVE
Microsoft Office / M365 Apps (Word, Excel, Outlook)	Çok sayıda, 12 Critical Preview Pane RCE dahil
SharePoint Server	17 CVE (4 RCE)
Exchange Server (on-prem)	2 öne çıkan CVE
Azure servisleri (Cosmos DB, AI Language, Entra ID, Spring Cloud)	Çok sayıda Critical
Hyper-V	2 guest-to-host kaçış
Dynamics 365 / Power Automate / Teams / Visual Studio / Copilot Studio	Çok sayıda

Bu tablo bültenin ağırlık merkezini gösterir; tam CVE dökümü ekteki Excel dosyasında ve MSRC portalındadır.

3. Önceliklendirme Metodolojisi

Microsoft'un “Critical / Important” etiketi ve CVSS taban puanı tek başına operasyonel öncelik vermez: CVSS 7.8'lik, aktif istismar edilen bir zafiyet, CVSS 9.8'lik teorik bir zafiyetten daha aciledir. Bu raporda sıralama **m3g Risk Puanı** ile yapılır — istismar durumunu, yayılabilirliği ve maruziyeti birlikte ağırlıklandıran 0–100 arası bir puandır.

PUANLAMA KRİTERİ	AĞIRLIK
Gerçek dünyada aktif olarak istismar edildiği doğrulanmış / CISA KEV kaydı	+55
Wormable: kimlik doğrulaması ve kullanıcı etkileşimi olmadan ağdan yayılabilir	+16
CVSS v3.1 taban puanı (9.8+ → 15 · 9.0+ → 13 · 8.0+ → 9 · 7.0+ → 6 · skor yok + Critical → 9)	+15
Kimlik doğrulaması gerekmiyor (unauthenticated)	+8
İnternete açık servis / ağ kenarı bileşeni	+6
Domain Controller veya kimlik altyapısı bileşeni	+6
Kullanıcı etkileşimi gerekmiyor (ör. Outlook Önizleme Bölmesi ile tetiklenebilir)	+5
Microsoft'un “istismar daha olası” (Exploitation More Likely) değerlendirmesi	+5

m3g Risk Puanı, m3g Yazılım ve Danışmanlık'ın kendi önceliklendirme modelidir; Microsoft veya CVSS tarafından yayınlanan resmî bir skor değildir. Kaynak CVSS puanları ayrı kolonda verilmiştir.

Puanlar ardından beş uygulama sınıfına (P1–P5) ayrılır. Sınıf, aksiyonun **ne zaman** yapılacağını; puan ise sınıf içindeki **sırayı** belirler.

SINIF	TANIM VE HEDEF SÜRE
P1 ACİL (48 saat)	Gerçek dünyada aktif olarak istismar edilen, CISA KEV listesinde yer alan zafiyetler. Bakım penceresi beklenmeden uygulanmalı.
P2 ÇOK YÜKSEK (72 saat)	Kimlik doğrulaması gerektirmeyen, wormable veya internete açık uzaktan kod çalıştırma zafiyetleri. Sunucu altyapısı hedefli.
P3 YÜKSEK (7 gün)	Kimlik katmanı, sanallaştırma izolasyonu ve kullanıcı etkileşimi gerektirmeyen Office/Windows RCE zafiyetleri.
P4 ORTA-YÜKSEK (test + 30 gün)	On-prem sunucu uygulamaları (Exchange, SharePoint, SQL Server). Uygulama uyumluluk testi ve planlı kesinti gerektirir.
P5 BİLGİLENDİRME / DÜŞÜK AKSİYON	Microsoft tarafından servis tarafında düzeltilen bulut zafiyetleri ve mobil/uygulama bağımlılığı güncellemeleri.

4. Öncelik Sıralı Bulgu Listesi (Özet)

Aşağıdaki 41 kayıt, bu ayın 972 CVE'si içinden operasyonel olarak öne çıkan zafiyetleri kapsar; bazı satırlar aynı bileşendeki birden fazla CVE'yi birlikte gösterir. Sıralama en önemliden en az önemliye doğrudur.

#	SINIF	CVE	ETKİLENEN ÜRÜN / BİLEŞEN	TÜR	CVSS	PUAN
1	P1	CVE-2026-81963	Windows Update Stack	EoP	7.8	**66**
2	P1	CVE-2026-85880	Windows ALPC (Advanced Local Procedure Call)	EoP	7.8	**66**
3	P2	CVE-2026-69730	Windows DNS Server	RCE	9.8	**61**
4	P2	CVE-2026-72982	Windows Netlogon	RCE	9.8	**55**
5	P2	CVE-2026-69858	Windows DNS Server	RCE	Yayınlanmadı	**50**
6	P2	CVE-2026-69524	Active Directory	RCE	Yayınlanmadı	**44**
7	P2	CVE-2026-69590	Windows RRAS (Routing and Remote Access Service)	RCE	Yayınlanmadı	**44**
8	P2	CVE-2026-69845 / CVE-2026-72979 / CVE-2026-69510	Windows DHCP Server	RCE	Yayınlanmadı	**44**
9	P2	CVE-2026-73009	Windows SSTP (Secure Socket Tunneling Protocol)	RCE	Yayınlanmadı	**44**
10	P2	CVE-2026-69525	Remote Desktop Services (RDS)	RCE	9.8	**39**
11	P2	CVE-2026-69530 / CVE-2026-78449 / CVE-2026-78450	Windows RMCAST (Pragmatic General Multicast)	RCE	Yayınlanmadı	**38**
12	P2	CVE-2026-69579 / CVE-2026-83997	Windows Message Queuing (MSMQ)	RCE	Yayınlanmadı	**38**
13	P2	CVE-2026-69595 / CVE-2026-78445	Windows NFS (ONCRPC XDR sürücüsü)	RCE	Yayınlanmadı	**38**
14	P2	CVE-2026-72936	Windows SMB Client	RCE	Yayınlanmadı	**38**
15	P2	CVE-2026-72983	Windows Internet Connection Sharing (ICS)	RCE	Yayınlanmadı	**38**
16	P2	CVE-2026-73010 / CVE-2026-78444	Windows Failover Cluster	RCE	Yayınlanmadı	**38**
17	P2	CVE-2026-66302	Skype for Business Server	RCE	9.8	**34**
18	P2	CVE-2026-72981	Windows IP Helper	RCE	Yayınlanmadı	**22**
19	P3	CVE-2026-77493	Windows Graphics Component	RCE	9.8	**33**
20	P3	CVE-2026-78509	Microsoft Outlook	RCE	9.8	**33**
21	P3	CVE-2026-78510	Microsoft Word	RCE	9.8	**33**
22	P3	CVE-2026-69676	Windows Kerberos	RCE	8.8	**28**
23	P3	CVE-2026-34182	CMS AuthEnvelopedData (kriptografi yığını)	RCE	Yayınlanmadı	**22**

#	SINIF	CVE	ETKİLENEN ÜRÜN / BİLEŞEN	TÜR	CVSS	PUAN
24	P3	CVE-2026-72986 / CVE-2026-73018	Windows Graphic Fonts	RCE	Yayınlanmadı	**22**
25	P3	CVE-2026-69603 / CVE-2026-80083	Windows Hyper-V	RCE	8.8	**14**
26	P3	CVE-2026-58599	HEVC Video Extensions / Windows Codecs Library	RCE	Yayınlanmadı	**9**
27	P3	CVE-2026-69518	Remote Desktop Client	RCE	8.8	**9**
28	P3	CVE-2026-69830	Windows Shell	RCE	Yayınlanmadı	**9**
29	P3	CVE-2026-77504	Microsoft Word	RCE	Yayınlanmadı	**9**
30	P3	CVE-2026-81948 … CVE-2026-81951	Microsoft Excel	RCE	Yayınlanmadı	**9**
31	P4	CVE-2026-55007	Microsoft Exchange Server (on-prem)	RCE	8.1	**28**
32	P4	CVE-2026-69465	Microsoft SharePoint Server	RCE	8.8	**25**
33	P4	CVE-2026-69380	Microsoft Exchange Server (on-prem)	EoP	8.1	**20**
34	P4	CVE-2026-65669	Microsoft SQL Server (SQL Copilot bileşeni)	EoP	9.6	**13**
35	P4	CVE-2026-67631 / 67643 / 67378 / 67636	Microsoft SQL Server	RCE	8.8	**9**
36	P5	CVE-2026-69854	Spring Cloud Azure	EoP	9.0	**19**
37	P5	CVE-2026-69857	Azure Cosmos DB	EoP	Yayınlanmadı	**15**
38	P5	CVE-2026-70352	Azure AI Language	RCE	Yayınlanmadı	**15**
39	P5	CVE-2026-80098	Microsoft Copilot Studio	RCE	Yayınlanmadı	**15**
40	P5	CVE-2026-83941	Microsoft Entra ID	EoP	Yayınlanmadı	**15**
41	P5	CVE-2026-80097	Microsoft Authenticator (Android)	EoP	8.6	**9**

5. Detaylı Bulgular — Etki, Giderme ve Azaltım

Her kayıt için etki değerlendirmesi, kalıcı giderme adımı (remediation) ve yama uygulanana kadar riski düşüren telafi edici kontroller (mitigation) verilmiştir. Microsoft'un resmî bir geçici çözüm yayınlamadığı durumlar açıkça belirtilmiş, m3g'nin önerdiği telafi edici kontroller ayrıca etiketlenmiştir.

P1 – ACİL (48 saat)

2 kayıt

Gerçek dünyada aktif olarak istismar edilen, CISA KEV listesinde yer alan zafiyetler. Bakım penceresi beklenmeden uygulanmalı.

#1 CVE-2026-81963 m3g Risk Puanı **66**/100

Windows Update Stack yetki yükseltme (link following)

Ürün: Windows Update Stack **Tür:** EoP **MS Önem:** Important **CVSS:** 7.8

AKTİF İSTİSMAR | CISA KEV | İSTİSMAR DAHA OLASI

ETKİ

Sisteme düşük yetkiyle erişmiş bir saldırgan, hatalı sembolik bağlantı çözümlemesi (improper link resolution) üzerinden SYSTEM yetkisine yükselir. Gerçek dünyada aktif olarak istismar ediliyor; tipik olarak bir kod çalıştırma zafiyetiyle zincirlenip fidye yazılımı/kötü amaçlı yazılım dağıtımında kullanılıyor.

GİDERME (REMEDİATİON)

Eylül 2026 kümülatif güncellemesini TÜM Windows istemci ve sunucularda 48 saat içinde uygulayın. CISA KEV son tarihi 22 Eylül 2026.

AZALTIM (MİTİGATİON)

Microsoft geçici çözüm yayınlamadı. Telafi edici kontrol (m3g önerisi): yerel yönetici haklarını kaldırın, LAPS kullanın, EDR üzerinde SYSTEM'e token çalma ve şüpheli junction/symlink oluşturma tespitlerini açın.

Kaynak: MSRC 2026-Sep; ZDI; CrowdStrike; CISA KEV (08.09.2026)

#2 CVE-2026-85880 m3g Risk Puanı **66**/100

Windows ALPC yetki yükseltme (heap-based buffer overflow)

Ürün: Windows ALPC (Advanced Local Procedure Call) **Tür:** EoP **MS Önem:** Important **CVSS:** 7.8

AKTİF İSTİSMAR | CISA KEV | İSTİSMAR DAHA OLASI

ETKİ

ALPC bileşenindeki heap taşması ile yetkili bir saldırgan yerel olarak SYSTEM yetkisi elde eder; AppContainer sandbox'ından kaçış sağlar. Volexity tarafından gerçek dünyada aktif istismar halinde tespit edildi; belge veya PDF içine gömülerek taşınabiliyor.

GİDERME (REMEDİATİON)

Eylül 2026 kümülatif güncellemesini 48 saat içinde uygulayın. CISA KEV son tarihi 22 Eylül 2026.

AZALTIM (MİTİGATİON)

Microsoft geçici çözüm yayınlamadı. Telafi edici kontrol (m3g önerisi): Office/PDF eklerinde Protected View ve ASR kurallarını (Office'in alt süreç oluşturmasını engelle) zorunlu kılın, EDR'de sandbox kaçış tespitlerini etkinleştirin.

Kaynak: MSRC 2026-Sep; ZDI; Volexity; CISA KEV (08.09.2026)

P2 – ÇOK YÜKSEK (72 saat)

16 kayıt

Kimlik doğrulaması gerektirmeyen, wormable veya internete açık uzaktan kod çalıştırma zafiyetleri. Sunucu altyapısı hedefli.

#3 CVE-2026-69730

m3g Risk Puanı **61**/100

Windows DNS Server uzaktan kod çalıştırma (use-after-free) – wormable

Ürün: Windows DNS Server **Tür:** RCE **MS Önem:** Critical **CVSS:** 9.8

WORMABLE | KİMLİK DOĞRULAMASI GEREKMİYOR | İNTERNETE AÇIK YÜZEY | DC / KİMLİK ALTYAPISI | KULLANICI ETKİLEŞİMİ GEREKMİYOR | İSTİSMAR DAHA OLASI

ETKİ

Kimlik doğrulaması olmayan bir saldırgan özel hazırlanmış tek bir paketle DNS servisinde kod çalıştırır. DNS rolü çoğu kurumda Domain Controller üzerinde çalıştığı için doğrudan domain ele geçirme riski taşır. 2020'deki SigRed'in 'manevi devamı' olarak nitelendirildi; Microsoft istismarı 'daha olası' olarak işaretledi.

GİDERME (REMEDİATİON)

DNS rolü çalışan tüm sunucuları (özellikle DC'leri) ilk bakım penceresinde yamalayın. Bu ay sırasında en yüksek öncelikli sunucu yaması.

AZALTIM (MİTİGATİON)

Yayınlanmış resmi workaround yok. Telafi edici kontrol (m3g önerisi): DNS'i internete kapatın, yalnızca gerekli forwarder'lara izin verin, iç ağda DNS trafiğini segmentleyin, DNS servisi çökme/yeniden başlama olaylarını izleyin.

Kaynak: Tenable; CrowdStrike; ZDI; SecurityAffairs

#4 CVE-2026-72982

m3g Risk Puanı **55**/100

Netlogon uzaktan kod çalıştırma (stack-based buffer overflow) – wormable

Ürün: Windows Netlogon **Tür:** RCE **MS Önem:** Critical **CVSS:** 9.8

WORMABLE | KİMLİK DOĞRULAMASI GEREKMİYOR | DC / KİMLİK ALTYAPISI | KULLANICI ETKİLEŞİMİ GEREKMİYOR | İSTİSMAR DAHA OLASI

ETKİ

Kimlik doğrulaması olmadan ağ üzerinden Netlogon servisinde kod çalıştırma. Netlogon doğrudan Domain Controller bileşeni olduğundan başarılı istismar tüm Active Directory ormanının ele geçirilmesi anlamına gelir.

GİDERME (REMEDİATİON)

Tüm Domain Controller'ları acil bakım penceresinde yamalayın. DC'ler bu ay ilk sırada güncellenmelidir.

AZALTIM (MİTİGATİON)

Workaround yok. Telafi edici kontrol: DC'lere SMB/RPC erişimini yalnızca yönetim ve üye sunucu segmentlerinden açın, Tier-0 yönetim modeli uygulayın, anormal Netlogon RPC çağrılarını izleyin.

Kaynak: CrowdStrike; ZDI; Qualys

#5 **CVE-2026-69858** m3g Risk Puanı **50**/100

DNS Server ikinci wormable uzaktan kod çalıştırma

Ürün: Windows DNS Server **Tür:** RCE **MS Önem:** Critical **CVSS:** Yayınlanmadı

WORMABLE KİMLİK DOĞRULAMASI GEREKMİYOR İNTERNETE AÇIK YÜZEY DC / KİMLİK ALTYAPISI KULLANICI ETKİLEŞİMİ GEREKMİYOR

ETKİ

CVE-2026-69730 ile aynı saldırı yüzeyinde ikinci wormable DNS zafiyeti; tek başına da domain ele geçirmeye götürebilir.

GİDERME (REMEDİATİON)

DNS sunucularını CVE-2026-69730 ile birlikte aynı pencerede yamalayın.

AZALTIM (MİTİGATİON)

Bkz. CVE-2026-69730 azaltımları.

Kaynak: ZDI

#6 **CVE-2026-69524** m3g Risk Puanı **44**/100

Active Directory uzaktan kod çalıştırma – wormable

Ürün: Active Directory **Tür:** RCE **MS Önem:** Critical **CVSS:** Yayınlanmadı

WORMABLE KİMLİK DOĞRULAMASI GEREKMİYOR DC / KİMLİK ALTYAPISI KULLANICI ETKİLEŞİMİ GEREKMİYOR

ETKİ

Kimlik doğrulaması olmadan, kullanıcı etkileşimi gerekmeden AD bileşeninde kod çalıştırma. Kimlik altyapısının doğrudan hedef alınması nedeniyle etki 'tam domain ele geçirme' seviyesindedir.

GİDERME (REMEDİATİON)

Tüm Domain Controller'ları bu ay ilk yamalanacak grup olarak planlayın.

AZALTIM (MİTİGATİON)

Telafi edici kontrol: Tier-0 izolasyonu, DC'lerde yalnızca gerekli portların açık olması, AD yönetim işlemlerinin ayrı PAW makinelerinden yapılması.

Kaynak: ZDI; SecurityAffairs

#7 **CVE-2026-69590** m3g Risk Puanı **44**/100

RRAS uzaktan kod çalıştırma – wormable

Ürün: Windows RRAS (Routing and Remote Access Service) **Tür:** RCE **MS Önem:** Critical **CVSS:** Yayınlanmadı

WORMABLE KİMLİK DOĞRULAMASI GEREKMİYOR İNTERNETE AÇIK YÜZEY KULLANICI ETKİLEŞİMİ GEREKMİYOR

ETKİ

RRAS rolü çalışan sunucularda kimlik doğrulaması olmadan kod çalıştırma. RRAS sunucuları sıklıkla ağ kenarında konumlanır.

GİDERME (REMEDİATİON)

RRAS/VPN/NAT rolü kurulu sunucuları yamalayın.

AZALTIM (MİTİGATİON)

Telafi edici kontrol: RRAS kullanılmıyorsa rolü kaldırın; kullanılıyorsa yönetim arayüzünü internetten ayırın.

Kaynak: ZDI

#8 **CVE-2026-69845 / CVE-2026-72979 / CVE-2026-69510** m3g Risk Puanı **44**/100

DHCP Server uzaktan kod çalıştırma (heap overflow + use-after-free) – wormable

Ürün: Windows DHCP Server **Tür:** RCE **MS Önem:** Critical **CVSS:** Yayınlanmadı

WORMABLE | KİMLİK DOĞRULAMASI GEREKMİYOR | DC / KİMLİK ALTYAPISI | KULLANICI ETKİLEŞİMİ GEREKMİYOR

ETKİ

DHCP servisi kimlik doğrulaması olmadan, yerel ağdan gelen hazırlanmış paketlerle kod çalıştırmaya açık. DHCP genelde altyapı/DC sunucularında çalışır; ele geçirilmesi ağ genelinde ortadaki adam ve kalıcılık imkânı verir.

GİDERME (REMEDİATİON)

DHCP rolü çalışan tüm sunucuları yamalayın; failover eşlerini sırayla güncelleyin.

AZALTIM (MİTİGATİON)

Telafi edici kontrol: DHCP sunucularını ayrı yönetim VLAN'ında tutun, DHCP snooping ve rogue DHCP tespiti uygulayın.

Kaynak: Qualys; CrowdStrike; ZDI

#9 **CVE-2026-73009** m3g Risk Puanı **44**/100

SSTP VPN uzaktan kod çalıştırma – wormable

Ürün: Windows SSTP (Secure Socket Tunneling Protocol) **Tür:** RCE **MS Önem:** Critical **CVSS:** Yayınlanmadı

WORMABLE | KİMLİK DOĞRULAMASI GEREKMİYOR | İNTERNETE AÇIK YÜZEY | KULLANICI ETKİLEŞİMİ GEREKMİYOR

ETKİ

SSTP TCP/443 üzerinden çalıştığı ve genellikle doğrudan internete bakan VPN uç noktalarında konumlandığı için, kimlik doğrulaması gerektirmeyen bu zafiyet dışarıdan doğrudan istismar edilebilecek en tehlikeli yüzeylerden biridir.

GİDERME (REMEDİATİON)

RRAS/SSTP VPN sunucularını acilen yamalayın; internete açık SSTP uç noktaları bu ayın en yüksek maruziyet noktasıdır.

AZALTIM (MİTİGATİON)

Telafi edici kontrol: SSTP kullanılmıyorsa RRAS rolünü/SSTP portunu devre dışı bırakın, IKEv2 veya modern ZTNA çözümüne geçin, 443/SSTP'yi WAF/NGFW arkasına alın.

Kaynak: CrowdStrike; ZDI

#10 CVE-2026-69525 m3g Risk Puanı **39**/100

Remote Desktop Services uzaktan kod çalıştırma (use-after-free)

Ürün: Remote Desktop Services (RDS) **Tür:** RCE **MS Önem:** Critical **CVSS:** 9.8

KİMLİK DOĞRULAMASI GEREKMİYOR | İNTERNETE AÇIK YÜZEY | KULLANICI ETKİLEŞİMİ GEREKMİYOR | İSTİSMAR DAHA OLASI

ETKİ

Kimlik doğrulaması yapılmamış bir saldırgan RDS üzerinde kod çalıştırabilir. Microsoft saldırganın 'ağ içinde' olması gerektiğini belirtiyor; ancak RDP'si internete açık sunucularda doğrudan istismar riski vardır. Kurumların uzaktan erişim altyapısını tamamen ele geçirebilir.

GİDERME (REMEDİATİON)

RDS/terminal sunucularını ve RD Gateway'leri öncelikli yamalayın. DİKKAT: Bu ayın yaması RDS'te kesinti hatası yarattı – aşağıdaki 'Bilinen Sorunlar' bölümünü mutlaka okuyun ve 14 Eylül OOB güncellemesini birlikte uygulayın.

AZALTIM (MİTİGATİON)

Telafi edici kontrol: RDP'yi doğrudan internete açmayın, RD Gateway + NLA + MFA zorunlu kılın, 3389'u dış dünyadan kapatın, oturum sayısı ve başarısız kimlik doğrulama anomalilerini izleyin.

Kaynak: Tenable; ZDI; SecurityAffairs

#11 CVE-2026-69530 / CVE-2026-78449 / CVE-2026-78450 m3g Risk Puanı **38**/100

RMCAST uzaktan kod çalıştırma – wormable (3 CVE)

Ürün: Windows RMCAST (Pragmatic General Multicast) **Tür:** RCE **MS Önem:** Critical **CVSS:** Yayınlanmadı

WORMABLE | KİMLİK DOĞRULAMASI GEREKMİYOR | KULLANICI ETKİLEŞİMİ GEREKMİYOR

ETKİ

PGM/RMCAST sürücüsü üzerinden kimlik doğrulaması olmadan kod çalıştırma; bu bileşen son iki yılda tekrar tekrar wormable zafiyet kaynağı oldu.

GİDERME (REMEDİATİON)

Kümülatif güncellemeyi uygulayın.

AZALTIM (MİTİGATİON)

Telafi edici kontrol: MSMQ/PGM kullanılmıyorsa 'Windows Pragmatic General Multicast (PGM)' bileşenini kaldırın.

Kaynak: ZDI

#12 CVE-2026-69579 / CVE-2026-83997 m3g Risk Puanı **38**/100

MSMQ uzaktan kod çalıştırma (use-after-free) – wormable

Ürün: Windows Message Queuing (MSMQ) **Tür:** RCE **MS Önem:** Critical **CVSS:** Yayınlanmadı

WORMABLE | KİMLİK DOĞRULAMASI GEREKMİYOR | KULLANICI ETKİLEŞİMİ GEREKMİYOR

ETKİ

MSMQ paket işleme sırasındaki use-after-free hatası, kimlik doğrulaması olmadan ağ üzerinden kod çalıştırmaya izin verir. MSMQ çoğu kurumda eski uygulamalar için açık bırakılmış ve unutulmuş bir servistir.

GİDERME (REMEDİATİON)

MSMQ rolü kurulu sunucuları yamalayın. Kurulu olup kullanılmayan yerlerde servisi tamamen kaldırın.

AZALTIM (MİTİGATİON)

Telafi edici kontrol: 'Message Queuing' servisinin çalışıp çalışmadığını ve TCP/1801'in dinlenip dinlenmediğini kontrol edin; gerekmiyorsa rolü kaldırın (kalıcı ve en etkili azaltım).

Kaynak: ZDI; CrowdStrike

#13 **CVE-2026-69595 / CVE-2026-78445** m3g Risk Puanı **38**/100

NFS ONCRPC XDR uzaktan kod çalıştırma – wormable

Ürün: Windows NFS (ONCRPC XDR sürücüsü) **Tür:** RCE **MS Önem:** Critical **CVSS:** Yayınlanmadı

WORMABLE KİMLİK DOĞRULAMASI GEREKMİYOR KULLANICI ETKİLEŞİMİ GEREKMİYOR

ETKİ

NFS sunucu rolündeki ONCRPC XDR sürücüsü üzerinden kimlik doğrulaması olmadan çekirdek seviyesinde kod çalıştırma. Karma Linux/Windows ortamlarında dosya sunucuları hedeftir.

GİDERME (REMEDİATİON)

NFS rolü çalışan dosya sunucularını yamalayın.

AZALTIM (MİTİGATİON)

Telafi edici kontrol: NFS kullanılmıyorsa 'Server for NFS' rolünü kaldırın; kullanılıyorsa TCP/UDP 2049 ve portmapper erişimini yalnızca bilinen istemci subnet'lerine kısıtlayın.

Kaynak: ZDI

#14 **CVE-2026-72936** m3g Risk Puanı **38**/100

SMB Client uzaktan kod çalıştırma – wormable

Ürün: Windows SMB Client **Tür:** RCE **MS Önem:** Critical **CVSS:** Yayınlanmadı

WORMABLE KİMLİK DOĞRULAMASI GEREKMİYOR KULLANICI ETKİLEŞİMİ GEREKMİYOR

ETKİ

Kötü amaçlı bir SMB sunucusuna yönlendirilen istemcide kod çalıştırma. İstemci tarafı olduğu için tüm son kullanıcı filosu etki alanındadır ve ağ içinde yayılma (lateral movement) için ideal bir zincir halkasıdır.

GİDERME (REMEDİATİON)

Tüm istemciler ve sunucular için kümülatif güncellemeyi uygulayın (SMB istemcisi her Windows'ta vardır).

AZALTIM (MİTİGATİON)

Telafi edici kontrol: Dışa doğru TCP/445 ve QUIC/443-SMB trafiğini güvenlik duvarında engelleyin, SMB imzalamayı zorunlu kılın, NTLM kullanımını kısıtlayın.

Kaynak: ZDI; SecurityAffairs

#15 **CVE-2026-72983** m3g Risk Puanı **38**/100

ICS uzaktan kod çalıştırma – wormable

Ürün: Windows Internet Connection Sharing (ICS) **Tür:** RCE **MS Önem:** Critical **CVSS:** Yayınlanmadı

WORMABLE KİMLİK DOĞRULAMASI GEREKMİYOR KULLANICI ETKİLEŞİMİ GEREKMİYOR

ETKİ

ICS servisi üzerinden kimlik doğrulaması olmadan yerel ağdan kod çalıştırma.

GİDERME (REMEDİATİON)

Kümülatif güncellemeyi uygulayın.

AZALTIM (MİTİGATİON)

Telafi edici kontrol: 'Internet Connection Sharing (ICS)' servisini GPO ile devre dışı bırakın – kurumsal ortamlarda neredeyse hiç gerekmez.

Kaynak: ZDI

#16 **CVE-2026-73010 / CVE-2026-78444** m3g Risk Puanı **38**/100

Failover Cluster uzaktan kod çalıştırma – wormable

Ürün: Windows Failover Cluster **Tür:** RCE **MS Önem:** Critical **CVSS:** Yayınlanmadı

WORMABLE KİMLİK DOĞRULAMASI GEREKMİYOR KULLANICI ETKİLEŞİMİ GEREKMİYOR

ETKİ

Cluster iletişim kanalı üzerinden kimlik doğrulaması olmadan kod çalıştırma. SQL Always On, Hyper-V cluster ve dosya sunucusu cluster'ları etkilenir; tek düğümün ele geçirilmesi tüm cluster'a yayılır.

GİDERME (REMEDİATİON)

Cluster düğümlerini rolling update ile, quorum'u koruyarak sırayla yamalayın.

AZALTIM (MİTİGATİON)

Telafi edici kontrol: Cluster heartbeat/iletişim trafiğini ayrı ve izole bir ağda tutun.

Kaynak: ZDI

#17 **CVE-2026-66302** m3g Risk Puanı **34**/100

Skype for Business uzaktan kod çalıştırma

Ürün: Skype for Business Server **Tür:** RCE **MS Önem:** Critical **CVSS:** 9.8

KİMLİK DOĞRULAMASI GEREKMİYOR İNTERNETE AÇIK YÜZEY KULLANICI ETKİLEŞİMİ GEREKMİYOR

ETKİ

CVSS 9.8 seviyesinde uzaktan kod çalıştırma. Skype for Business / Lync sunucuları genellikle Edge rolüyle internete açıktır ve AD ile entegredir.

GİDERME (REMEDİATİON)

On-prem Skype for Business / Lync sunucuları varsa acil yamalayın; yoksa Teams'e göç planını hızlandırın.

AZALTIM (MİTİGATİON)

Telafi edici kontrol: Edge sunucularını reverse proxy arkasına alın, kullanılmayan federasyon ve dial-in servislerini kapatın.

Kaynak: CrowdStrike

#18 **CVE-2026-72981** m3g Risk Puanı **22**/100

IP Helper servisi uzaktan kod çalıştırma

Ürün: Windows IP Helper **Tür:** RCE **MS Önem:** Critical **CVSS:** Yayınlanmadı

KİMLİK DOĞRULAMASI GEREKMİYOR KULLANICI ETKİLEŞİMİ GEREKMİYOR

ETKİ

IP Helper (iphlpsvc) servisi üzerinden ağdan kod çalıştırma; servis varsayılan olarak tüm Windows sistemlerde çalışır.

GİDERME (REMEDİATİON)

Kümülatif güncellemeyi uygulayın.

AZALTIM (MİTİGATİON)

Telafi edici kontrol: IPv6 geçiş teknolojileri (Teredo/6to4/ISATAP) kullanılmıyorsa GPO ile kapatın.

Kaynak: BleepingComputer; ZDI

P3 – YÜKSEK (7 gün)

12 kayıt

Kimlik katmanı, sanallaştırma izolasyonu ve kullanıcı etkileşimi gerektirmeyen Office/Windows RCE zafiyetleri.

#19 CVE-2026-77493

m3g Risk Puanı **33**/100

Windows Graphics uzaktan kod çalıştırma – Outlook Önizleme Bölmesi ile tetiklenebilir

Ürün: Windows Graphics Component **Tür:** RCE **MS Önem:** Critical **CVSS:** 9.8

KİMLİK DOĞRULAMASI GEREKMİYOR | KULLANICI ETKİLEŞİMİ GEREKMİYOR | İSTİSMAR DAHA OLASI

ETKİ

Kullanıcı hiçbir şeye tıklamadan, e-posta Outlook Önizleme (Reading/Preview) Bölmesinde görüntülendiği anda kod çalıştırılabilir. Bu ay bu şekilde tetiklenebilen 12 Critical zafiyet var; kimlik avı kampanyaları için en verimli giriş yolu.

GİDERME (REMEDİATİON)

Office/M365 Apps ve Windows güncellemelerini son kullanıcı filosunda 7 gün içinde tamamlayın.

AZALTIM (MİTİGATİON)

Telafi edici kontrol: Outlook'ta Önizleme Bölmesini geçici olarak kapatın, e-postaları düz metin olarak okuyun, ASR kurallarını ve ek karantinasını (sandboxing) zorunlu kılın.

Kaynak: CrowdStrike

#20 CVE-2026-78509

m3g Risk Puanı **33**/100

Outlook uzaktan kod çalıştırma – Önizleme Bölmesi ile tetiklenebilir

Ürün: Microsoft Outlook **Tür:** RCE **MS Önem:** Critical **CVSS:** 9.8

KİMLİK DOĞRULAMASI GEREKMİYOR | KULLANICI ETKİLEŞİMİ GEREKMİYOR | İSTİSMAR DAHA OLASI

ETKİ

Outlook'ta e-postanın görüntülenmesi kod çalıştırmak için yeterli; kullanıcı etkileşimi gerekmiyor.

GİDERME (REMEDİATİON)

Office / Microsoft 365 Apps güncellemelerini dağıtın.

AZALTIM (MİTİGATİON)

Önizleme Bölmesini kapatın, dış e-postalarda otomatik içerik indirmeyi engelleyin.

Kaynak: CrowdStrike

#21 CVE-2026-78510

m3g Risk Puanı **33**/100

Word uzaktan kod çalıştırma – Önizleme Bölmesi ile tetiklenebilir

Ürün: Microsoft Word **Tür:** RCE **MS Önem:** Critical **CVSS:** 9.8

KİMLİK DOĞRULAMASI GEREKMİYOR | KULLANICI ETKİLEŞİMİ GEREKMİYOR | İSTİSMAR DAHA OLASI

ETKİ

Kötü amaçlı bir Word dosyası açılmadan, yalnızca önizlenerek kod çalıştırabilir.

GİDERME (REMEDİATİON)

Office / Microsoft 365 Apps güncellemelerini dağıtın.

AZALTIM (MİTİGATİON)

Önizleme Bölmesini kapatın, Protected View'ı tüm internet kaynaklı dosyalar için zorunlu kılın, .docm/.rtf eklerini e-posta ağ geçidinde engelleyin.

Kaynak: CrowdStrike

#22 **CVE-2026-69676** m3g Risk Puanı **28**/100

Kerberos kimlik doğrulama atlatma / uzaktan kod çalıştırma (capture-replay)

Ürün: Windows Kerberos **Tür:** RCE **MS Önem:** Critical **CVSS:** 8.8

KİMLİK DOĞRULAMASI GEREKMİYOR | DC / KİMLİK ALTYAPISI | KULLANICI ETKİLEŞİMİ GEREKMİYOR

ETKİ

Capture-replay yöntemiyle kimlik doğrulama atlatılıp keyfi kod çalıştırılabiliyor. Kerberos kimlik katmanının tamamını etkilediği için kimlik hırsızlığı ve yetkisiz erişim zinciri açar.

GİDERME (REMEDİATİON)

Tüm DC'ler ve üye sunucular için kümülatif güncellemeyi uygulayın.

AZALTIM (MİTİGATİON)

Telafi edici kontrol: Kerberos armoring (FAST), AES-only şifreleme, RC4 devre dışı bırakma, anormal TGS/TGT taleplerinin izlenmesi.

Kaynak: Tenable; CrowdStrike

#23 **CVE-2026-34182** m3g Risk Puanı **22**/100

CMS AuthEnvelopedData ayrıştırma zafiyeti

Ürün: CMS AuthEnvelopedData (kriptografi yığını) **Tür:** RCE **MS Önem:** Critical **CVSS:** Yayınlanmadı

KİMLİK DOĞRULAMASI GEREKMİYOR | KULLANICI ETKİLEŞİMİ GEREKMİYOR

ETKİ

Şifreli/imzalı mesaj yapılarının ayrıştırılmasında kritik hata; S/MIME e-posta ve sertifika işleyen servisleri etkiler.

GİDERME (REMEDİATİON)

Windows kümülatif güncellemesi.

AZALTIM (MİTİGATİON)

Yayınlanmış workaround yok.

Kaynak: BleepingComputer

#24 **CVE-2026-72986 / CVE-2026-73018** m3g Risk Puanı **22**/100

Graphic Fonts uzaktan kod çalıştırma (2 CVE)

Ürün: Windows Graphic Fonts **Tür:** RCE **MS Önem:** Critical **CVSS:** Yayınlanmadı

KİMLİK DOĞRULAMASI GEREKMİYOR | KULLANICI ETKİLEŞİMİ GEREKMİYOR

ETKİ

Font ayrıştırma bileşenindeki hata; belge, web sayfası veya e-posta içeriğiyle tetiklenebilir ve tarihsel olarak bu sınıf zafiyetler hızla silahlandırılır.

GİDERME (REMEDİATİON)

Windows kümülatif güncellemesi.

AZALTIM (MİTİGATİON)

Web ve e-posta içeriğinin ağ geçidinde taranması; ASR kuralları.

Kaynak: BleepingComputer

#25 **CVE-2026-69603 / CVE-2026-80083** m3g Risk Puanı **14**/100

Hyper-V guest-to-host kaçış (2 CVE)

Ürün: Windows Hyper-V **Tür:** RCE **MS Önem:** Critical **CVSS:** 8.8

KULLANICI ETKİLEŞİMİ GEREKMİYOR

ETKİ

Misafir sanal makine içindeki bir saldırgan host üzerinde kod çalıştırabilir. Çok kiracılı (multi-tenant) ve hosting ortamlarında izolasyon sınırının kırılması anlamına gelir; tek VM'in ele geçirilmesi tüm host'u ve üzerindeki diğer VM'leri riske atar.

GİDERME (REMEDİATİON)

Hyper-V host'larını planlı olarak yamalayın; cluster'larda live migration ile kesintisiz rolling update yapın.

AZALTIM (MİTİGATİON)

Telafi edici kontrol: Güvenilmeyen kiracı VM'lerini ayrı host'larda toplayın, gereksiz entegrasyon servislerini ve cihaz geçişlerini (device passthrough) kapatın.

Kaynak: CrowdStrike

#26 **CVE-2026-58599** m3g Risk Puanı **9**/100

HEVC Video Extensions uzaktan kod çalıştırma (heap taşması)

Ürün: HEVC Video Extensions / Windows Codecs Library **Tür:** RCE **MS Önem:** Critical **CVSS:** Yayınlanmadı

ETKİ

Hazırlanmış video dosyasının açılması/önizlenmesiyle kod çalıştırma. Store üzerinden güncellenen bir bileşendir; WSUS/SCCM ile dağıtılmadığı için kolayca gözden kaçar.

GİDERME (REMEDİATİON)

Microsoft Store uygulama güncellemelerinin istemcilerde etkin olduğunu doğrulayın (kapalı ortamlarda ayrı dağıtım gerekir).

AZALTIM (MİTİGATİON)

Kullanılmayan medya eklentilerini kaldırın.

Kaynak: Qualys

#27 **CVE-2026-69518** m3g Risk Puanı **9**/100

Remote Desktop pano (clipboard) üzerinden kod çalıştırma

Ürün: Remote Desktop Client **Tür:** RCE **MS Önem:** Important **CVSS:** 8.8

ETKİ

Kötü amaçlı bir RDP sunucusuna bağlanan istemcide, pano yönlendirmesi üzerinden kod çalıştırma. Yönetici iş istasyonları için kritik.

GİDERME (REMEDİATİON)

İstemci kümülatif güncellemesi.

AZALTIM (MİTİGATİON)

RDP profillerinde pano ve sürücü yönlendirmesini kapatın; yalnızca bilinen RDP hedeflerine bağlanmayı GPO ile kısıtlayın.

Kaynak: CrowdStrike

#28 **CVE-2026-69830** m3g Risk Puanı **9**/100

Windows Shell uzaktan kod çalıştırma (heap taşması)

Ürün: Windows Shell **Tür:** RCE **MS Önem:** Critical **CVSS:** Yayınlanmadı

ETKİ

Explorer/Shell bileşeni üzerinden, hazırlanmış dosya veya kısayolla kod çalıştırma.

GİDERME (REMEDİATİON)

Windows kümülatif güncellemesi.

AZALTIM (MİTİGATİON)

Dosya indirme politikaları, SmartScreen/MoTW zorlaması.

Kaynak: Qualys

#29 **CVE-2026-77504** m3g Risk Puanı **9**/100

Word uzaktan kod çalıştırma (double-free)

Ürün: Microsoft Word **Tür:** RCE **MS Önem:** Critical **CVSS:** Yayınlanmadı

ETKİ

Hazırlanmış bir belgenin açılmasıyla kullanıcı bağlamında kod çalıştırma.

GİDERME (REMEDİATİON)

Office / M365 Apps güncellemesi.

AZALTIM (MİTİGATİON)

Protected View, ASR kuralları, makro politikası.

Kaynak: Qualys

#30 **CVE-2026-81948 … CVE-2026-81951** m3g Risk Puanı **9**/100

Excel uzaktan kod çalıştırma – 4 adet heap taşması

Ürün: Microsoft Excel **Tür:** RCE **MS Önem:** Critical **CVSS:** Yayınlanmadı

ETKİ

Hazırlanmış çalışma kitaplarının açılmasıyla kod çalıştırma; finans/muhasebe kullanıcıları tipik hedef.

GİDERME (REMEDİATİON)

Office / M365 Apps güncellemesi.

AZALTIM (MİTİGATİON)

Protected View, internetten gelen dosyalarda makroların engellenmesi, ek filtreleme.

Kaynak: Qualys

P4 – ORTA-YÜKSEK (test + 30 gün)

5 kayıt

On-prem sunucu uygulamaları (Exchange, SharePoint, SQL Server). Uygulama uyumluluk testi ve planlı kesinti gerektirir.

#31 CVE-2026-55007

m3g Risk Puanı **28**/100

Exchange Server kimlik doğrulaması gerektirmeyen uzaktan kod çalıştırma (Visio eki)

Ürün: Microsoft Exchange Server (on-prem) **Tür:** RCE **MS Önem:** Critical **CVSS:** 8.1

KİMLİK DOĞRULAMASI GEREKMİYOR | İNTERNETE AÇIK YÜZEY | KULLANICI ETKİLEŞİMİ GEREKMİYOR

ETKİ

Uzaktaki kimliği doğrulanmamış bir saldırgan, kötü amaçlı bir Visio eki üzerinden Exchange sunucusunda kod çalıştırabilir. ZDI 'istismar güvenilir olmayabilir, ancak saldırganın bir kez tutturması yeterli' diyor. Exchange AD'ye yüksek yetkiyle bağlı olduğu için etki domain seviyesine taşınabilir.

GİDERME (REMEDİATİON)

On-prem Exchange sunucularında planlı kesinti alın ve Eylül 2026 Security Update'i uygulayın. Exchange yamaları servis kesintisi gerektirir – bakım penceresi şart.

AZALTIM (MİTİGATİON)

Telafi edici kontrol: Visio (.vsd/.vsdx/.vsdm) eklerini Exchange Transport Rule ile geçici olarak engelleyin, OWA/ECP'yi internetten kısıtlayın, Exchange Emergency Mitigation Service'in (EEMS) açık olduğunu doğrulayın.

Kaynak: ZDI

#32 CVE-2026-69465

m3g Risk Puanı **25**/100

SharePoint Server uzaktan kod çalıştırma (güvenlik kontrolü atlatma)

Ürün: Microsoft SharePoint Server **Tür:** RCE **MS Önem:** Critical **CVSS:** 8.8

İNTERNETE AÇIK YÜZEY | KULLANICI ETKİLEŞİMİ GEREKMİYOR | İSTİSMAR DAHA OLASI

ETKİ

Kimliği doğrulanmış bir kullanıcı güvenlik kontrollerini atlayıp saldırgan kontrolündeki kodu sunucuya yükleyip çalıştırabilir. SharePoint 2025 yazında aktif istismar edilen bir zafiyet zincirine sahne olmuştu; internete açık SharePoint farm'ları yüksek risk taşıyor. Bu ay toplam 17 SharePoint CVE'sinden 4'ü RCE.

GİDERME (REMEDİATİON)

İnternete açık SharePoint farm'larını en geç 7 gün içinde test edip yamalayın; ardından PSConfig'i çalıştırmayı unutmayın.

AZALTIM (MİTİGATİON)

Telafi edici kontrol: AMSI entegrasyonunu etkin tutun, SharePoint'i WAF arkasına alın, dış paylaşımı ve anonim erişimi kapatın.

Kaynak: ZDI; SecurityAffairs

#33 **CVE-2026-69380** m3g Risk Puanı **20**/100

Exchange Server yetkilendirme eksikliği – başkasının posta kutusuna erişim

Ürün: Microsoft Exchange Server (on-prem) **Tür:** EoP **MS Önem:** Important **CVSS:** 8.1

İNTERNETE AÇIK YÜZEY | KULLANICI ETKİLEŞİMİ GEREKMİYOR

ETKİ

Kimliği doğrulanmış herhangi bir kullanıcı, yetkilendirme kontrolü eksikliği nedeniyle başka kullanıcıların posta kutusu içeriğine erişebilir. Veri gizliliği ve KVKK açısından yüksek riskli; iç tehdit senaryosunda doğrudan kullanılabilir.

GİDERME (REMEDİATİON)

Exchange Eylül 2026 Security Update'i uygulayın.

AZALTIM (MİTİGATİON)

Telafi edici kontrol: Posta kutusu erişim denetim kayıtlarını (mailbox auditing) açın ve olağandışı Get-MailboxFolder/EWS Impersonation aktivitesini izleyin.

Kaynak: Tenable; SecurityAffairs

#34 **CVE-2026-65669** m3g Risk Puanı **13**/100

SQL Server yetki yükseltme (SQL Copilot)

Ürün: Microsoft SQL Server (SQL Copilot bileşeni) **Tür:** EoP **MS Önem:** Critical **CVSS:** 9.6

ETKİ

SQL Copilot bileşeni üzerinden, kullanıcı etkileşimi ile veritabanına kullanıcı yetkisi seviyesinde erişim ve yetki yükseltme. Bu ay 60'tan fazla SQL Server CVE'si yayınlandı.

GİDERME (REMEDİATİON)

SQL Server yamaları uygulama uyumluluğu testi gerektirir: önce test/UAT ortamı, ardından 30 gün içinde üretim. Always On yapılarında rolling update planlayın.

AZALTIM (MİTİGATİON)

Telafi edici kontrol: SQL Copilot özelliği kullanılmıyorsa kapatın, en az yetki ilkesini uygulayın, sysadmin üyeliklerini gözden geçirin.

Kaynak: ZDI; CrowdStrike

#35 **CVE-2026-67631 / 67643 / 67378 / 67636** m3g Risk Puanı **9**/100

SQL Server uzaktan kod çalıştırma (4 CVE, CVSS 8.5–8.8)

Ürün: Microsoft SQL Server **Tür:** RCE **MS Önem:** Critical **CVSS:** 8.8

ETKİ

SQL Server üzerinde kod çalıştırma; veri tabanı sunucusunun ele geçirilmesi veri sızdırma ve fidye senaryolarının merkezidir.

GİDERME (REMEDİATİON)

SQL Server CU/GDR paketlerini test edip 30 gün içinde uygulayın.

AZALTIM (MİTİGATİON)

Telafi edici kontrol: SQL sunucularını ayrı segmentte tutun, xp_cmdshell ve CLR'ı kapatın, TDS portunu yalnızca uygulama sunucularına açın.

Kaynak: CrowdStrike

P5 – BİLGİLENDİRME / DÜŞÜK AKSİYON

6 kayıt

Microsoft tarafından servis tarafında düzeltilen bulut zafiyetleri ve mobil/uygulama bağımlılığı güncellemeleri.

#36 **CVE-2026-69854** m3g Risk Puanı **19**/100

Spring Cloud Azure yetki yükseltme

Ürün: Spring Cloud Azure **Tür:** EoP **MS Önem:** Critical **CVSS:** 9.0

İNTERNETE AÇIK YÜZEY

ETKİ

Azure'a bağlanan Java/Spring uygulamalarında yetki yükseltme; uygulama kimlik bilgilerinin kötüye kullanımına yol açabilir.

GİDERME (REMEDİATİON)

Uygulama bağımlılıklarını güncelleyin (kod tarafı aksiyon gerektirir – geliştirme ekibine iletilmeli).

AZALTIM (MİTİGATİON)

Managed Identity kullanımı, secret rotasyonu.

Kaynak: CrowdStrike

#37 **CVE-2026-69857** m3g Risk Puanı **15**/100

Azure Cosmos DB kritik zafiyeti

Ürün: Azure Cosmos DB **Tür:** EoP **MS Önem:** Critical **CVSS:** Yayınlanmadı

İNTERNETE AÇIK YÜZEY

ETKİ

Cosmos DB servisinde kritik zafiyet.

GİDERME (REMEDİATİON)

Servis tarafında düzeltildi; müşteri aksiyonu gerekmez.

AZALTIM (MİTİGATİON)

Veri tabanı erişim anahtarlarını rotasyona alın, RBAC kullanın.

Kaynak: BleepingComputer

#38 **CVE-2026-70352** m3g Risk Puanı **15**/100

Azure AI Language kritik zafiyeti

Ürün: Azure AI Language **Tür:** RCE **MS Önem:** Critical **CVSS:** Yayınlanmadı

İNTERNETE AÇIK YÜZEY

ETKİ

Azure AI Language servisinde kritik zafiyet.

GİDERME (REMEDİATİON)

Servis tarafında düzeltildi; müşteri aksiyonu gerekmez.

AZALTIM (MİTİGATİON)

—

Kaynak: BleepingComputer

#39 **CVE-2026-80098** m3g Risk Puanı **15**/100

Copilot Studio kritik zafiyeti

Ürün: Microsoft Copilot Studio **Tür:** RCE **MS Önem:** Critical **CVSS:** Yayınlanmadı

İNTERNETE AÇIK YÜZEY

ETKİ

Copilot Studio servisinde kritik zafiyet; kurumsal veri kaynaklarına bağlı ajanlar etkilenebilir.

GİDERME (REMEDİATİON)

Servis tarafında düzeltildi; müşteri aksiyonu gerekmez.

AZALTIM (MİTİGATİON)

Ajan bağlantılarını ve veri kaynağı izinlerini gözden geçirin.

Kaynak: BleepingComputer

#40 **CVE-2026-83941** m3g Risk Puanı **15**/100

Entra ID kritik zafiyeti

Ürün: Microsoft Entra ID **Tür:** EoP **MS Önem:** Critical **CVSS:** Yayınlanmadı

İNTERNETE AÇIK YÜZEY

ETKİ

Bulut kimlik sağlayıcısında kritik seviyeli zafiyet; kiracı genelinde kimlik riski.

GİDERME (REMEDİATİON)

Microsoft tarafından servis tarafında düzeltildi – müşteri aksiyonu gerekmez; yine de kiracı denetim kayıtlarını ve ayrıcalıklı rol atamalarını gözden geçirin.

AZALTIM (MİTİGATİON)

Conditional Access, MFA ve Privileged Identity Management (PIM) kontrollerini doğrulayın.

Kaynak: BleepingComputer

#41 **CVE-2026-80097** m3g Risk Puanı **9**/100

Microsoft Authenticator yetki yükseltme

Ürün: Microsoft Authenticator (Android) **Tür:** EoP **MS Önem:** Important **CVSS:** 8.6

ETKİ

Kötü amaçlı bir Android uygulamasının kurulması ve kullanıcının kimlik doğrulamayı tamamlaması koşuluyla yetki yükseltme. MFA uygulamasını hedef aldığı için kimlik güvenliği açısından dikkat çekici.

GİDERME (REMEDİATİON)

Kullanıcılara Authenticator uygulamasını Play Store üzerinden güncellemelerini duyurun; MDM ile minimum sürüm zorlayın.

AZALTIM (MİTİGATİON)

Yalnızca yönetilen uygulama katalogundan kurulum, bilinmeyen kaynaklardan kurulumun engellenmesi.

Kaynak: ZDI

6. Uygulama Planı

1. **Saat 0–48: P1 zafiyetleri.** Tüm Windows istemci ve sunucularına Eylül kümülatif güncellemesini uygulayın (CVE-2026-81963, CVE-2026-85880). CISA KEV son tarihi 22 Eylül 2026. Bu adımda bakım penceresi beklenmez.
2. **İlk bakım penceresi (48–72 saat): kimlik ve ağ altyapısı.** Sırayla: Domain Controller'lar (DNS, Netlogon, Active Directory, Kerberos) → DHCP sunucuları → RRAS/SSTP VPN uç noktaları → dosya sunucuları (SMB, NFS) → RDS/RD Gateway. RDS yamalarında 14 Eylül OOB güncellemesini **aynı pencerede** uygulayın.
3. **İlk 7 gün: istemci filosu ve Office.** Windows istemci kümülatifi + Microsoft 365 Apps / Office güncellemeleri. Önizleme Bölmesi ile tetiklenebilen 12 Critical zafiyet bu adımda kapanır. Yama tamamlanana kadar Önizleme Bölmesini kapatmayı değerlendirin.
4. **İlk 7 gün: internete açık sunucu uygulamaları.** On-prem Exchange (planlı kesinti gerekir) ve internete açık SharePoint farm'ları. SharePoint'te yamadan sonra PSConfig çalıştırmayı unutmayın.
5. **7–30 gün: uygulama uyumluluğu gerektirenler.** SQL Server CU/GDR paketleri (60+ CVE) ve Hyper-V host'ları. Önce test/UAT, ardından üretimde rolling update.
6. **Sürekli: doğrulama ve raporlama.** Yama uyum oranını WSUS / Intune / SCCM üzerinden raporlayın, başarısız cihazları listeleyin ve bulgu listesini yeniden tarayın.

Yayınlanan güncelleme paketleri (8 Eylül 2026)

İŞLETİM SİSTEMİ	KB	YENİ DERLEME
Windows 11 24H2 / 25H2	KB5124008	26100.9445 / 26200.9445
Windows 11 26H1	KB5124012	28000.2954
Windows 11 23H2	KB5122880	22621.7582
Windows 10 21H2 / 22H2 (ESU)	KB5122878	—
Windows Server 2025	KB5122871	26100.33438

Windows Server 2022 ve 2019 için Eylül kümülatif güncellemeleri de aynı gün yayınlanmıştır; ortamınızdaki sürümler için MSRC portalını referans alın.

Doğrulama adımları

```
# Kurulu güncellemenin doğrulanması
Get-HotFix | Sort-Object InstalledOn -Descending | Select-Object -First 5

# İşletim sistemi derleme numarasının kontrolü (yukarıdaki tabloyla karşılaştırın)
[System.Environment]::OSVersion.Version
(Get-ItemProperty 'HKLM:\SOFTWARE\Microsoft\Windows NT\CurrentVersion').UBR

# Riskli servislerin çalışıp çalışmadığının tespiti (MSMQ / NFS / ICS / RRAS / SSTP)
Get-Service MSMQ,NfsServer,SharedAccess,RemoteAccess -ErrorAction SilentlyContinue |
  Select-Object Name,Status,StartType
```

7. Bilinen Sorunlar ve Bant Dışı (OOB) Güncellemeler

Remote Desktop Services kesintileri — 14 Eylül 2026 bant dışı düzeltmeleri

Eylül 2026 kümülatif güncellemelerinden sonra bazı kurumlarda Remote Desktop Services bağlantı ve oturum açma hataları, sunucuların yanıt vermemesi, MMC ve Dosya Gezgini'nin donması yaşandı. Windows 11 tarafında ayrıca Linux misafir VM'lerde Hyper-V sorunları ve USB Audio Class 1.0 çok kanallı ses problemleri görüldü.

İŞLETİM SİSTEMİ	OOB KB	DÜZELTİLEN SORUNLAR
Windows 11 24H2 / 25H2	KB5129195	RDS + Hyper-V (Linux VM) + USB ses
Windows 11 26H1	KB5129194	RDS + Hyper-V (Linux VM) + USB ses
Windows 10 21H2 / 22H2	KB5129236	RDS
Windows Server 2025	KB5129235	RDS
Windows Server 2022	KB5129237	RDS
Windows Server 2019	KB5129238	RDS

Yamayı kaldırmak çözüm değildir

Microsoft kalıcı düzeltmeden önce Group Policy tabanlı azaltımlar yayınlamıştı. Eylül güvenlik güncellemesini kaldırmak sorunu çözüyordu ancak kritik güvenlik korumalarını da geri alıyordu – ÖNERİLMEZ.

WSUS senkronizasyon hata detayları görünmüyor

KB5070881 ve sonrasında WSUS, CVE-2025-59287'nin giderilmesi kapsamında senkronizasyon hata detaylarını göstermiyor. Bu beklenen bir davranıştır; WSUS kullanan müşterilerde yama dağıtım sorunları teşhis edilirken bu durum göz önünde bulundurulmalıdır.

8. Yama Kapsamı Dışındaki Risk: ShieldCrash

Microsoft Defender — ShieldBreak (CVE-2026-69414) yama atlatması

Eylül Patch Tuesday'in ardından, Microsoft Defender'daki 'ShieldBreak' (CVE-2026-69414) zafiyeti için yayınlanan yamanın belirli koşullarda atlatılabildiğini gösteren bir PoC kamuya açıldı. Araştırmacıya göre tam güncel Windows 10, Windows 11 ve Windows Server sistemlerinde aynı sorun yeniden tetiklenebiliyor ve SYSTEM erişimi elde edilebiliyor.

Durum: ShieldCrash için ayrı bir CVE atanmadı ve rapor tarihi itibarıyla yayınlanmış bir yama veya resmi Microsoft azaltımı bulunmuyor. Microsoft konuya ilişkin kamuya açık bir açıklama yapmadı.

Önerilen aksiyon: Eylül yamalarını eksiksiz uygulayın (ShieldBreak yaması yine de gereklidir), Microsoft güvenlik duyurularını Ekim Patch Tuesday'e kadar günlük takip edin, Defender bileşenlerine yönelik yerel yetki yükseltme denemelerini EDR ile izlemeye alın ve son kullanıcılarda yerel yönetici hakkını kaldırın.

9. Aynı Gün Yayınlanan Üçüncü Taraf Güncellemeleri

Microsoft ile aynı gün Adobe 10 bültende 172 CVE yayınladı; 50'si Critical. Microsoft ortamıyla birlikte yönetilen sunucularda bu bültenler de değerlendirilmelidir.

BÜLTEN	ÜRÜN	DEĞERLENDİRME
APSB26-146	Adobe Commerce / Magento	Öncelik 1 – AKTİF İSTİSMAR. CVE-2026-75650 (CVSS 10.0) şablon motoru enjeksiyonu, 7 Eylül'de bant dışı yayınlandı. E-ticaret müşterilerinde acil.
APSB26-142	Campaign Classic	Öncelik 1
APSB26-119	ColdFusion	Öncelik 1 – 9 CVE
APSB26-141	Acrobat / Reader	Öncelik 2 – 32 CVE, kod çalıştırma dahil

10. Kaynaklar

1. Microsoft Security Response Center – September 2026 Security Updates (2026-Sep)
   https://msrc.microsoft.com/update-guide/releaseNote/2026-Sep
2. Zero Day Initiative – The September 2026 Security Update Review
   https://www.zerodayinitiative.com/blog/2026/9/8/the-september-2026-security-update-review
3. Tenable – Microsoft's September 2026 Patch Tuesday Addresses 964 CVEs
   https://www.tenable.com/blog/microsofts-september-2026-patch-tuesday-addresses-964-cves-cve-2026-81963-cve-2026-85880
4. BleepingComputer – Microsoft September 2026 Patch Tuesday fixes 966 flaws, 2 zero-days
   https://www.bleepingcomputer.com/news/microsoft/microsoft-september-2026-patch-tuesday-fixes-966-flaws-2-zero-days/
5. CrowdStrike – September 2026 Patch Tuesday: Updates and Analysis
   https://www.crowdstrike.com/en-us/blog/patch-tuesday-analysis-september-2026/
6. Qualys – Microsoft and Adobe Patch Tuesday, September 2026 Security Update Review
   https://blog.qualys.com/vulnerabilities-threat-research/2026/09/08/microsoft-patch-tuesday-september-2026-security-update-review
7. SecurityAffairs – Microsoft's Biggest Patch Tuesday: 974 CVEs, 2 Zero-Days and 20 Wormable Bugs
   https://securityaffairs.com/198705/security/microsofts-biggest-patch-tuesday-974-cves-2-zero-days-and-20-wormable-bugs.html
8. CISA – Known Exploited Vulnerabilities Catalog (08.09.2026 eklemeleri)
   https://www.cisa.gov/news-events/alerts/2026/09/08/cisa-adds-four-known-exploited-vulnerabilities-catalog
9. Microsoft Support – KB5122871 (Windows Server 2025, 8 Eylül 2026)
   https://support.microsoft.com/en-us/servicing/os/windows-server/2026/09/kb5122871-windows-server-2025-security-update
10. Microsoft Support – KB5129235 (Windows Server 2025 OOB, 14 Eylül 2026)
    https://support.microsoft.com/en-us/servicing/os/windows-server/2026/09/kb5129235-windows-server-2025-update
11. BleepingComputer – Microsoft releases emergency Windows updates to fix RDS failures
    https://www.bleepingcomputer.com/news/microsoft/microsoft-releases-emergency-windows-updates-to-fix-rds-failures/
12. BleepingComputer – New Microsoft Defender 'ShieldCrash' zero-day grants SYSTEM access
    https://www.bleepingcomputer.com/news/security/new-microsoft-defender-shieldcrash-zero-day-grants-system-access/

11. Kapsam ve Sorumluluk Notu

Kapsam. Bu rapor 8 Eylül 2026 (Salı) tarihli Microsoft güvenlik güncellemelerini (2026-Sep) konu alır ve 21 Eylül 2026 itibarıyla kamuya açık bilgilere dayanır. 972 CVE'nin tamamının satır satır dökümü değildir; operasyonel olarak öne çıkan 41 kayıt önceliklendirilerek sunulmuştur. Tam liste MSRC portalından alınabilir.

Puanlama. “m3g Risk Puanı” m3g'ye ait bir önceliklendirme modelidir; CVSS veya Microsoft tarafından yayınlanan resmî bir değer değildir. CVSS puanları kaynak yayınlardan alınmıştır ve Microsoft skor yayınlamadığı durumlarda “Yayınlanmadı” olarak işaretlenmiştir.

Azaltımlar. “Telafi edici kontrol (m3g önerisi)” olarak işaretlenen maddeler Microsoft'un resmî geçici çözümleri değildir; yama uygulanana kadar riski düşürmeye yönelik genel sıkılaştırma önerileridir. Uygulanmadan önce ortamınızda etki analizi yapılmalıdır.

Öncelik sıralaması ortama göre değişir. Bu sıralama genel bir kurumsal Windows/Active Directory ortamı varsayımıyla yapılmıştır. Ortamınızda ilgili rol kurulu değilse (ör. NFS, MSMQ, Skype for Business) o kaydın önceliği düşer; internete açık yüzeyiniz genişse yükselir. m3g olarak talebiniz üzerine bu raporu envanterinize göre yeniden önceliklendirebiliriz.