

Recordbrekende patchronde, Copilot-reboot en naderende Windows-deadline

Editie 17-09-2026 t/m 01-10-2026

September 2026 was een drukke maand in het Microsoft-universum: de grootste Patch Tuesday ooit, een ingrijpende herpositionering van Copilot als zakelijk platform én een naderende ondersteuningsdeadline voor Windows 11. In deze editie zetten wij de belangrijkste ontwikkelingen voor u op een rij en leggen wij uit wat dit in de praktijk voor uw organisatie betekent.

Windows

September-beveiligingsupdate uitgerold — noodherstelupdate snel gevolgd

Op 8 september 2026 bracht Microsoft de maandelijkse beveiligingsupdate uit voor alle ondersteunde versies van Windows. De update was omvangrijker dan normaal: zij bevatte patches voor bijna duizend kwetsbaarheden. Kort daarna bleek echter dat de update op sommige systemen problemen introduceerde: het venster van Windows Verkenner kon na het inloggen zwart blijven, de File History-back-upfunctie herkende geen externe schijven meer en Remote Desktop Services (veelvuldig gebruikt voor thuiswerken en systeembeheer) werkte niet correct. Microsoft reageerde snel met een noodupdate op 14 september (KB5129236/KB5129239) die de Remote Desktop- en Hyper-V-problemen oplost. Eigenaren van HP- en Lenovo-apparaten ondervonden aanvullende problemen als gevolg van de cumulatieve effecten van de augustus- en septemberupdates. Wij hebben deze situatie nauwgezet gevolgd en de juiste updates toegepast binnen ons beheer, zodat uw systemen stabiel en beschermd blijven.

Windows 11 versie 24H2 Home en Pro: ondersteuning stopt op 13 oktober 2026

Microsoft heeft bevestigd dat Windows 11 versie 24H2 in de uitvoeringen Home en Pro (inclusief Pro Education en Pro for Workstations) op 13 oktober 2026 het einde van de ondersteuning bereikt. Na die datum ontvangen apparaten met deze versie geen maandelijkse beveiligingsupdates, bugfixes, tijdzone-correcties of technische ondersteuning meer van Microsoft. Zakelijke uitvoeringen (Enterprise en Education) vallen

onder een andere levenscyclus en behouden ondersteuning tot oktober 2027. De opvolger, Windows 11 versie 25H2, is beschikbaar en is functioneel identiek — de overgang vergt geen volledige herinstallatie. Wij zien toe op een tijdige overgang van alle door ons beheerde apparaten die aan deze deadline raken en bewaken de compatibiliteit vooraf.

Windows 11 versie 25H2: terugkerende taakbalk en vernieuwde Secure Boot-certificaten

De september-preview-update (KB5124010) voor Windows 11 versies 24H2, 25H2 en 26H1 bevat een gebruikersgerichte verbetering: de taakbalk is in versie 25H2 opnieuw verplaatsbaar, een functie die al sinds Windows 95 bestond maar eerder tijdelijk werd weggehaald. Tegelijkertijd rolt Microsoft vernieuwde Secure Boot-certificaten uit, die gefaseerd worden geïnstalleerd op beheerde en niet-beheerde apparaten nadat zij voldoende stabiele update-signalen hebben doorgegeven. Deze achtergrondwijziging versterkt de beveiligde opstart van Windows-apparaten zonder zichtbare gevolgen voor het dagelijks gebruik. Wij monitoren de uitrol hiervan binnen ons beheer.

Microsoft 365

Outlook krijgt de mogelijkheid om vergaderorganisator over te dragen

Microsoft introduceert een langverwachte functie in Outlook: het overzetten van een vergadering (of een terugkerende reeks) naar een andere organisator binnen dezelfde organisatie, zonder de vergadering te hoeven annuleren en opnieuw aan te maken. De huidige organisator stuurt een overdrachtverzoek, dat de nieuwe organisator eerst moet accepteren voordat de eigendom daadwerkelijk overgaat. Bestaande vergaderbeschrijvingen, bijlagen en gevoeligheidslabels blijven bewaard, en interne deelnemers ontvangen geen nieuwe uitnodiging. In de eerste fase (uitrol wereldwijd van eind september tot eind oktober 2026) worden alleen niet-online vergaderingen ondersteund; Teams-vergaderingen volgen in een latere fase. De functie werkt in de nieuwe Outlook voor Windows, Outlook op het web en de Teams-agenda, maar nog niet in het klassieke Outlook voor Windows. Dit neemt een veelgehoorde frustratie bij functiewisselingen en uitdiensttreding van medewerkers weg.

OneDrive introduceert pay-as-you-go-opslag voor bedrijven

Microsoft voegt een nieuwe, verbruiksgebaseerde opslagoptie toe aan OneDrive voor bedrijven. In plaats van op voorhand een vaste hoeveelheid extra opslagruimte in te kopen, betalen organisaties voortaan alleen voor de opslagruimte die zij werkelijk boven hun inbegrepen quota gebruiken. Dit biedt flexibiliteit voor organisaties waarvan de opslagbehoefte sterk wisselt per afdeling of seizoen. De functie wordt gefaseerd uitgerold en is beschikbaar voor Microsoft 365-abonnementen met OneDrive for Business. Wij volgen de beschikbaarheid van deze optie en kunnen u informeren wanneer zij voor uw tenant actief is.

Microsoft Purview versterkt gegevensbescherming in Edge for Business

Microsoft Purview krijgt een uitgebreidere inline-gegevensbescherming voor zakelijke apps die worden bereikt via Microsoft Edge for Business. De verbetering integreert Data Loss Prevention (DLP) — het voorkomen van onbedoeld lekken van vertrouwelijke informatie — direct in de browsersessie voor apps die worden beheerd via Microsoft Entra (het identiteitsplatform). Dat betekent dat gevoelige informatie beter wordt afgeschermd, ook wanneer medewerkers werken in webbased zakelijke applicaties. Voor organisaties die al gebruikmaken van Purview-beleid, wordt de bescherming automatisch uitgebreid. Wij nemen dit mee in ons beheer van uw beveiligingsbeleid.

Copilot & AI

Microsoft lanceert volledig vernieuwd Copilot: Home, Code en Autopilot in één app

Op 25 september 2026 presenteerde Microsoft een ingrijpende herpositionering van Copilot. De consumentenversie en de zakelijke versie worden samengevoegd tot één product dat volledig op zakelijke klanten is gericht. De vernieuwde app bestaat uit drie zones: **Home** (de beginpagina waar chat en taakopdrachten samenkomen, inclusief de volledige functionaliteit van Word, Excel en PowerPoint), **Code** (waarmee ook niet-technische medewerkers eenvoudige automatiseringen en oplossingen kunnen bouwen, aangedreven door dezelfde technologie als GitHub Copilot) en **Autopilot** — voorheen 'Scout' geheten — een persistente digitale assistent die zelfstandig taken blijft uitvoeren, ook wanneer de gebruiker niet actief is. Tegelijkertijd introduceert Microsoft **Copilot Managed Runtime**: een beveiligde hostingomgeving binnen de Microsoft 365-tenant van uw organisatie, waarbinnen gebouwde applicaties kunnen draaien, beheerd door IT. Home en Code starten in het Frontier-programma; Autopilot gaat eind september naar een uitgebreide preview. Dit is de meest significante herpositionering van Copilot tot nu toe en bevestigt Microsofts focus op zakelijke automatisering boven de consumentenmarkt.

Nieuw prijsmodel: vaste licentie voor chat, verbruikskosten voor agentische taken

Parallel aan de functionele vernieuwing introduceert Microsoft een tweeledige prijsstructuur voor Copilot. De bestaande, vaste gebruikerslicentie dekt regulier AI-gebruik zoals chatten en inhoud genereren. Taken die Copilot zelfstandig en meerstapsgewijs uitvoert — zoals het automatisch verwerken van e-mails, beheren van bestanden of uitvoeren van werkstromen — vallen onder een verbruiksmodel op basis van zogenoemde 'Copilot Credits'. Beheerders krijgen daarbij uitgebreide FinOps-mogelijkheden: zij kunnen per gebruikersgroep instellen welke modellen en taakniveaus beschikbaar zijn, drempelwaarschuwingen instellen en verbruiksrapportages raadplegen. Wij volgen deze ontwikkelingen en houden u op de hoogte van de impact op uw licentiekosten zodra de nieuwe mogelijkheden breed beschikbaar worden in uw tenant.

Copilot breidt uit naar SharePoint, OneDrive, mobiel en Teams Phone

Naast de grote herpositionering zijn er in september diverse functie-uitbreidingen beschikbaar gekomen. Copilot in SharePoint en in OneDrive zijn nu algemeen beschikbaar.

In de mobiele Microsoft 365-apps voor Android (Word, Excel en PowerPoint) kunnen gebruikers voortaan ook met Copilot bewerken — een mogelijkheid die eerder al op iOS beschikbaar was. Verder introduceert Microsoft de Teams Phone Agent: een AI-gestuurde telefonische receptionist die bellers naar de juiste persoon of informatie leidt. In PowerPoint kan Copilot langlopende taken nu op de achtergrond afmaken, ook wanneer de gebruiker de applicatie heeft afgesloten of van apparaat is gewisseld. Wij zien erop toe dat deze functies, zodra zij breed beschikbaar zijn, correct zijn geconfigureerd binnen uw Microsoft 365-omgeving.

Kwetsbaarheden & patches

Applicatie	CVE	Risico
Microsoft Windows (Update Stack)	CVE-2026-81963	Actief misbruikt (zero-day)
Microsoft Windows (ALPC)	CVE-2026-85880	Actief misbruikt (zero-day)
Microsoft Outlook	CVE-2026-78509	Kritiek – CVSS 9.8
Google Chrome (V8-engine)	CVE-2026-85046	Actief misbruikt – CISA KEV
Mozilla Firefox	CVE-2026-75874	Hoog – CVSS 10.0 (sandbox-escape)
WinRAR	CVE-2025-8088	Actief misbruikt – CISA KEV (nation-state)
7-Zip	CVE-2026-58052	Gemiddeld – CVSS 4.8 (geen auto-update)

Wij monitoren deze kwetsbaarheden en voeren de benodigde updates uit binnen ons beheer. U hoeft hiervoor zelf geen actie te ondernemen.

Twee actief misbruikte zero-days in Windows — Patch Tuesday september 2026

De september-Patch Tuesday — de grootste in de geschiedenis van Microsoft met bijna duizend gedichte kwetsbaarheden — bevat twee kwetsbaarheden die al actief worden misbruikt voordat de patch beschikbaar was. **CVE-2026-81963** treft de Windows Update Stack: een aanvaller met een lokaal account kan via een fout in de manier waarop de updatecomponent bestandskoppelingen volgt, zichzelf SYSTEM-rechten (de hoogste machtigingen in Windows) toekennen. **CVE-2026-85880** betreft het Advanced Local Procedure Call-mechanisme (ALPC), een kernonderdeel van Windows dat processen onderling laat communiceren, en maakt eveneens ongeautoriseerde bevoegdheidsverhoging mogelijk. Beide kwetsbaarheden staan op de CISA Known Exploited Vulnerabilities-lijst en zijn door Microsoft als prioriteit aangemerkt. Wij hebben deze patches opgenomen in ons patchbeheer en toegepast op de door ons beheerde systemen.

Kritieke Outlook-kwetsbaarheid: schadelijke code via het leesvenster (CVE-2026-78509)

Een van de opvallendste bevindingen van deze Patch Tuesday is **CVE-2026-78509** in Microsoft Outlook, beoordeeld met CVSS 9.8 (kritiek). De kwetsbaarheid stelt een aanvaller in staat om schadelijke code uit te voeren op het systeem van het slachtoffer, zonder dat de ontvanger de e-mail hoeft te openen of op een bijlage hoeft te klikken — het is voldoende dat de e-mail zichtbaar is in het leesvenster van Outlook. Microsoft omschrijft dit als een zogeheten heap-based buffer overflow in de weergave-engine van Outlook. Hoewel Microsoft actief misbruik op dit moment als minder waarschijnlijk beoordeelt, maakt de drempelvrije werking deze kwetsbaarheid bijzonder risicovol voor zakelijke omgevingen waar Outlook voortdurend geopend staat. Wij hebben de bijbehorende Office-updates toegepast als onderdeel van ons reguliere patchbeheer.

Google Chrome zero-day (CVE-2026-85046) — zesde actief misbruikte Chrome-kwetsbaarheid van 2026

Op 3 september 2026 bracht Google een noodupdate uit voor Chrome na bevestiging dat **CVE-2026-85046** al actief werd misbruikt. De kwetsbaarheid, met CVSS-score 8.8 (hoog), zit in V8 — de JavaScript-engine die Chrome gebruikt om nagenoeg elke webpagina te verwerken. Door een zogeheten type-confusion-fout kan aanvallen via een speciaal geconstrueerde webpagina willekeurige code uitvoeren in de browsersandbox. De Amerikaanse overheidsinstantie CISA plaatste de kwetsbaarheid direct op de Known Exploited Vulnerabilities-lijst en stelde een patchdeadline van 18 september 2026. Het betreft de zesde actief misbruikte Chrome zero-day van dit jaar. De gepatchte versie is Chrome 152.0.7977.82 of hoger. Omdat Chrome automatisch bijwerkt zodra de browser opnieuw wordt gestart, hebben wij dit bewaakt en gecontroleerd binnen ons beheer.

Firefox 156 sluit meerdere hoge kwetsbaarheden, waaronder sandbox-escapes

Op 15 september 2026 bracht Mozilla Firefox versie 156 en ESR 153.3 uit, met fixes voor tientallen kwetsbaarheden. De ernstigste — **CVE-2026-75874** met een maximale CVSS-score van 10.0 — betreft een sandbox-escape in de Remote Settings Client-component: een aanvaller zou theoretisch buiten de beveiligde browseromgeving kunnen opereren. Andere opvallende kwetsbaarheden betreffen use-after-free-fouten in de JavaScript-engine (CVE-2026-84118), de audio/video-component (CVE-2026-84120) en het navigatieonderdeel (CVE-2026-84119), die eveneens sandbox-escapes of code-uitvoering mogelijk maken. Er zijn geen meldingen van actief misbruik van de Firefox-kwetsbaarheden in het wild. Wij verwerken deze updates in ons patchbeheer voor systemen waarop Firefox wordt gebruikt.

WinRAR en 7-Zip: kwetsbaarheden zonder automatische update blijven risico

WinRAR blijft hoog op de kwetsbaarheidsslijst staan: **CVE-2025-8088** (CVSS 8.4), een pad-traversal-fout waarbij een speciaal aangemaakt archief bij het openen automatisch een bestand naar de Windows-opstartmap schrijft — waarna de schadelijke code bij de eerstvolgende aanmelding wordt uitgevoerd, zonder verdere interactie van de gebruiker. De fix bestaat al ruim veertien maanden (WinRAR 7.13), maar omdat WinRAR geen

automatische updatefunctie heeft, draaien wereldwijd nog honderden miljoenen installaties de kwetsbare versie. Staatsgesponsorde aanvalsgroepen maken actief misbruik van deze kwetsbaarheid. Voor 7-Zip geldt **CVE-2026-58052**: een Mark-of-the-Web-bypass in het verwerken van RAR5-archieven, waarbij de beveiligingswaarschuwing die Windows normaal toont voor bestanden van internet, stilzwijgend wordt uitgeschakeld. Dit is opgelost in 7-Zip versie 26.03 (begin september 2026), maar ook 7-Zip heeft geen automatische update. Wij zien er binnen ons beheer op toe dat de actuele versies van deze archiefprogramma's zijn geïnstalleerd.

Vragen over een van deze onderwerpen of hulp nodig bij de implementatie?

Neem contact op met support@netmask.nl • www.netmask.nl

© 2026 Netmask. U ontvangt deze nieuwsbrief als klant van Netmask.