

Windows 26H2, Copilot-doorbraken & kritieke patches

Editie 29-09-2026 t/m 13-10-2026

De afgelopen twee weken stonden in het teken van grote veranderingen: Microsoft bracht de nieuwe Windows 11-versie 26H2 uit, terwijl tegelijkertijd versie 24H2 het einde van zijn levenscyclus bereikt. Daarnaast introduceerde Microsoft ingrijpende vernieuwingen in Copilot en Microsoft 365, en werden er buiten het vaste patchritme urgente beveiligingsupdates uitgebracht voor Exchange Server en TeamViewer. In deze editie leest u de belangrijkste ontwikkelingen op een rij.

Windows

Windows 11 versie 26H2 is nu beschikbaar

Microsoft rolt de Windows 11 2026 Update (versie 26H2) geleidelijk uit naar compatibele apparaten. Het gaat om een relatief kleine update die geen volledige herinstallatie vereist als een apparaat al draait op versie 25H2 of 24H2. De update bevat onder andere verbeterde zoekfunctionaliteit in Windows: een nieuwe instelling bepaalt of web- en Store-suggesties naast lokale zoekresultaten worden getoond, en Windows indexeert voortaan automatisch de meest gebruikte mappen voor snellere zoekresultaten. Verder zijn er verbeterde voortgangsindicatoren bij opstarten, aanmelden en updates. Wij nemen deze upgrade mee in ons beheerproces, zodat uw apparaten op het juiste moment en op een zorgvuldige manier worden bijgewerkt.

October Patch Tuesday: nieuwe functies én einde ondersteuning 24H2

De maandelijkse beveiligingsupdate van 13 oktober (Patch Tuesday) brengt naast beveiligingsfixes ook diverse verbeteringen mee. Zo introduceert Microsoft een nieuwe functie waarmee u kunt instellen dat apps altijd gemaximaliseerd openen, en ontvangt Verkenner nuttige verbeteringen. Verder voegt Microsoft een nieuwe Tips-widget toe en kan de Windows-herstelomgeving (WinRE) eerder opgeslagen Wi-Fi-profielen hergebruiken. Tegelijk is dit een historisch moment: Windows 11 versie 24H2 Home en Pro bereiken op 13 oktober 2026 het einde van de ondersteuning, waarna Microsoft stopt met het leveren van beveiligingsupdates, bugfixes en technische ondersteuning. Enterprise- en

Education-edities blijven nog ondersteund tot 12 oktober 2027. Wij zien er binnen ons beheer op toe dat alle apparaten tijdig worden overgezet naar een ondersteunde versie, zodat u zonder onderbrekingen beveiligd blijft.

Einde betaalde beveiliging voor Windows Server 2012 en 2012 R2

Het betaalde Extended Security Updates-programma (ESU) voor Windows Server 2012 loopt op 13 oktober 2026 definitief af — alleen voor volume-gelicenseerde edities. Hetzelfde geldt voor Windows Server 2012 R2: het betaalde ESU-programma bood tot 13 oktober 2026 voortgezette beveiligingsupdates. Na deze datum zijn deze serverversies volledig buiten ondersteuning en ontvangen zij geen enkele beveiligingspatch meer. Mocht uw omgeving nog systemen draaien op deze verouderde versies, dan nemen wij dit met u op in het kader van ons lifecycle-advies.

Microsoft 365

Teams krijgt deepfake-detectie en verbeterd vergaderbeheer

Microsoft Teams introduceert ondersteuning voor externe detectie van synthetische audio en video, waarmee organisaties gecertificeerde deepfake-detectie-oplossingen direct in de vergaderervaring kunnen integreren. Wanneer een detectieoplossing signalen van gemanipuleerd of AI-gegenereerd beeld of geluid vaststelt, toont Teams waarschuwingen aan deelnemers — zodat mogelijke identiteitsfraude tijdig wordt herkend. Aanvullend introduceert Teams ook een centraal dashboard voor beheerders: in het Teams Beheercentrum komt één overzichtspagina voor het monitoren en oplossen van problemen met vergaderingen en gesprekken binnen de organisatie. Beheerders kunnen terugkerende patronen identificeren, problemen onderzoeken en proactief ingrijpen. Dit zijn waardevolle tools voor organisaties die steeds meer via online vergaderingen communiceren met klanten en partners.

Productwijzigingen: Project Online stopt, nieuwe licentievormen

Project Online is op 30 september 2026 definitief buiten gebruik gesteld. De productvoorwaarden per 1 oktober verwijderen geselecteerde Plan 5- en Project Essentials-verwijzingen, maar Microsoft behoudt een migratiebepaling voor Plan 3/5-abonnees en behoudt voor hen toegang tot de premiumfuncties van Planner. Verder heeft Microsoft nieuwe licentiecategorieën geïntroduceerd: per 1 oktober 2026 worden Microsoft 365 Education A7, Microsoft 365 G7 en GCC Agent 365 opgenomen in de beschikbaarheidstabellen. Deze wijzigingen zijn voornamelijk relevant voor overheids- en onderwijsinstellingen. Heeft u vragen over hoe deze wijzigingen uw licentiesituatie raken? Neem dan contact met ons op via support@netmask.nl.

Sterkere aanmeldbeveiliging via passkeys in Microsoft Entra

Gebruikers kunnen voortaan een passkey of wachtwoordloze aanmeldmethode instellen als hun eerste meervoudige verificatiemethode (MFA). De uitrol in Microsoft Entra (voor Worldwide en GCC) start halverwege oktober 2026 en loopt naar verwachting door tot half

november 2026. Een passkey is een moderne, phishing-resistente aanmeldmethode die het traditionele wachtwoord vervangt door een versleutelde sleutel op uw apparaat. Gebruikers die zich aanmelden via Windows Hello for Business of macOS Platform SSO kunnen daarmee voortaan voldoen aan MFA-vereisten zonder een extra passkey te registreren. Wij houden deze uitrol nauwlettend in de gaten en zien toe op een soepele invoering binnen uw omgeving.

Copilot & AI

Copilot in SharePoint en OneDrive nu algemeen beschikbaar

Een van de grootste updates van deze periode is de officiële algemene beschikbaarheid van Copilot in SharePoint. Elke gebruiker kan nu inhoud aanmaken en ordenen, vragen stellen op basis van SharePoint-gegevens, bibliotheken verrijken met AI-gegenereerde metadata en herbruikbare vaardigheden opbouwen. Aanvullende mogelijkheden zijn onder meer het genereren en bewerken van afbeeldingen, AI-gegenereerde site-analyserapporten en vrijwel realtime automatisch aanvullen van metadata. Copilot kan bovendien versiegeschiedenis van bestanden raadplegen en eerdere versies terugzetten via een gewoon gesprek. Dit maakt samenwerken aan documenten in SharePoint een stuk efficiënter en veiliger. Wij zien toe op de correcte beschikbaarheid van deze functies binnen uw Microsoft 365-omgeving.

Nieuw prijsmodel: standaard en verbruiksgestuurd gebruik

Microsoft heeft Copilot opgesplitst in twee factureringsmodellen en de app opgebouwd rondom een nieuw startscherm, een Code-module en een altijdactieve agent genaamd Autopilot — waardoor beheerders nu uitgavenbeleid en toegangsstandaarden moeten vastleggen vóórdat gebruikers dit te zien krijgen. Concreet betekent dit: alledaagse AI-functies (zoals modelkeuze en automatische routing) blijven gedekt door het bestaande Copilot-abonnement, terwijl geavanceerde functies en nieuwe frontiersmodellen via verbruiksgestuurd gebruik (Copilot Credits) worden afgerekend. Dit is een relevante wijziging voor organisaties die actief gebruikmaken van Copilot. Wij informeren u zodra dit voor uw specifieke licentiesituatie concrete gevolgen heeft.

Copilot Notebooks: Office-bewerking en AI-automatisering direct in de werkruimte

De oktober 2026-update voor Copilot Notebooks brengt taakdelegatie, terugkerende automatiseringen, directe Office-bewerking, interactieve rapporten en nieuwe manieren om projectinformatie om te zetten in afgewerkte producten. Microsoft brengt de volledige kracht van Office naar Copilot Notebooks: gebruikers kunnen documenten inline openen en Word-, Excel- en PowerPoint-bestanden direct op het canvas bewerken, of Copilot vragen om inhoud toe te voegen en opmaak aan te passen. Teams kunnen tegelijkertijd samenwerken aan dezelfde bestanden. Copilot voegt ook naadloze integratie van zoeken en chatten toe, alternatief antwoorden genereren en nieuwe beheermogelijkheden voor Copilot-connectoren, plus uitbreidingen voor PowerPoint met aangepaste vaardigheden

en bestandsverwijzingen. Copilot groeit daarmee van een assistent naar een volwaardig samenwerkingsplatform. Wij volgen de uitrol van deze functies op de voet.

Kwetsbaarheden & patches

Applicatie	CVE	Risico
Google Chrome (& Microsoft Edge)	CVE-2026-85046	Actief misbruikt – Zero-day
Adobe Acrobat / Acrobat Reader	CVE-2026-34621	Actief misbruikt – Kritiek (CVSS 9.6)
Microsoft Exchange Server (on-premises)	CVE-2026-96940	Hoog (CVSS 8.8) – Misbruik waarschijnlijk
TeamViewer (Full Client & Host)	CVE-2026-19743 e.a.	Hoog (CVSS 7.8–8.8) – Geen actief misbruik bekend

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

Google Chrome & Microsoft Edge – CVE-2026-85046 (Zero-day, actief misbruikt)

Google heeft Chrome bijgewerkt om een actief misbruikte, ernstige zero-day in de V8-engine te verhelpen, naast elf andere kwetsbaarheden. De uitgebuite kwetsbaarheid, CVE-2026-85046, is een zogenoemde type-confusion-fout. Dat houdt in dat de browser gegevens verkeerd interpreteert, waardoor een aanvaller willekeurige code kan uitvoeren — simpelweg door een kwaadaardige webpagina te bezoeken. De update brengt Chrome naar versie 152.0.7977.82/.83 op Windows en macOS, als onderdeel van een geleidelijke uitrol. Omdat Microsoft Edge op dezelfde Chromium-engine is gebaseerd, geldt deze kwetsbaarheid ook voor Edge. Google heeft niet bekendgemaakt welke organisaties of sectoren het doelwit zijn, maar de actieve uitbuiting maakt snelle actie noodzakelijk. Wij nemen deze update mee in ons patchbeheer voor alle beheerde werkstations.

Adobe Acrobat & Reader – CVE-2026-34621 (Kritiek, actief misbruikt, CISA KEV)

Adobe heeft noodpatches uitgebracht voor een kritieke zero-day in Acrobat en Reader die al gedurende enkele maanden actief werd uitgebuit. De kwetsbaarheid heeft CVE-identificator CVE-2026-34621 en een CVSS-score van 9.6. De kwetsbaarheid heeft een CVSS-score van 8.6 en stelt aanvallers in staat willekeurige code uit te voeren via een kwaadaardig PDF-bestand. Het openen van zo'n bestand volstaat al als trigger, waarna aanvallers systemen kunnen profileren, gegevens kunnen stelen en aanvullende kwaadaardige software kunnen inzetten. De kwetsbaarheid staat op de CISA KEV-lijst (actief misbruikte kwetsbaarheden) sinds 13 april 2026. De correcte versies zijn Acrobat DC en Acrobat Reader DC versie 26.001.21411, en Acrobat 2024 versies 24.001.30362 (Windows) en 24.001.30360 (macOS). Wij hebben deze update al meegenomen in ons patchbeheer voor alle beheerde systemen met Adobe Acrobat.

Microsoft Exchange Server – CVE-2026-96940 (Hoog, noodpatch buiten patchcyclus)

Op 2 oktober 2026 brak Microsoft met zijn vaste patchritme en bracht een speedupdate uit voor Microsoft Exchange Server. De reden: CVE-2026-96940, een kwetsbaarheid voor bevoegdheidsuitbreiding die een geauthenticeerde aanvaller in staat stelt de mailboxen van andere gebruikers binnen dezelfde organisatie te lezen. Microsoft beoordeelde de ernst als CVSS 8.8 (Hoog) en kende — uitzonderlijk — de status "Misbruik waarschijnlijk" toe, ook al zijn er nog geen aanvallen waargenomen. Organisaties met een on-premises Exchange Server 2016, 2019 of Subscription Edition RTM zijn kwetsbaar; klanten van Exchange Online zijn niet getroffen. Wij hebben deze noodpatch direct meegenomen in ons beheer van alle relevante Exchange-omgevingen.

TeamViewer – CVE-2026-19743 e.a. (Vijf kwetsbaarheden, update naar v15.82)

TeamViewer heeft beveiligingsupdates uitgebracht voor vijf ernstige kwetsbaarheden in zijn Full Client, Host en gerelateerde componenten voor Windows, Linux en macOS. De meest ernstige kwetsbaarheid kan aanvallers in staat stellen geconfigureerde beveiliging van remote sessies te omzeilen en mogelijk code uit te voeren op kwetsbare systemen. CVE-2026-19743 betreft een onjuiste padvalidatie in de lokale IPC-service, waardoor een lokaal geauthenticeerde gebruiker met beperkte rechten via aangepaste opdrachten bestanden kan schrijven met verhoogde systeemrechten (NT AUTHORITY/SYSTEM of root). Er is tot nu toe geen actief misbruik bevestigd. TeamViewer meldde op 29 september dat het geen openbaar beschikbare exploitcode of misbruik in het wild heeft vastgesteld. De afwezigheid van bevestigd misbruik neemt het risico echter niet weg, zeker niet voor systemen die gebruikt worden voor bevoorrechte IT-operaties op afstand. Wij nemen de update naar versie 15.82 mee in ons patchbeheer voor alle beheerde systemen waarop TeamViewer is 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.