Cyberdreigingsrapport - 10 maart 2026

Briefing Cyberspace | Digiweerbaar BV

Datum: maandag 10 maart 2026 | Classificatie: TLP:AMBER

1. Patchoverzicht - Directe actie vereist

Product	CVE	CVSS	Actief misbruikt	Actie
Hikvision (diverse modellen)	CVE-2017-7921	10.0	Ja (KEV)	Firmware updaten of apparaat uit dienst nemen
Apple macOS/iOS/iPadOS/Safari	CVE-2023-43000	8.8	Ja (KEV)	Beveiligingsupdates toepassen
Apple iOS/iPadOS	CVE-2023-41974	7.8	Ja (KEV)	Beveiligingsupdates toepassen
Apple tvOS/macOS/Safari/iPadOS/watchOS	CVE-2021-30952	7.8	Ja (KEV)	Beveiligingsupdates toepassen
ExifTool (macOS)	CVE-2026-3102	Hoog	Onbekend	Updaten naar versie 13.50
Nginx UI (alle versies voor 2.3.2)	CVE-2026-27944	9.8	PoC beschikbaar	Upgraden naar versie 2.3.3

Meest urgent voor NL/BE: Hikvision camera's zijn wijdverspreid in Nederland en Belgie. CVE-2017-7921 maakt volledige authenticatie bypass mogelijk. CISA deadline: 26 maart 2026. Organisaties met Hikvision apparatuur moeten onmiddellijk actie ondernemen.

1b. Trending CVE's op Sociale Media

#	CVE	CVSS	EPSS	KEV	Hype
1	CVE-2024-23225	7.8	0,1%	Ja	13
2	CVE-2024-23296	7.8	0,1%	Ja	13
3	CVE-2025-59287	9.8	75,9%	Ja	12
4	CVE-2025-43300	10.0	0,7%	Ja	11
5	CVE-2025-26399	9.8	12,5%	Ja	9

CVE-2025-59287 (Windows Server Update Service, deserialisatie) en CVE-2025-43300 (Apple iOS, out of bounds write met CVSS 10.0) domineren de trending lijst. Beide staan in de KEV catalogus. CVE-2025-26399 (SolarWinds Web Help Desk) komt ook terug in de misbruikte kwetsbaarheden lijst hieronder.

1c. Actief Misbruikte Kwetsbaarheden (CISA KEV / NCSC)

NL/BE Top 5 (NCSC):

#	CVE	Vendor/Product	CVSS	EPSS	NCSC
1	CVE-2026-1731	BeyondTrust Remote Support/PRA	9.8	64,6%	H/H
2	CVE-2026-20127	Cisco Catalyst SD-WAN	10.0	2,6%	H/H
3	CVE-2026-1603	Ivanti EPM	8.6	11,7%	M/H
4	CVE-2022-20775	Cisco SD-WAN CLI	7.8	0,5%	H/H
5	CVE-2026-22719	VMware Aria Operations	8.1	7,4%	M/H

Wereldwijd Top 5 (CISA KEV):

#	CVE	Vendor/Product	CVSS	EPSS	Ransomware
1	CVE-2017-7921	Hikvision (diverse)	10.0	94,3%	Nee
2	CVE-2020-7796	Zimbra Collaboration	9.8	93,5%	Nee
3	CVE-2025-49113	Microsoft Windows	9.9	90,4%	Nee
4	CVE-2021-22054	Omnissa Workspace ONE	7.5	88,9%	Nee
5	CVE-2024-43468	Microsoft SCCM	9.8	85,1%	Nee

CVE-2026-1731 (BeyondTrust) is de enige met een ransomware badge en staat bovenaan zowel de NL/BE als gecombineerde lijst. CVE-2026-20127 (Cisco SD-WAN, CVSS 10.0) verschijnt ook in het patchoverzicht via de Cisco artikelen van afgelopen dagen. Organisaties met Cisco SD-WAN omgevingen moeten met spoed patchen.

2. Datalekken en Incidenten

- Ericsson US - Aanvallers hebben data van werknemers en klanten gestolen via een gehackte serviceprovider. De inbreuk vond plaats tussen 17 en 22 april 2025, maar is pas in maart 2026 gemeld. Blootgestelde data omvat namen, adressen, burgerservicenummers, rijbewijsnummers, financiele informatie en medische gegevens. In Texas zijn 4.377 personen getroffen. Ericsson biedt getroffen personen gratis identiteitsbescherming aan, inclusief een vergoeding tot 1 miljoen dollar bij identiteitsfraude. Geen ransomwaregroep heeft de aanval opgeist. *(Bron: Ericsson, procureur-generaal Californie en Texas)*
- Agencia Tributaria (AEAT), Spanje - Een dreigingsactor heeft persoonlijke gegevens van medewerkers van de Spaanse belastingdienst gelekt op het darkweb. Het lek omvat personeel van alle rangen en leeftijden. De gelekte informatie kan leiden tot intimidatie of gerichte social engineering aanvallen. *(Bron: Cybercrimeinfo darkweb monitoring)*
- Yummy Rides, Venezuela - Een database met circa 30.000 foto's en volledige namen van chauffeurs van de Venezolaanse taxidienst is gratis beschikbaar gesteld op het darkweb. *(Bron: Cybercrimeinfo darkweb monitoring)*

Benelux impact: Het Ericsson incident betreft een supply chain aanval via een serviceprovider, een scenario dat ook Nederlandse en Belgische telecomklanten van Ericsson kan raken. Dit onderstreept het belang van third party risk management conform NIS2 Artikel 21.

3. Dreigingsactoren - Wie is actief

- Russische staatshackers (MIVD/AIVD waarschuwing) - Wereldwijde campagne gericht op Signal- en WhatsApp accounts van overheidsfunctionarissen, militairen en journalisten. Nederlandse overheidsmedewerkers behoren tot de slachtoffers. Aanvalsmethoden omvatten social engineering via nep supportberichten en misbruik van de "gekoppelde apparaten" functie via kwaadaardige QR codes. *(Bron: AIVD/MIVD)*
- Iraanse cyberactoren - Check Point documenteert honderden hackpogingen op consumentencamera's in het Midden-Oosten, getimed rondom Iraanse raketaanvallen op Israel, Qatar en Cyprus. Camera's worden gebruikt voor doelselectie, planning en inspectie van schade. *(Bron: Check Point)*
- Seedworm/MuddyWater (Iran, MOIS) - Actief in netwerken van Amerikaanse organisaties sinds februari 2026, waaronder een bank, luchthaven en defensiegerelateerd softwarebedrijf. Twee nieuwe backdoors ontdekt (Dindoor en Fakeset). *(Bron: Symantec Threat Hunter Team)*
- SHub Stealer operators - Verspreiden macOS malware via nep CleanMyMac website met ClickFix techniek. De malware steelt

wachtwoorden, browserdata, Keychain inhoud en vervangt stilletjes de core bestanden van vijf cryptowallets (Exodus, Atomic, Ledger, Trezor Suite). Russischtalige geofencing suggereert een operator uit het CIS gebied. *(Bron: Malwarebytes)*

- VIP Keylogger operators - Geavanceerde credential stealing campagne met steganografie en in memory executie. Modulair MaaS product dat tientallen browsers, e-mail clients en platforms aanvalt. *(Bron: K7 Security Labs)*

- Rutgers University onderzoekers (ScamAgent) - Publicatie van een AI framework dat aantoont hoe LLM's volledig geautomatiseerde oplichtingsgesprekken kunnen voeren, inclusief omzeiling van veiligheidsfilters via rollenspelcontexten. *(Bron: Rutgers University, arXiv)*

Opvallend: De MIVD/AIVD waarschuwing over Signal- en WhatsApp kapingen door Russische staatshackers is direct relevant voor Nederlandse organisaties. Dit is geen technische aanval op de apps zelf, maar pure social engineering. De combinatie van Russische en Iraanse activiteit toont dat staatshackers actief opereren op meerdere fronten tegelijk.

4. Awareness aandachtspunten - Doorstuurbaar naar teams

- Valse SMS uit naam van MijnOverheid - De Fraudehelpdesk waarschuwt voor berichten per sms die vragen om gegevens bij te werken via een link. Na de sms volgt soms een telefoontje van een "bankmedewerker" die dreigt een wijkagent te sturen. *Advies: klik niet op de link, vul geen gegevens in, maak geen geld over. Bij twijfel bel zelf uw bank of gemeente.*

- Afpersmail dreigt met publicatie op darkweb - Criminelen versturen mails waarin ze beweren persoonlijke gegevens te bezitten en dreigen deze op het darkweb te publiceren tenzij bitcoins worden betaald. De mail kan lijken van uw eigen adres te komen (spoofing). *Advies: beschouw dit als bluf, niet reageren, verwijderen. De mails spelen in op onrust door recente datalekken.* *(Bron: Fraudehelpdesk)*

- Valse AI browserextensies stelen chatgeschiedenissen - Microsoft waarschuwt voor kwaadaardige Chromium extensies die zich voordoen als AI assistenten en bijna 900.000 keer werden geinstalleerd. Ze verzamelen interne code, strategische plannen en bedrijfsinformatie uit AI chatsessies. *Advies: controleer alle browserextensies, verwijder onbekende extensies, blokkeer de domeinen deepaichats[.]com en chatsaigpt[.]com.* *(Bron: Microsoft)*

- Signal en WhatsApp account kaping - Deel nooit verificatiecodes, scan geen onbekende QR codes en negeer berichten die zogenaamd van Signal support afkomstig zijn. Controleer regelmatig uw lijst met gekoppelde apparaten. *Advies: verwijder onbekende gekoppelde apparaten onmiddellijk.* *(Bron: AIVD/MIVD)*

5. Executive Summary - Top 3 kritieke dreigingen

1. Russische staatshackers richten zich op Signal en WhatsApp van Nederlandse overheidsfunctionarissen

De MIVD en AIVD waarschuwen dat Russische hackers actief Signal- en WhatsApp accounts van Nederlandse overheidsmedewerkers, militairen en journalisten proberen over te nemen via social engineering. Dit is een directe bedreiging voor de vertrouwelijkheid van overheidscommunicatie.

- *NIS2 implicatie:* Organisaties in de essentieel en belangrijke categorie moeten hun personeel waarschuwen en de lijst gekoppelde apparaten controleren als onderdeel van incidentrespons (Artikel 21, lid 2c).

- *AVG implicatie:* Gecompromitteerde accounts kunnen leiden tot ongeautoriseerde toegang tot persoonsgegevens in chatgeschiedenissen, wat een meldplicht bij de AP kan triggeren.

2. Hikvision camera's met CVSS 10.0 kwetsbaarheid breed misbruikt

CVE-2017-7921 stelt aanvallers in staat authenticatie volledig te omzeilen op Hikvision camera's, met EPSS 94,3 procent. CISA heeft een deadline van 26 maart 2026 gesteld. Hikvision camera's zijn wijdverbreid in Nederlandse en Belgische bedrijven en overheidsinstellingen.

- *NIS2 implicatie:* IoT apparaten vallen onder de supply chain vereisten van NIS2. Ongepatchte camera's die verbonden zijn met bedrijfsnetwerken vormen een direct risico voor de integriteit van het netwerk.
- *AVG implicatie:* Gecompromitteerde bewakingscamera's kunnen leiden tot ongeautoriseerde toegang tot beeldmateriaal van personen, een verwerking van bijzondere persoonsgegevens.

3. Supply chain risico via macOS malware en valse AI extensies

Twee parallelle campagnes tonen het groeiende risico van supply chain aanvallen. SHub Stealer vervangt core bestanden van cryptowallets en installeert persistente backdoors op macOS. Tegelijkertijd hebben valse AI browserextensies meer dan 20.000 bedrijfsomgevingen gecompromitteerd en bedrijfsinformatie uit AI chatsessies verzameld.

- *NIS2 implicatie:* Beide campagnes onderstrepen de noodzaak van software supply chain beveiliging en endpoint management conform Artikel 21.
- *AVG implicatie:* De verzamelde AI chatgeschiedenissen kunnen persoonsgegevens bevatten die medewerkers met AI tools hebben gedeeld, wat een datalek kan opleveren.

6. Sectorspecifieke Risico's

Sector	Risiconiveau	Dreigingen
Overheid	KRITIEK	Russische staatshackers richten zich op Signal/WhatsApp van overheidsfunctionarissen (MIVD/AIVD)
Telecom	HOOG	Ericsson supply chain datalek, Iraanse MuddyWater actief bij Amerikaanse telecom
Financiele dienstverlening	HOOG	Argenta phishing in Belgie, valse MijnOverheid sms met bankfraude opvolging, MuddyWater bij Amerikaanse bank
Defensie	HOOG	Signal/WhatsApp kaping gericht op militairen, Iran gebruikt bewakingscamera's voor militaire doelselectie
IT/Technologie	VERHOOGD	Valse AI extensies bij 20.000+ bedrijven, ExifTool RCE op macOS, Nginx UI backup lek

7. Operationele Verstoringen

Geen meldingen van operationele verstoringen in veelgebruikte diensten vandaag.

8. Regelgeving en Compliance

- Trump Cyberstrategie - De VS heeft een nieuwe Nationale Cyberstrategie gepresenteerd. Het vier pagina's tellende document focust op offensieve cyberacties en deregulering. National Cyber Director Sean Cairncross noemde specifiek de SEC disclosure rule en de aankomende CIRCIA als regelgeving die moet worden "aangepakt". Dit kan gevolgen hebben voor internationale bedrijven die aan Amerikaanse beurzen genoteerd staan. *(Bron: Recorded Future/The Record)*
- Trump NSA/Cyber Command benoeming - Luitenant-generaal Joshua Rudd passeert een Senaatshorde (68-28) voor de gecombineerde leiding van NSA en Cyber Command. De definitieve stemming wordt dinsdag verwacht. Senator Wyden noemt de benoeming een "vergissing" vanwege gebrek aan ervaring in signaleringsactiviteiten. *(Bron: Recorded Future/The Record)*
- Privacy First vs. Europese digitale identiteit - Stichting Privacy First waarschuwt dat de Europese antiwitwasautoriteit AMLA het gebruik van de Europese digitale identiteit verplicht wil stellen bij banken voor niet fysieke identificatie, in strijd met de eIDAS verordening die vrijwilligheid voorschrijft. Dit is relevant voor financiele instellingen in Nederland die zich voorbereiden op de antiwitwasverordening (halverwege 2027). *(Bron: Privacy First)*

- Kamervragen cloudrisico's - D66, GroenLinks-PvdA en CDA stellen Kamervragen aan minister Van Weel over een rapport dat oorspronkelijk offline was gehaald, over risico's van Amerikaanse cloudoplossingen (Amazon). Hoogleraar Bharosa (TU Delft) stelt dat het rapport te zwaar leunt op aannames over AWS techniek. Minister Van Weel heeft drie weken om te reageren. *(Bron: Security.NL)*

Bronnen: AIVD/MIVD, Check Point, Symantec Threat Hunter Team, Malwarebytes, K7 Security Labs, Microsoft, Fraudehelpdesk, CISA, Kaspersky, Ericsson, Privacy First, Security.NL, Recorded Future/The Record, Rutgers University, Politie.nl

Rapport samengesteld door Digiweerbaar BV