www.CyberSecured.be

WEKELIJKSE CYBERDREIGINGSBRIEFING

Voor Belgische organisaties | Week van 1 maart 2026

KMO's • Ziekenhuizen • Overheden • Non-profits • Grote bedrijven

KRITIEK | HOOG | GEMIDDELD | LAAG

1. Openingsboodschap

Het CCB op woensdag 26 februari drie kritieke waarschuwingen op één dag: Cisco Catalyst SD-WAN (CVSS 10.0, actief uitgebuit), Juniper PTX-routers (CVSS 9.8, noodpatch) en Zyxel-routers (CVSS 9.8). Dit is uitzonderlijk. Het Amerikaanse CISA vaardigt dezelfde dag een Emergency Directive uit voor Cisco SD-WAN — het sterkste noodmechanisme dat de Amerikanen kennen.

En dan is er nog het datalek bij de Franse FICOBA-databank: 1,2 miljoen bankrekeningen blootgesteld via gestolen inloggegevens van één ambtenaar. Geen MFA. Geen drempel. Dat kan ook hier morgen gebeuren.

Dit is een week voor actie, niet voor reflectie. Wie Cisco SD-WAN of Juniper PTX draait: ga nu naar punt 3.Iedereen: kijk of MFA geactiveerd is op al uw kritieke systemen.

2. BE Belgische dreigingen en bevestigde slachtoffers

Geen bevestigde meldingen

Hoewel uit verschillende rapporten blijkt dat Coinbase Cartel beweert dat 2 Belgische bedrijven het slachtoffer zouden zijn van een door hen uitgevoerde ransomware aanval, konden we dit niet onafhankelijk verifiëren. Alle bronnen verwijzen naar de claim die Coinbase Cartel zelf maakt maar dat beschouwen we niet als voldoende betrouwbare informatie.

Identiteitsfraude — Naam Belgische Koning misbruikt

HOOG — Lopende fraude gericht op bedrijfsleiders en overheden

Het CCB en het Federaal Parket waarschuwen voor een lopende zwendelcampagne waarbij criminelen de identiteit misbruiken van Zijne Majesteit de Koning, zijn kabinetschef Vincent Houssiau en Majoor-Generaal Stéphane Dutron (hoofd ADIV). Slachtoffers worden telefonisch, via WhatsApp of per e-mail gecontacteerd met valse betaalverzoeken.

Extra alert voor bedrijfsleiders: valse uitnodigingen voor een fictief galadiner van de Koning Boudewijn Stichting in februari en april 2026 circuleren. Dit is geen echt evenement. Bedragen worden gevraagd als sponsoring of bijdrage.

Impact: identiteitsdiefstal, financiële fraude, reputatieschade bij organisaties die ingaan op de verzoeken.

Bron: CCB — Waarschuwing identiteitsfraude (Belgische Koning)

3. 🔧 Kwetsbaarheden — actie vereist van IT

🟤 NOODGEVAL: Cisco Catalyst SD-WAN — Zero-day uitgebuit sinds 2023 (CVSS 10.0)

Het CCB publiceerde op 26 februari 2026 een kritieke waarschuwing voor CVE-2026-20127, een authenticatie-bypass in Cisco Catalyst SD-WAN Controller (vSmart) en Manager (vManage) met een maximale CVSSv3-score van 10.0. De kwetsbaarheid wordt actief uitgebuit — en dit al minstens sinds 2023, wat betekent dat systemen al jarenlang gecompromitteerd konden zijn zonder dat dit is opgemerkt. CISA vaardigt Emergency Directive ED 26-03 uit. Dit is de zwaarste noodmaatregel voor federale systemen in de VS.

Actief uitgebuite kwetsbaarheden in dit cluster:

- **CVE-2026-20127 (CVSS 10.0):** Authenticatie-bypass — ongeauthenticeerde aanvaller verkrijgt beheerdersrechten op SD-WAN Controller/Manager.
- **CVE-2022-20775 (CVSS hoog):** Path traversal / privilege escalation — gecombineerd met CVE-2026-20127 voor volledige root-toegang.
- **CVE-2026-20126 (CVSS 8.8):** Lokale privilege escalation in SD-WAN Manager voor geverifieerde gebruikers.

Actie: Patch onmiddellijk. Geen workaround beschikbaar voor CVE-2026-20127. Controleer op indicators of compromise (rogue peers, onbekende SSH-sleutels, root-logins). Zie Technische Bijlage T1.

- **Bron:** CCB — Cisco Catalyst SD-WAN (26 feb 2026)
- **Bron:** CISA ED 26-03 + Alert (25 feb 2026)
- **Bron:** The Hacker News — Cisco SD-WAN zero-day

🟤 DRINGEND: Juniper Junos OS Evolved — Ongeauthenticeerde root-RCE (CVSS 9.8)

Op 25 februari 2026 publiceerde Juniper Networks een noodpatch voor CVE-2026-21902, een kritieke kwetsbaarheid (CVSS 9.8) in Junos OS Evolved op PTX-reeksen. Een foute toegangsrechten-toewijzing in het On-Box Anomaly Detection-framework stelt een ongeauthenticeerde aanvaller in staat om willekeurige code uit te voeren als root. De dienst is standaard ingeschakeld en extern bereikbaar — wat betekent dat elk systeem dat het netwerk ziet kwetsbaar kan zijn. Juniper rapporteert geen actieve exploitatie op het moment van publicatie, maar gezien de eenvoudige exploiteerbaarheid is onmiddellijke actie vereist.

- **Getroffen versies:** Junos OS Evolved op PTX Serie — versies 25.4 vóór 25.4R1-S1-EVO en 25.4R2-EVO. Oudere versies zijn NIET getroffen.
- **Patch:** Upgrade naar 25.4R1-S1-EVO, 25.4R2-EVO of 26.2R1-EVO. Workaround: beperk toegang via ACLs/firewall-filters of schakel de dienst uit via 'request pfe anomalies disable'.

Context: PTX-routers zijn kern- en peeringrouters bij ISPs, telco's en grote ondernemingen — ook in België actief.

- **Bron:** CCB — Junos OS Evolved (27 feb 2026)
- **Bron:** Security Affairs — CVE-2026-21902
- **Bron:** BleepingComputer — Juniper PTX root takeover

www.CyberSecured.be

DRINGEND: DRINGEND: SolarWinds Serv-U — Vier kritieke RCE-kwetsbaarheden (CVSS 9.1)

Op 24 februari 2026 patchte SolarWinds vier kritieke kwetsbaarheden in Serv-U Managed File Transfer (update naar versie 15.5.4). De vier flaws — broken access control, type confusion (2x) en IDOR — laten een aanvaller met beheerdersrechten toe om willekeurige code uit te voeren als root of SYSTEM. Geen actieve exploitatie bevestigd, maar Serv-U heeft een verleden van gerichte exploitatie (o.a. door China-gebonden APT Storm-0322).

Getroffen CVEs: CVE-2025-40538, CVE-2025-40539, CVE-2025-40540, CVE-2025-40541 (alle CVSS 9.1).

Actie: Update onmiddellijk naar Serv-U 15.5.4. Versies 15.5.1 en eerder hebben geen support meer sinds 18 februari 2026.

- **Bron:** CCB — SolarWinds Serv-U (25 feb 2026)
- **Bron:** The Hacker News — SolarWinds Serv-U patches
- **Bron:** Help Net Security — Serv-U kwetsbaarheden

DRINGEND: Zyxel routers — Kritieke Command Injection (CVSS 9.8)

Het CCB waarschuwde op 26 februari 2026 voor CVE-2025-13942 (CVSS 9.8), een command injection-kwetsbaarheid in de UPnP-functie van meer dan een dozijn Zyxel-routers (CPEs, Fiber ONTs, security routers, wireless extenders). Een ongeauthenticeerde aanvaller kan OS-commando's uitvoeren via kwaadaardige UPnP SOAP-verzoeken, op voorwaarde dat WAN-toegang EN de kwetsbare UPnP-functie zijn ingeschakeld. WAN-toegang is standaard uitgeschakeld.

Actie: Controleer of WAN-toegang en UPnP ingeschakeld zijn op Zyxel-apparaten. Pas de laatste Zyxel-firmware toe.

- **Bron:** CCB — Zyxel routers (26 feb 2026)
- **Bron:** Security Affairs — Zyxel CVE-2025-13942
- **Bron:** BleepingComputer — Zyxel critical RCE flaw

HOOG: VMware Aria Operations — RCE & Privilege Escalation

Het CCB waarschuwde op 25 februari 2026 voor ernstige kwetsbaarheden in VMware Aria Operations en VMware Cloud Foundation, waaronder CVE-2026-22719 (CVSS 8.1, command injection via unauthenticated RCE tijdens support-migratie) en CVE-2026-22720 (CVSS 8.0, XSS). Broadcom heeft patches uitgebracht.

Actie: Upgrade VMware Aria Operations en Cloud Foundation naar de gefixte versies conform Broadcom VMSA-2026-0001.

- **Bron:** CCB — VMware Aria Operations (25 feb 2026)
- **Bron:** SecurityWeek — VMware Aria Operations RCE

GEMIDDELD: SAP CRM / S/4HANA / NetWeaver — Kritieke autorisatiekwetsbaarheden

Het CCB publiceerde op 10 februari 2026 een waarschuwing voor twee kritieke missing-authorization-kwetsbaarheden in SAP CRM, S/4HANA Scripting Editor en NetWeaver AS ABAP

(CVE-2026-0488, CVE-2026-0509). Exploitatie vereist lage bevoegdheden maar geen gebruikersinteractie. Geen actieve exploitatie bevestigd.

Actie: Installeer de SAP Security Patch Day-updates van februari 2026.

- **Bron:** CCB — SAP February 2026 Security Patch Day

4. 🌍 Europese en mondiale dreigingen relevant voor Belgie

Cisco SD-WAN: gecoördineerde wereldwijde aanvalscampagne (UAT-8616)

CISA, het Britse NCSC en de Australische ACSC waarschuwen gezamenlijk voor een actieve, gecoördineerde campagne die wereldwijd Cisco SD-WAN-infrastructuur viseert. De dreigingsactor UAT-8616 misbruikt CVE-2026-20127 om 'rogue peers' toe te voegen en persistente root-toegang te verwerven. Campagne begon in 2023 — systemen kunnen al jarenlang gecompromitteerd zijn zonder detectie. Belgische organisaties met SD-WAN-infrastructuur dienen ONMIDDELLIJK te handelen.

- **Bron:** CISA + NCSC + ASD/ACSC gezamenlijk advies (25 feb 2026)
- **Bron:** Sophos — Cisco SD-WAN actieve exploitatie

UPDATE — Datalek Franse FICOBA-databank: 1,2 miljoen bankrekeningen

Op 18-19 februari 2026 maakte het Franse Ministerie van Economie een groot datalek bekend bij FICOBA, de nationale databank van alle Franse bankrekeningen (>80 miljoen personen, >300 miljoen rekeningen). Een aanvaller gebruikte gestolen inloggegevens van één ambtenaar — zonder MFA — om 1,2 miljoen rekeningen te raadplegen. Blootgestelde data: IBAN, naam, adres en in sommige gevallen fiscaal identificatienummer. Geen toegang tot saldo's of transacties.

Relevantie voor België: De techniek (credential misbruik zonder MFA op gevoelige databanken) is universeel. ANSSI en banken waarschuwen voor phishing-campagnes gericht op gedupeerden. Organisaties met grensoverschrijdende activiteiten in Frankrijk of Franse klanten dienen extra waakzaam te zijn.

- **Bron:** The Record — FICOBA breach (19 feb 2026)
- **Bron:** BleepingComputer — French bank registry breach
- **Bron:** Cybernews — FICOBA analyse

CoinbaseCartel — Nieuwe ransomware-groep met focus op Europa

CoinbaseCartel is een relatief nieuwe ransomware-groep die in het najaar van 2025 opkwam en al twee Belgische slachtoffers claimt. We noteren deze claims maar wijzen er op dat deze NIET geverifieerd zijn en dus met de nodige voorzichtigheid moeten bekeken en beoordeeld worden. De groep onderscheidt zich door 'encryptorloze' extortie: data wordt gestolen en gepubliceerd zonder noodzakelijk bestanden te versleutelen. Dit maakt aanvallen sneller en discreter. De groep richt zich op healthcare, technologie, zakelijke dienstverlening en communicatie — allemaal sterk vertegenwoordigd in België.

- **Bron:** Bitdefender — CoinbaseCartel profiel (feb 2026)

www.CyberSecured.be

ENISA: Overheden zijn het meest geviseerde doelwit in Europa

ENISA rapporteerde in november 2025 dat overheden 38% van alle bijgehouden EU-cyberincidenten voor hun rekening nemen — meer dan enige andere sector. Dit sluit aan bij de FICOBA-aanval in Frankrijk en de eerder gemelde aanval op de Waalse administratie (november 2025, herstel nog lopend).

- **Bron:** ENISA — Overheid meest geviseerde sector (via American Banker)
- **Bron:** ITdaily.be — Waalse administratie aanval (nov 2025)

n8n workflow-automatisering — Kritieke RCE-kwetsbaarheid

Het CCB publiceerde op 27 februari 2026 een waarschuwing voor kritieke kwetsbaarheden in n8n (open-source workflow-automatiseringsplatform), waaronder CVE-2025-68613 die RCE via werkstromen mogelijk maakt. n8n wordt ingezet door IT-teams als alternatief voor dure enterprise-integratieplateaus. Geen actieve exploitatie bevestigd maar technische details zijn publiek.

- **Bron:** CCB — n8n kritieke kwetsbaarheden (27 feb 2026)

5. ☑ Wat kan je concreet doen

Prioriteit	Actie	Wie	Bron
NOODGEVAL	Inventariseer en patch Cisco Catalyst SD-WAN Controller en Manager. Controleer op rogue peers, onbekende SSH-sleutels en onverwachte root-logins. Volg CISA ED 26-03 (forensisch onderzoek vereist naast patching). Zie Technische Bijlage T1.	IT-team / CISO	CISA ED 26-03
NOODGEVAL	Patch Juniper PTX-routers (Junos OS Evolved 25.4) naar versie 25.4R1-S1-EVO of hoger. Beperk via ACLs intussen toegang tot het On-Box Anomaly Detection-eindpunt.	Netwerk-admins	CCB Advisory
DRINGEND	Update SolarWinds Serv-U naar versie 15.5.4 (vier kritieke CVEs, CVSS 9.1). Audit admin-accounts op Serv-U-instanties, controleer logs op ongewoon gedrag.	IT-team / Sys-admins	The Hacker News
DRINGEND	Controleer Zyxel-routers op ingeschakelde WAN-toegang + UPnP. Patch naar laatste firmware. Schakel UPnP uit als dit niet noodzakelijk is.	Netwerk-admins	CCB Advisory (26 feb)
HOOG	Patch VMware Aria Operations (CVE-2026-22719 en CVE-2026-22720) conform Broadcom VMSA-2026-0001. Patch SAP CRM/S4HANA/NetWeaver via SAP Security Patch Day feb 2026.	IT-team / Sys-admins	CCB Advisory (25 feb)

Prioriteit	Actie	Wie	Bron
HOOG	Informeer bedrijfsleiders over de actieve identiteitsfraude die de naam van de Belgische Koning misbruikt. Verificeer altijd betaalverzoeken via een bekend telefoonnummer.	Management / HR	CCB Waarschuwing
HOOG	Controleer of MFA is ingeschakeld op alle kritieke systemen — met name beheerdersaccounts voor netwerkapparatuur, fileservers en CRM/ERP-systemen. FICOBA-incident toont de kostprijs van ontbrekende MFA.	CISO / IT-management	Help Net Security (FICOBA)
MEDIUM	Test het back-upproces: wanneer is de laatste restore getest? Zijn back-ups offline (air-gapped) bewaard? Hoelang duurt een volledige restore? Dit zijn de cruciale vragen die vóór een aanval beantwoord moeten zijn.	IT-team / Management	CCB NIS2-gids

Bron: CCB/Safeonweb Advisories — volledig patchoverzicht

6. Dreigingsniveau-overzicht per categorie

Categorie	Niveau	Toelichting
Ransomware (België)	**Kritiek**	(CoinbaseCartel). Encryptorloze extortie-tactiek is sneller en discreter.
Netwerk-infrastructuur	**Kritiek**	Cisco SD-WAN CVSS 10.0 + Juniper CVSS 9.8 + Zyxel CVSS 9.8 — noodpatching vereist. Actieve wereldwijde aanvallen.
Softwarekwetsbaarheden	**Kritiek**	Zes kritieke patches deze week: Cisco, Juniper, SolarWinds, Zyxel, VMware, SAP. Aanvallers scannen actief.
Fraude & Social Engineering	**Hoog**	Actieve fraude via naam Belgische Koning. Nep-uitnodigingen voor galadiners van de Koning Boudewijn Stichting.
Overheidsinfrastructuur	**Hoog**	ENISA bevestigt: overheden zijn meest geviseerde sector in Europa (38% van EU-incidenten). FICOBA in Frankrijk.
Managed File Transfer (MFT)	**Hoog**	SolarWinds Serv-U: vier kritieke CVEs (CVSS 9.1). MFT-servers zijn aantrekkelijk doel wegens gevoelige data.
Cloudvirtualisatie	**Hoog**	VMware Aria Operations: RCE via ongeauthenticeerde command injection. Patch VMSA-2026-0001 toepassen.

www.CyberSecured.be

Categorie	Niveau	Toelichting
KMO's	🔴 **Hoog**	Onderbeschermd, zonder NIS2-compliance, kwetsbaar voor opportunistische aanvallen na publicatie van IOCs.
Lokale besturen / Overheden	🟡 **Hoog**	Geen nieuwe Belgische overheidsincidenten bevestigd deze week — achtergronddreiging van NoName057(16) blijft.
DDoS	🟡 **Gemiddeld**	Verhoogd door geopolitieke context (NAVO-gerelateerd). Geen grootschalige aanvallen op BE bevestigd.

✉ Incidenten melden | Verdachte berichten

cert.be/report-incident | verdacht@safeonweb.be | +32 (0)2 501 05 60

Volgende briefing: 9 maart 2026