OT-TOOLSERIE

OT Vulnerability Besluitsheet

NL · één kwetsbaarheid per blad

1 VULNERABILITY CONTEXT

CVE-NUMMER | ASSET / SYSTEEM | ZONE | DATUM BEOORDELING

LEVERANCIER EN VERSIE | BEOORDELAAR | FUNCTIE VAN DIT ASSET IN HET PROCES

2 BLOOTSTELLING & EXPLOITABILITY

Bron, vanwaar begint een aanval? ☐ internet ☐ IT-netwerk ☐ leverancier ☐ USB ☐ aangrenzende zone

Bereikbaarheid, is er vandaag een pad? ☐ ja ☐ nee ☐ onbekend

BESCHRIJF HET PAD IN ÉÉN ZIN

Draait de kwetsbare component? ☐ ja ☐ nee ☐ onbekend

Benodigde rechten ☐ anoniem ☐ gebruiker ☐ al binnen

Bewijs van misbruik ☐ in CISA KEV ☐ EPSS-score _____ ☐ publieke PoC ☐ alleen theoretisch ☐ leverancier zegt “not affected” (VEX)

3 OPERATIONAL IMPACT ALS MISBRUIK LUKT

☐ verlies van zicht ☐ verlies van sturing ☐ productiestop ☐ kwaliteitsverlies ☐ schade aan apparatuur ☐ milieu-effect ☐ veiligheidsrisico

WAT GEBEURT ER CONCREET | HOE LANG TOT HERSTEL

4 BESTAANDE MAATREGELEN - COMPENSATING CONTROLS

WAT VANGT DIT RISICO NU AL AF

	GEVERIFIEERD	AANGENOMEN
	☐	☐
	☐	☐
	☐	☐
	☐	☐

Een maatregel waarvan niemand heeft gecontroleerd of hij werkt, telt niet.

5 PATCH HAALBAARHEID

Gevalideerde patch van de leverancier? ☐ ja ☐ nee ☐ in behandeling

Herstart nodig? ☐ ja ☐ nee Onderhoudsvenster (datum) _____

Raakt dit een veiligheidsinstrumentatie (SIS)? ☐ ja ☐ nee

Als ja, dan is dit geen patch maar een management-of-change-traject onder IEC 61511.

Terugvalpad getest? ☐ ja ☐ nee

RISICO VAN DE MAATREGEL ZELF

6 HET BESLUIT — KIES ÉÉN

☐ **PATCH**
Gevalideerd, past in een venster.

☐ **MITIGATE**
Pad weg in plaats van kwetsbaarheid weg.
MAATREGEL + WIE VERIFIEERT

☐ **MONITOR**
WAT MONITOREN WE
WAAR VALT HET OP
WANNEER OPNIEUW

☐ **ACCEPT**
Restrisico begrepen en belegd.

7 EIGENAAR EN REVIEW

RESTRISICO IN ÉÉN ZIN — IN GEVOLGEN, NIET IN EEN SCORE

RISICO-EIGENAAR (PERSOON) | DATUM BESLUIT | REVIEWDATUM | HANDTEKENING / PARAAF

Beslisroute — datastroom

START (1 CVE)

Bepaal bron, pad en operationele impact
BLOK 1 T/M 3

BLOK 2
Exposure & exploitability

1 Is er vandaag een open internetpad van de bron naar dit asset?

NEE → **MONITOR**
Leg vast wat er moet veranderen om een pad te laten ontstaan, en wanneer je opnieuw kijkt.

JA

2 Draait de kwetsbare component?

NEE → **MONITOR**
Bewaak herinschakeling van de component, niet patchen.

JA

BLOK 5
Patch feasibility

3 Raakt dit een veiligheidsinstrumentatie (SIS)?

JA → **MITIGATE**
Geen patch: management of change onder IEC 61511. Noteer wie de wijziging beoordeelt.

NEE

4 Gevalideerde patch, onderhoudsvenster én getest terugvalpad?

JA → **PATCH**
Plan in het venster. Noteer datum, terugvalpad en wie de uitvoering verifieert.

NEE

BLOK 4
Bestaande maatregelen

5 Is het pad weg te nemen of af te knijpen?

JA → **MITIGATE**
Noem de maatregel én wie verifieert dat hij werkt. Aangenomen telt niet.

NEE

6 Is de impact aanvaardbaar tot de reviewdatum?

JA → **ACCEPT**
Restrisico in gevolgen, eigenaar met naam, paraaf en reviewdatum.

NEE · ESCALEER NAAR DE ASSET OWNER

EINDE

Werk van boven naar beneden en stop bij de eerste uitkomst. Bij **onbekend**: ga verder alsof het antwoord ja is en noteer dat in blok 2.