PatchRun

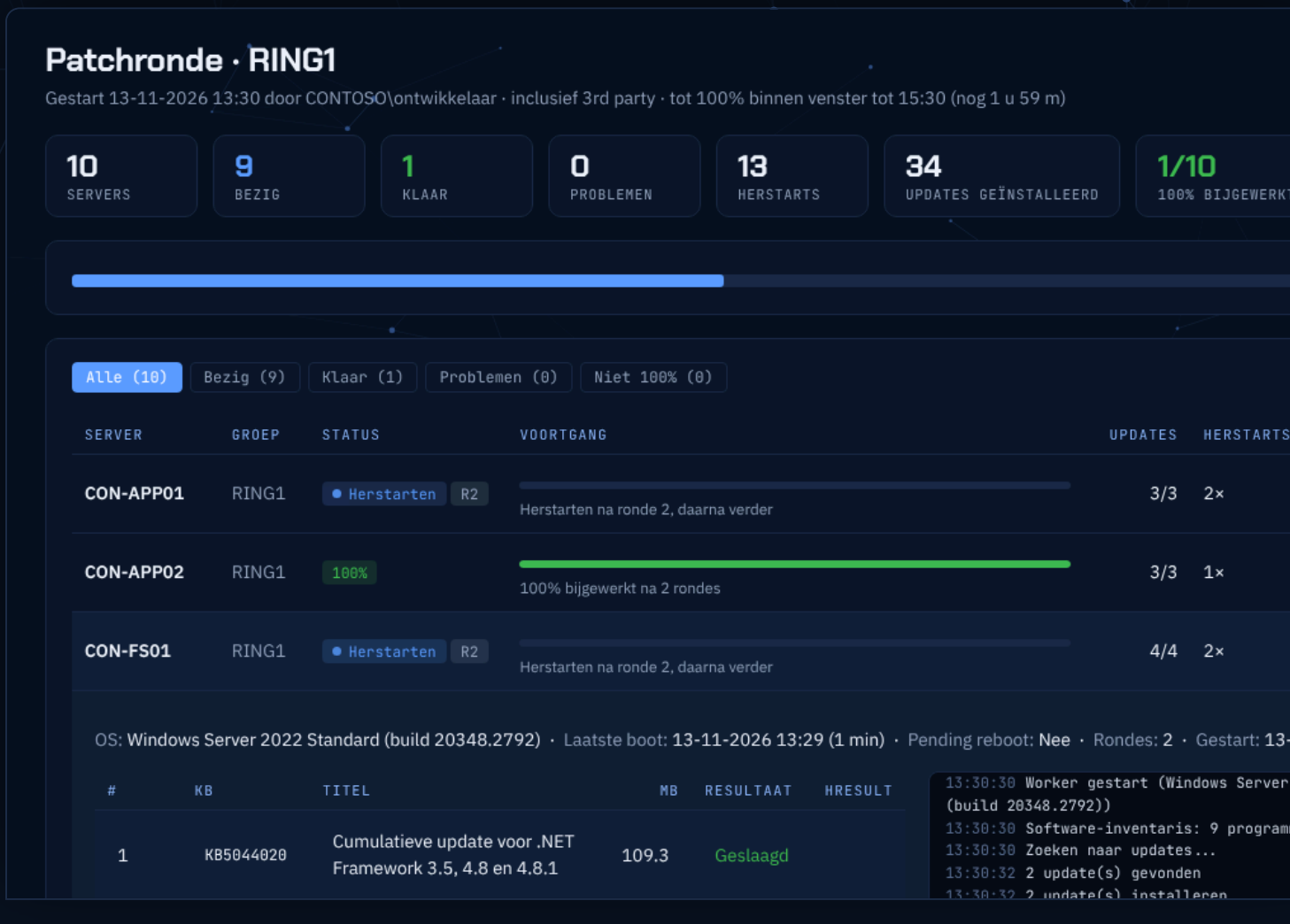
Versie 1.12 · november 2026

```
beheer@patchrun:~$ patchrun --ring RING1 --window 2h
```

Windows-servers op 100%, binnen het onderhoudsvenster.

Een webconsole die WSUS-updates, 3rd party software en kwetsbaarheden van je hele serverpark beheert, en je live laat zien wat er op elke server gebeurt.

Live voortgang per server · Rondes tot 100% · Planning per ring · 3rd party apps · CVE · CVSS · KEV · EPSS · Werklijst



WAAROM PATCHRUN

Patchen hoort voorspelbaar te zijn

In de praktijk is het dat zelden: na een herstart staan er nog updates klaar, een update faalt elke maand opnieuw zonder dat iemand het ziet, en de 3rd party software loopt achter.

Zonder PatchRun

- Scripts die "installeren" en hopen dat het goed gaat
- Een tweede ronde handmatig na de herstart
- Logbestanden doorspitten om fouten te vinden
- 3rd party apps (PuTTY, Acrobat, 7-Zip…) apart en vaak vergeten
- Geen zicht op welke CVE's echt openstaan

Met PatchRun

- Servers worden in rondes naar 100% gebracht, binnen het venster
- Live per server zien wat er gebeurt, tot op de update
- Fouten die terugkomen staan de volgende ochtend op een werklijst
- 3rd party apps worden meegenomen, met goedkeuring en per ring
- Per server en per app zie je CVE's, CVSS, KEV en EPSS

WAT HET KAN

100

Tot 100% binnen het venster

Zoeken, installeren, direct herstarten, opnieuw zoeken. Rondes tot er niets meer openstaat of het venster op is.

●

Live meekijken

Per server: uitrollen, zoeken, downloaden 43%, installeren 2/5, herstarten, ronde 2, 100%. Een run of server annuleren kan op elk moment.

AD

Groepen uit Active Directory

Servers komen uit AD. Deel ze in groepen in, zoals TEST / PROD of RING0 / RING1 / RING2.

::

Planningen

Eenmalig, wekelijks (bijv. di + vr 20:00) of Patch Tuesday + N dagen, elk met starttijd en venster.

3P

3rd party patching

Eigen repository met goedkeuring, handtekeningcontrole en wachttijd per ring. Met software-inventaris: wat staat waar?

!

Kwetsbaarheden

Microsoft (MSRC) en NVD gekoppeld aan builds en apps, aangevuld met CISA KEV en EPSS voor prioriteit.

≡

Werklijst

Updates en apps die blijven falen, met uitleg per foutcode. Oppakken, notitie, opgelost. Exporteren en afdrukken.

#

Veilig ontworpen

Windows-login met AD-rollen, geen wachtwoorden in taken, token per server, audit log.

{ }

API en PowerShell

Alles wat de console kan, ook via de REST-API met API-sleutels per rol. Met OpenAPI-beschrijving en PowerShell-module.

HOE HET WERKT

Van Active Directory tot 100% bijgewerkt

01 /
Servers ophalen
Dagelijks uit AD, met OS, OU en laatste aanmelding. CSV-import kan ook.

02 /
Indelen in groepen
Elke server in één groep, bijv. RING0 test, RING1 en RING2 productie.

03 /
Plannen
Starttijd en venster per groep, of nu direct starten.

04 /
Patchronde
Rondes tot 100%, met directe herstarts binnen het venster.

05 /
Nalopen
Wat niet lukte staat op de werklijst, met advies per foutcode.

Rondes in plaats van één poging

Na een herstart komen er vaak nieuwe updates (servicing stack, .NET, cumulatieve updates). PatchRun gaat daarom door:

`Ronde 1 · 5 updates` → herstart →

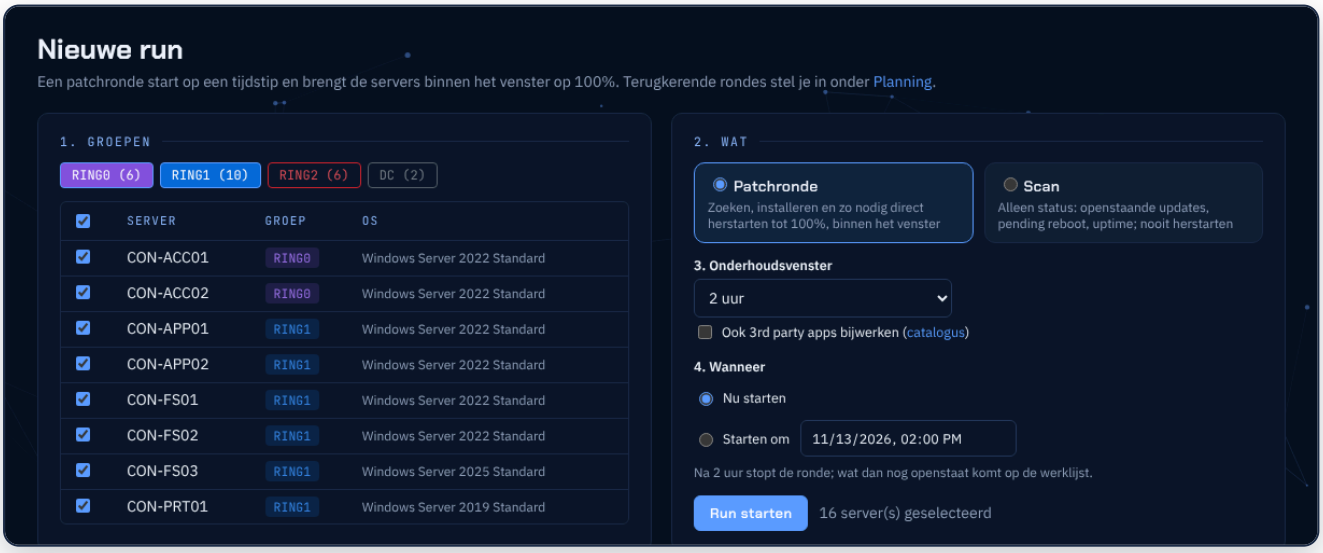
`Ronde 2 · 2 updates` → herstart →

`Ronde 3 · 0` → `100%`

Een update die mislukt wordt niet eindeloos opnieuw geprobeerd. Als het venster bijna op is, start er geen nieuwe installatie of herstart meer. Herstart Windows zelf nog een keer (servicing van een cumulatieve update), dan gaat de ronde gewoon verder. Komt een server echt niet terug, dan zie je dat meteen.

Een voorbeeld

GROEP	PLANNING	VENSTER
RING0 (test)	Patch Tuesday + 1, 20:00	2 uur
RING1	Elke di en vr, 20:00	2 uur
RING2 (kritiek)	Patch Tuesday + 8, 20:00	2 uur
DC	Elke ma 07:00	alleen scan

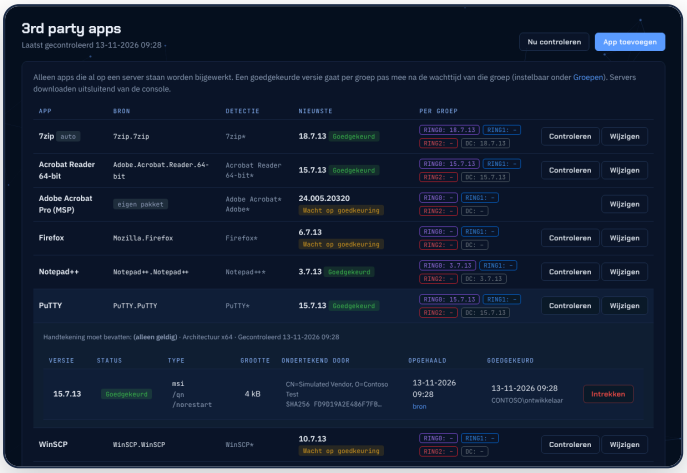


Nieuwe run: groepen kiezen, patchronde of scan, venster en nu of later starten. Terugkerende rondes stel je in onder Planning.

MEER DAN WINDOWS UPDATE

3rd party software en kwetsbaarheden

Dezelfde patchronde werkt ook de applicaties bij die op een server staan, en laat zien welke kwetsbaarheden er nog openstaan.



3rd party catalogus met versie, goedkeuring en uitrol per ring.

Eigen repository, eigen tempo

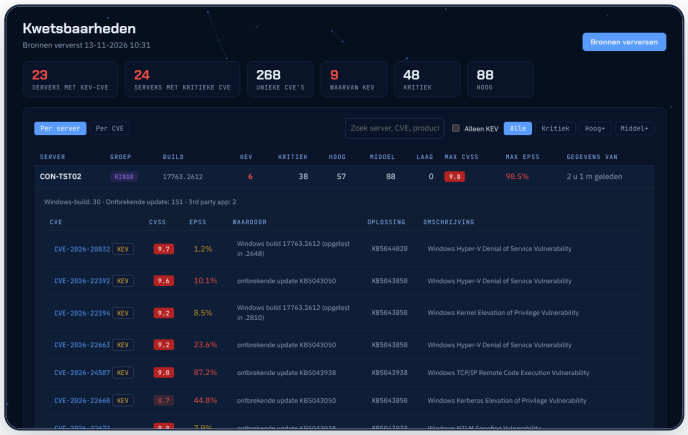
- Nieuwe versies via winget-metadata of eigen pakketten (bijv. Acrobat Pro MSP)
- Pas na goedkeuring beschikbaar
- Per groep een wachttijd: RING0 direct, RING1 na 3 dagen, RING2 na 7 dagen
- Authenticode-handtekening en ondertekenaar worden gecontroleerd
- Servers downloaden alleen van de console, niet van internet
- Er wordt nooit iets nieuw geïnstalleerd, alleen bijgewerkt

Weten wat er openstaat

PatchRun koppelt openstaande updates, Windows-builds en geïnstalleerde apps aan CVE's:

MSRC	Microsoft-CVE's met KB en vaste build
NVD	CVE's en CVSS voor 3rd party apps
CISA KEV	Wordt actief misbruikt
FIRST EPSS	Kans op misbruik in 30 dagen

Per server en per CVE: welke servers zijn kwetsbaar, waardoor, en welke update of versie het oplost.

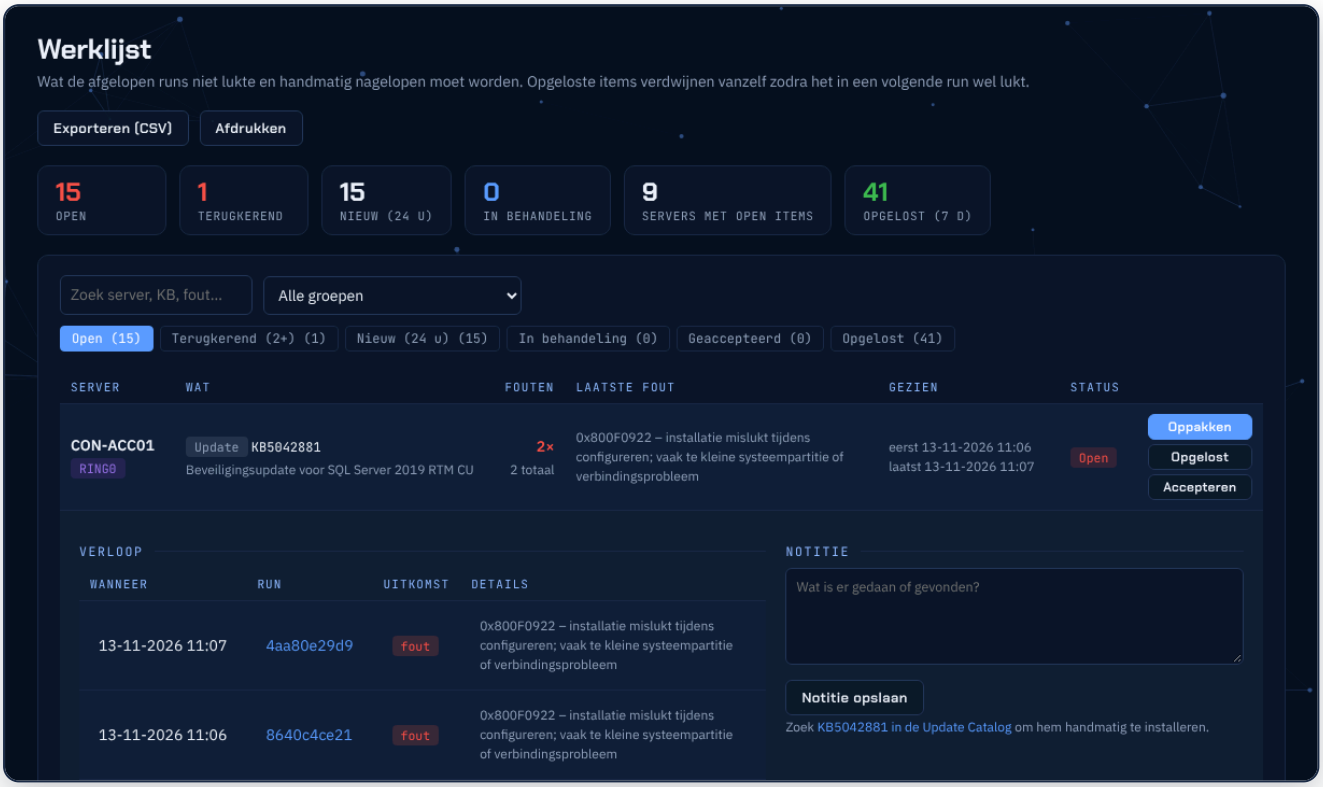


Kwetsbaarheden per server, met KEV, CVSS, EPSS en oplossing.

DE OCHTEND ERNA

Een werklijst in plaats van logbestanden

Alles wat in de afgelopen runs niet lukte staat op één lijst, per server, update of app. Fouten die terugkomen vallen meteen op, en wat later alsnog lukt verdwijnt vanzelf.



Werklijst met foutcode, uitleg (bijv. DISM /RestoreHealth), verloop per run en notities.

Oppakken
Wie is ermee bezig, met notitie

Terugkerend
Faalt twee keer of vaker op rij

Uitleg
Advies per HRESULT-foutcode

CSV / print
Voor het ochtendoverleg

BEVEILIGING

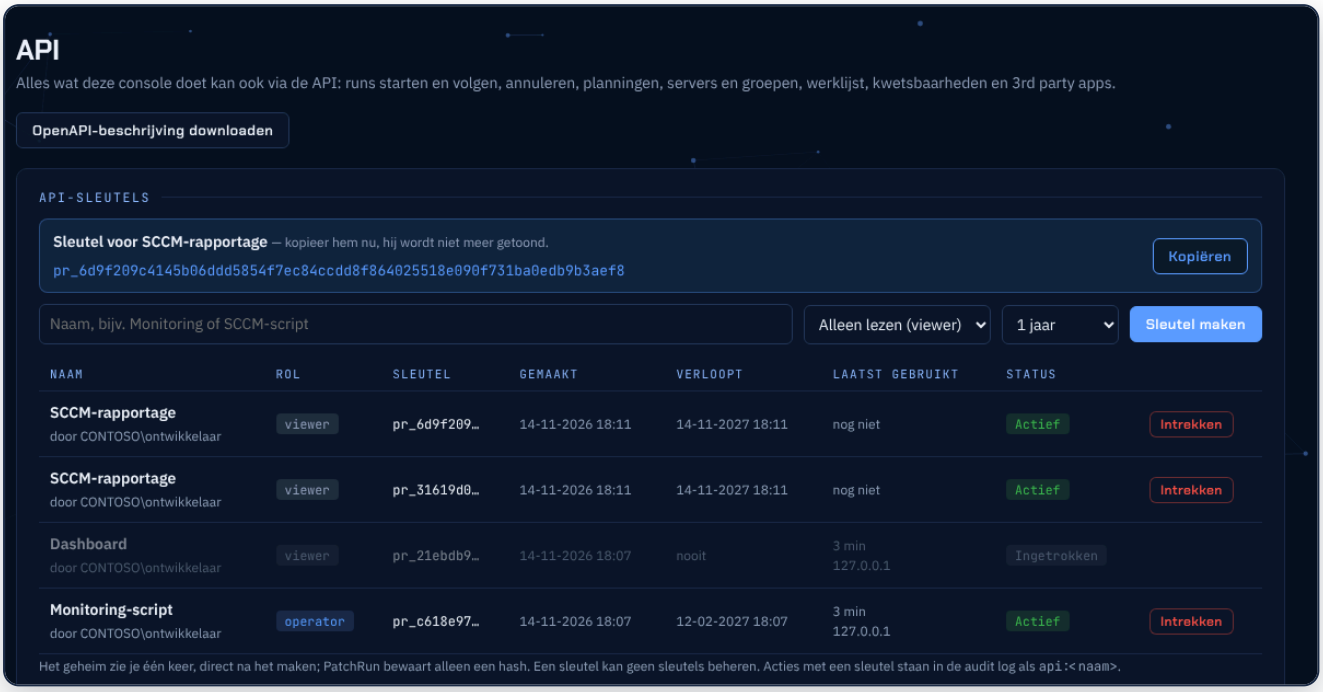
- Windows-login (Kerberos/NTLM); alleen leden van de AD-groepen *Operator* of *Viewer* hebben toegang
- De console draait als gMSA, de worker als SYSTEM. Er staan geen wachtwoorden in geplande taken.
- Per run en per server een eigen token, alleen als hash opgeslagen
- CSRF-bescherming en een strikte Content Security Policy
- Audit log: wie startte, annuleerde of keurde wat goed, ook via de API

OOK HANDIG

- **Serverstatus**: uptime, pending reboot, open updates en CVE's in één tabel
- **Scan**: status ophalen zonder iets te installeren of te herstarten
- **Problemen**: mislukte updates per periode met HRESULT
- **Opnieuw voor probleemservers**: één klik na een mislukte uitrol
- Gemiste planningen (console uit) starten nog tot een uur te laat

Ook te bedienen via de API

Wat je in de console doet, kan ook vanuit een script, SCCM of monitoring: runs starten en volgen, annuleren, planningen, servers, werklijst en kwetsbaarheden.

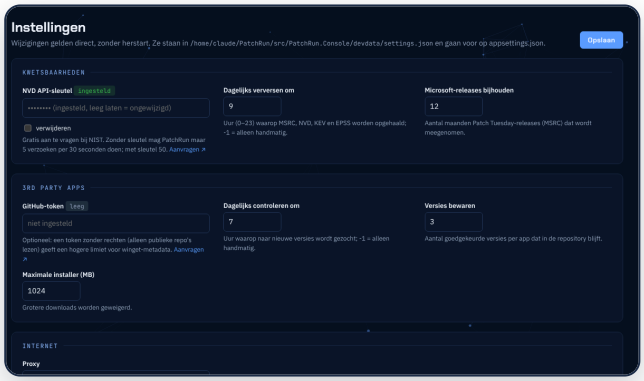


API-sleutels met naam, rol, geldigheid en laatst gebruikt. De sleutel zie je één keer.

REST-API en PowerShell

- Aanmelden met een API-sleutel (`Bearer pr_…`) of met het Windows-account
- Dezelfde rollen als in de console: alleen lezen of beheren
- Een sleutel kan geen sleutels beheren; acties staan in de audit log als `api:<naam>`
- OpenAPI-beschrijving van alle endpoints, te importeren in Postman of Swagger UI
- PowerShell-module voor Windows PowerShell 5.1 en PowerShell 7

```
Connect-PatchRun -Url $url -ApiKey $key
Start-PatchRun -Group RING0 -Mode Patch -Wait
Get-PatchRunWorklist -Status open
```

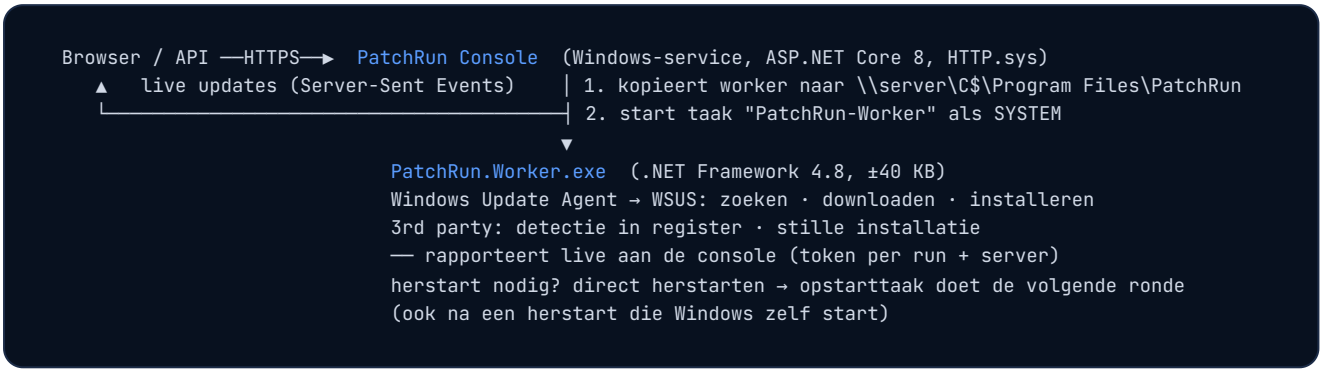


Instellingen: bronnen voor kwetsbaarheden, 3rd party, proxy, AD en patchrondes.

ONDER DE MOTORKAP

Licht, zonder agents of database

Eén console en een kleine worker die per run naar de server wordt gekopieerd. Er draait niets permanent op de servers.



Vereisten

Console	Windows Server 2016 of nieuwer, certificaat voor HTTPS (.NET 8 zit in de setup); draait als Windows-service
Account	gMSA met lokale adminrechten op de servers
Servers	Windows Server 2016 t/m 2025, gekoppeld aan WSUS, met .NET Framework 4.8 (op 2016 en 2019 eerst installeren; de console controleert het)
Netwerk	SMB (445, firewallregel SMB-In aan) + Taakplanner (RPC) naar servers; HTTPS terug naar de console
Internet	Alleen de console, optioneel via proxy (winget, MSRC, NVD, KEV, EPSS)
Opslag	JSON-bestanden en installers; geen SQL nodig

Installatie: één setup

`PatchRun-Setup.exe` bevat alles (ook .NET 8). De wizard controleert account, certificaat, poort en groepen en regelt de rest.

1. Vooraf: gMSA, servercertificaat en twee AD-groepen
2. `PatchRun-Setup.exe` starten en de wizard volgen
3. In de console: synchroniseren met AD, groepen indelen, planning maken

Stil installeren kan ook (`/quiet`), en bijwerken en verwijderen gaat via Programma's en onderdelen.

Meer weten of een demo zien?
In de demomodus draait de console met gesimuleerde servers, zonder risico.

Martijn Peeters
info@mpeeters.nl