Kiteworks

TECHNISCHE GIDS

MOVEit: drie jaar kwetsbaarheden in beeld

Historisch overzicht van inbreuken, analyse van de beveiligingsarchitectuur, regelgevingsimplicaties en het architecturale alternatief

In mei 2023 werd een kritieke SQL-injectiekwetsbaarheid in Progress MOVEit Transfer (CVE-2023-34362) het voertuig voor een van de grootste ooit gedocumenteerde supplychain-datalekken. Drie jaar later heeft MOVEit ten minste 11 openbaar gemaakte CVE's over drie productlijnen verzameld, waarvan vijf met een NVD CVSS-score van 9.0 of hoger, en het platform blijft in actieve exploitatiecycli. De openbaarmaking op 30 april 2026 van **CVE-2026-4670** (bypass van authenticatie met CVSS 9.8) en **CVE-2026-5174** in MOVEit Automation markeert de derde kwetsbaarheidsgolf die het platform in drie jaar treft.

Deze diepgaande analyse onderzoekt wat het MOVEit-overzicht aan beveiligings- en compliance-verantwoordelijken vertelt over de architectuur van managed file transfer als categorie. Het patroon is structureel -- een eigenschap van platforms die een internet-blootgesteld oppervlak, door de klant beheerde infrastructuur, gevoelige content in rust en beperkte containment bij een gevonden kwetsbaarheid combineren. Het architecturale antwoord is niet een ander MFT-product. Het is een volledig ander model.

Wat dit rapport beargumenteert

Het MOVEit-kwetsbaarheidspatroon is geen pechreeks. Het is de voorspelbare uitkomst van een architectuur die een internet-blootgestelde webapplicatie, een door de klant beheerd besturingssysteem, een SQL-backend en een bestandsopslag op één vertrouwensgrens plaatst.

Wisselen van MFT-leverancier herstart de patch-cyclus. Veranderen van architectuur beëindigt hem.

11+ openbaar gemaakte MOVEit-CVE's over drie productlijnen in drie jaar

5 met NVD CVSS 9.0 of hoger -- kritieke severity

1.440+ internet-blootgestelde MOVEit Automation-instanties vandaag in risico

1

Drie jaar in beeld

In één oogopslag

2023

Cl0p exploiteert MOVEit Transfer massaal. Meer dan 2.700 organisaties, ~93 mln personen.

2024

Twee bypasses van authenticatie met NVD CVSS 9.1. Exploitcode op dag één publiek.

2025

Privilege escalation in de SFTP Shared Accounts-module.

2026

Bypass van authenticatie met NVD CVSS 9.8 + privilege escalation in MOVEit Automation. Geen workaround.

De Cl0p-massa-exploitatie van 2023 en de daaropvolgende CVE's

Op 27 mei 2023 begon de ransomwaregroep Cl0p met de massa-exploitatie van CVE-2023-34362, een SQL-injectiekwetsbaarheid met CVSS 9.8 in MOVEit Transfer. Progress bracht op 31 mei een patch uit, maar in sommige gevallen zag Mandiant gegevensdiefstal **binnen enkele minuten na ontwikkeling van de webshell** -- de patch kwam pas na het grootste deel van de schade. De aanvalsketen combineerde SQL-injectie in de webapplicatie, een deserialisatielek dat het resulterende sysadmin-token omzette in remote code execution, en het ontbreken van architecturale containment tussen de applicatie en de onderliggende Azure Blob-opslag. Cl0p plaatste een aangepaste ASP.NET-webshell genaamd LEMURLOOT, vermomd als *human2.aspx*, die verborgen administratoraccounts aanmaakte met de naam „Health Check Service” en gegevens exfiltreerde via aangepaste HTTP-headers.

Hoe de Cl0p-aanvalsketen van 2023 de gegevens bereikte

1 SQL-injectie in de weblaag

Niet-geauthenticeerde SQL-injectie in de openbare MOVEit Transfer-webinterface -- het oppervlak dat nodig is voor partnertoegang -- legde tokens met sysadmin-rechten bloot.

2 Deserialisatie naar remote code execution

Een deserialisatielek zette het buitgemaakte token om in willekeurige code-uitvoering op de host. De webapplicatie en de database voerden nu de instructies van de aanvaller uit.

3 LEMURLOOT-webshell geïnstalleerd

Een aangepaste ASP.NET-webshell (human2.aspx) creëerde verborgen administratoraccounts met de naam „Health Check Service” en kanaliseerde de exfiltratie via aangepaste HTTP-headers.

4 Directe toegang tot de bestandsopslag

Geen laaggrens scheidde de applicatie van de bestandsopslag of de Azure Blob-credentials. Eenmaal binnen besloeg de schadestraal elk klantbestand dat het platform huisvestte.

Tegen het einde van 2023 had de campagne meer dan 2.700 organisaties gecompromitteerd en persoonsgegevens van ongeveer 93,3 miljoen mensen blootgelegd. CISA schatte dat meer dan 3.000 Amerikaanse entiteiten en meer dan 8.000 wereldwijd werden geraakt wanneer de downstream-blootstelling werd meegerekend -- meer dan vier op de vijf slachtofferorganisaties hadden geen directe relatie met Progress. In de zes weken na de eerste openbaarmaking identificeerde Progress vijf extra CVE's: CVE-2023-35036 (9 juni), CVE-2023-35708 (15 juni) en het juli-servicepack dat CVE-2023-36932, CVE-2023-36933 en CVE-2023-36934 (CVSS 9.1 kritiek) behandelde.

Genoemd in de Cl0p-onthullingen over MOVEit Transfer in 2023

BBC	British Airways	U.S. Department of Energy	Johns Hopkins University
Shell	Louisiana Airways	Oregon DMV	Maximus (11,3 mln)
Welltok (10 mln)	Delta Dental of CA (6,9 mln)	CMS / WPS (3,1 mln)	+ 2.700 meer

Het authenticatie-bypass-paar van 2024

Op 25 juni 2024 maakte Progress **CVE-2024-5805** (kritieke bypass van authenticatie met CVSS 9.1 in MOVEit Gateway) en **CVE-2024-5806** (aanvankelijk CVSS 7.4, twee dagen later opgeschaald naar 9.1 kritiek toen een kwetsbaarheid in de externe bibliotheek IPWorks SSH werd onthuld) bekend. Beide waren onjuiste-authenticatie-lekken in de SFTP-module. De Shadowserver Foundation zag binnen enkele uren na de openbaarmaking exploitatiepogingen tegen CVE-2024-5806. WatchTowr Labs publiceerde diezelfde dag werkende proof-of-concept-exploitcode. Exploitatie vereiste slechts een geldige gebruikersnaam, bereikbaar via credential spraying tegen de SFTP-service.

> “Exploitatiepogingen volgden binnen enkele uren na de openbaarmaking. Werkende proof-of-concept-code was diezelfde dag publiek. Exploitatie had alleen een geldige gebruikersnaam.” --
>
> Bypass van authenticatie in MOVEit Gateway / Transfer -- juni 2024

Het privilege-escalation-probleem van 2025 en de onthulling van 2026

In 2025 maakte Progress **CVE-2025-2324** bekend, een kwetsbaarheid door onjuist beheer van privileges in de SFTP-module van MOVEit Transfer die gebruikers raakte die als Shared Accounts waren geconfigureerd. De aankondiging van 30 april 2026 onthulde vervolgens **CVE-2026-4670** en **CVE-2026-5174** in MOVEit Automation, de productlijn die MFT-bewerkingen automatiseert en plant -- loonadministratie, zorgvergoedingen, financiële transacties, regelgevingsindieningen. Shodan identificeerde meer dan 1.440 internet-blootgestelde MOVEit Automation-instanties in risico, waaronder 16 verbonden met Amerikaanse staats- en lokale overheden.

Het patroon over leveranciers heen: vier kritieke MFT-kwetsbaarheden in 18 maanden

MOVEit is het meest behandelde voorbeeld, maar het patroon beperkt zich niet tot één leverancier. Over heel 2024 en 2025 publiceerden vier verschillende MFT-platforms kwetsbaarheden met kritieke severity, die elk binnen een kort venster na publieke openbaarmaking werden geëxploiteerd.

Cleo	CrushFTP	Wing FTP	MOVEit
Dec. 2024	Mrt. 2025	Jul. 2025	Apr. 2026
Cl0p-massa-exploitatie; 300+ geclaimde slachtoffers in transport, productie en voedsel.	Bypass van authenticatie; de vervolgonthulling van juli 2025 maakte volledige serverovername mogelijk.	Ongeauthenticeerde RCE via Lua-injectie; impact op root-/SYSTEM-privileges.	Bypass van authenticatie met NVD CVSS 9.8 + privilege escalation in Automation. Geen workaround.

MOVEit CVE-overzicht, 2023-2026

Jaar	CVE	Vector	CVSS NVD	Impact
2023	CVE-2023-34362	SQL-injectie (Transfer)	9.8	Cl0p-zeroday; 2.700+ org's, 93 mln+ personen
2023	CVE-2023-35036	SQL-injectie (Transfer)	Kritiek	Vervolgonthulling op 9 juni
2023	CVE-2023-35708	SQL-injectie (Transfer)	Kritiek	Vervolgonthulling op 15 juni
2023	CVE-2023-36932	SQL-injectie (Transfer)	Hoog	Juli-servicepack
2023	CVE-2023-36933	Onafgehandelde uitzondering	Hoog	Juli-servicepack
2023	CVE-2023-36934	SQL-injectie (Transfer)	9.1	Juli-servicepack
2024	CVE-2024-5805	Auth-bypass (Gateway SFTP)	9.1	Onthuld op 25 juni; PoC dezelfde dag
2024	CVE-2024-5806	Auth-bypass (Transfer SFTP)	9.1	Shadowserver-exploitatie binnen uren
2025	CVE-2025-2324	Privilege escalation (SFTP)	Hoog	Shared Accounts-module
2026	CVE-2026-4670	Auth-bypass (Automation)	9.8	Huidige aankondiging; geen workaround
2026	CVE-2026-5174	Invoervalidatie (Automation)	8.8	Geketend met CVE-2026-4670

2

Waarom de architectuur blijft falen

MOVEit is een voor de categorie typisch managed-file-transfer-product: een webapplicatie die draait op door de klant beheerde Windows-infrastructuur, ondersteund door een SQL Server-database, optioneel met een Gateway-component ervoor en bestanden in rust op het lokale bestandssysteem of in Azure Blob Storage. Vier architecturale eigenschappen combineren tot het CVE-patroon.

De structurele lezing

Elk van de volgende vier eigenschappen is normaal voor de MFT-categorie. Gecombineerd op één vertrouwensgrens leveren ze de faalmodus die het CVE-overzicht documenteert.

1. Internet-blootgesteld webapplicatie-oppervlak

De openbare webinterface is nodig voor partnertoegang. Elke onthulde SQL-injectie, bypass van authenticatie of invoervalidatie-zwakte bereikt het platform via dit oppervlak.

2. Door de klant beheerde infrastructuur

Beveiliging hangt ervan af dat de klant Windows, IIS, SQL Server en het netwerk correct hardent. Elke verkeerde configuratie is een potentiële CVE in de besturingsomgeving.

3. Geen containment eenmaal binnen

Zodra een aanvaller RCE heeft, isoleert niets de applicatie van de database, de bestandsopslag of de Azure Blob-credentials. De schadestraal is totaal.

4. Patch-cyclus zonder workaround

Elke onthulde CVE vereiste een volledige installer-upgrade. Exploitatie waargenomen binnen enkele uren na onthulling in meerdere gevallen. De cyclus stapelt op.

3

Regelgevingsimplicaties

MFT-platforms staan op het knooppunt van gegevensuitwisseling voor gereguleerde workloads: beschermde gezondheidsinformatie onder HIPAA, gecontroleerde niet-geclassificeerde informatie onder CMMC en DFARS, kaarthoudergegevens onder PCI DSS, persoonsgegevens onder AVG en deelstatelijke privacywetten, financiële gegevens onder SOX en SEC-regels. Wanneer het MFT-platform het voertuig van het datalek is, draagt de klant de regelgevingsblootstelling -- niet Progress. Elke MOVEit-onthulling verkort bovendien de beschikbare regelgevingsverdediging: de Cl0p-campagne van 2023 was een zeroday, het authenticatie-bypass-paar van 2024 werd onthuld met werkende exploitcode op dag één, en bij de onthulling van 2026 staan meer dan 1.440 internet-blootgestelde instanties in risico.

Regime	Norm	Blootstelling	MOVEit-gerelateerde trigger
VS federaal	SEC Item 1.05 (dec. 2023)	Publieke 8-K-melding van materieel incident binnen 4 werkdagen	De SEC opende op 2 oktober 2023 een formeel onderzoek naar Progress
VS zorg	HIPAA Security Rule 45 CFR §164.308	OCR-standaard voor redelijke veiligheidsmaatregelen; civiele boetes tot 2,1 mln USD jaarplafond per overtredingsniveau	CMS/WPS-datalek gemeld bij OCR, raakte 3,1 mln personen
VS defensie	CMMC niveau 2 / DFARS 252.204-7012	C3PAO-beoordeling vereist; DoD-incidentmelding binnen 72 uur	Internet-blootgestelde MFT raakt rechtstreeks SC.L2-3.13.1, SC.L2-3.13.5, AC.L2-3.1.20
EU	Artikel 32 AVG + NIS 2 (okt. 2024)	Tot 4 % van de wereldwijde omzet; vroege waarschuwing in 24 u / incidentmelding in 72 u	De ICO legde Capita in okt. 2025 een boete van 14 mln £ op met verwijzing naar artikel 32
Australië	APP 11 + Privacy Amendment Act 2024	Tot 50 mln AUD of 30 % van de aangepaste omzet bij ernstige of herhaalde inbreuken	OAIC NDB-meldingen +25 % jaar-op-jaar in 2024; de Medibank-procedure schept precedent

„De vraag van de toezichthouder is niet of het datalek voorzienbaar was. Het is of het blijven uitvoeren van het platform na drie kwetsbaarheidsgolven in drie jaar een redelijke beveiligingsmaatregel is."

4

Het architecturale alternatief

MOVEit inwisselen voor een ander MFT-product zet de patch-cyclus-klok terug zonder het onderliggende model te veranderen. Het architecturale antwoord is een platform dat het gegevensuitwisselingsoppervlak consolideert op een gehard, single-tenant virtual appliance, met één policy-engine, één audit log en beveiliging als productcapaciteit in plaats van als klantconfiguratielast.

Gehard virtual appliance, geen door de klant beheerde infrastructuur

Kiteworks wordt uitgerold als een gehard virtual appliance met ingebouwde netwerk-firewall, ingebouwde web application firewall, ingebouwde intrusion detection en een uitgekleed besturingssysteem dat door Kiteworks wordt onderhouden. Klanten configureren het besturingssysteem niet, beheren de database niet en patchen de onderliggende stack niet apart. Volledige systeem-updates met één klik patchen het hele appliance -- applicatie, runtime, besturingssysteem, bibliotheken -- in één gecoördineerde handeling.

Defense in depth, aangetoond

Tijdens het Log4Shell-incident in december 2021 was de branche-NVD CVSS-score voor het onderliggende Log4j-lek 10,0.

De gelaagde controls van Kiteworks beperkten de praktische exploiteerbaarheid van Log4Shell in onze omgeving voordat de formele patch arriveerde. De interne beoordeling van Kiteworks schatte de resterende exploiteerbaarheid op ongeveer CVSS 4,0; dit cijfer is een interne schatting, geen door NIST of de CVE Numbering Authority officieel uitgegeven CVSS-score.

Defense in depth is hier niet theoretisch -- het is de reden waarom een NVD CVSS van 10 ingedamd bleef.

Single-tenant-isolatie en FIPS 140-3-encryptie

Elke Kiteworks-uitrol is single-tenant van opzet -- geen gedeelde databases, bestandssystemen of runtimes tussen klanten. Intern isoleert een gelaagde architectuur de weblaag van de database en de bestandsopslag, zodat een gecompromitteerde applicatielaag de database niet rechtstreeks kan bevragen en geen sleutels op bestandsniveau kan afleiden. Bestanden in rust worden beschermd door twee onafhankelijke encryptielagen (bestand- en schijfniveau) via FIPS 140-3-gevalideerde cryptografische modules, met TLS 1.3 in transit en optioneel klantgestuurd sleutelbeheer voor soevereiniteitsworkloads.

MOVEit-architectuur vs. Kiteworks-architectuur

Zes architecturale eigenschappen onderscheiden de twee platforms. Elk komt rechtstreeks overeen met een van de in het MOVEit-overzicht gedocumenteerde faalmodi. Datum publicatie van de vergelijking: 12 mei 2026. De karakterisering van MOVEit weerspiegelt het platform zoals door Progress gedocumenteerd op de datum van de aankondiging van 30 april 2026; productmogelijkheden en uitrolopties kunnen veranderen in latere Progress-versies.

Dimensie	MOVEit-architectuur	Kiteworks-architectuur
Infrastructuur	Door de klant beheerde Windows Server, IIS en SQL Server; OS en netwerk gehardent door de klant	Door Kiteworks onderhouden gehard virtual appliance; ingebouwde firewall, WAF en IDS; updates met één klik
Containment	De webapplicatie heeft directe toegang tot alle klantbestanden en tot de database	Gelaagde architectuur; de weblaag kan niet bij de bestandsopslag noch sleutels op bestandsniveau afleiden
Gegevensbescherming	Encryptie op applicatielaag; applicatielogs; SIEM-integratie is verantwoordelijkheid van de klant	FIPS 140-3-dubbellaagse encryptie (bestand + schijf); manipulatie-bestendig audit log; SIEM-levering in realtime
Bevoorrechte beheerderstoegang	De beheerconsole is het Windows-OS zelf, waardoor beheerders toegang hebben tot servercode en bestandssysteem en applicaties kunnen installeren. Aanvallers die bevoorrechte toegang tot de console krijgen, kunnen eigen code installeren voor taken zoals remote control en data-exfiltratie.	Beheerders hebben geen toegang tot het OS, het bestandssysteem, de applicatiecode of de database, die zich volledig binnen het geharde virtual appliance bevinden. De beheerconsole is een webinterface met strikte rolgebaseerde toegangscontroles (systeem, applicatie, support, custom); beheerderscapaciteiten manipuleren het systeem alleen via specifieke API-calls, en beheerders kunnen geen software installeren op het appliance.
Gebruikersbeheer	Gebruikt het Windows-gebruikersbeheer als applicatiegebruikersbeheer. Afhankelijk van de configuratie kan de schadestraal verder reiken dan de MOVEit-omgeving.	Speciaal ontworpen gebruikersbeheersysteem, volledig gescheiden van het gebruikersbeheer van het besturingssysteem
Patch-cadans	Drie kritieke golven in drie jaar; geen workarounds; nood-changevensters	Routine-leveranciers-patchevenement; de praktische exploiteerbaarheid van Log4Shell werd ingedamd door gelaagde controls voordat de patch arriveerde

Als u MOVEit Automation vandaag uitvoert

Vier acties die het waard zijn om deze week te ondernemen

- Patch naar MOVEit Automation 2025.1.5, 2025.0.9 of 2024.1.8 met de volledige installer -- Progress bevestigt dat er geen workaround is voor CVE-2026-4670 noch CVE-2026-5174.
- Inventariseer internet-blootgestelde Automation-instanties en bekijk audit logs op compromisindicatoren in de commandopoort-interfaces van de service-backend.
- Zet een architectuurreview op de eerstvolgende planningscyclus. De vraag is niet langer of er gepatcht wordt -- het is of het platformmodel verdedigbaar blijft na drie kritieke golven in drie jaar.
- Praat met Kiteworks over een architectuurreview van 30 minuten -- zie hoe een gehard, single-tenant appliance-model de schadestraal zou veranderen bij de volgende MFT-klasse-CVE.

Juridische disclaimer

Deze analyse is gebaseerd op publiek onthulde beveiligingsadviezen, derdenonderzoek en de architectuurbeoordeling van Kiteworks per 11 mei 2026. Technische kenmerken van producten van derden kunnen veranderen. Dit document vormt geen juridisch of beveiligingsadvies.

Kiteworks

Mei 2026

www.kiteworks.com