Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

NCSC-2026-0226

Kwetsbaarheden verholpen in Progress MOVEit Transfer

NCSC Security Advisory
Prioriteit: Normaal
Gepubliceerd op: 13-07-2026

TLP:WHITE

Toegestane verspreiding van TLP:WHITE
(Traffic Light Protocol)

Deze handreiking bevat het label TLP:WHITE en wordt door het NCSC verspreid. Het NCSC gebruikt het Traffic Light Protocol (TLP) om eenduidig te definiëren wat er met de informatie mag gebeuren. Wanneer informatie is voorzien van een TLP-aanduiding weet u met wie u deze informatie mag delen. Dit staat beschreven in de standaard First (www.first.org/tlp).

Ontvangers van TLP:WHITE mogen de informatie publiek verspreiden.

Uw reacties zijn welkom op info@ncsc.nl

Feiten

Progress heeft kwetsbaarheden verholpen in MOVEit Transfer, specifiek in de Custom Reports modules en de Ad Hoc module.

Duiding

De kwetsbaarheden betreffen meerdere versies van MOVEit Transfer, waaronder 25.0.0 tot en met 25.0.7, 25.1.0 tot en met 25.1.3, en 26.0.0 tot net voor 26.0.1. Eén kwetsbaarheid in de Custom Reports modules betreft een onjuiste neutralisatie van speciale elementen binnen data query logica, waardoor queryparameters gemanipuleerd kunnen worden wat kan leiden tot ongeautoriseerde data toegang of corruptie. Daarnaast is er een geheugenrelease-kwetsbaarheid in dezelfde modules die te maken heeft met de levensduur van geheugen, wat kan resulteren in onjuiste geheugenbeheer. Verder is er een cross-site scripting (XSS) kwetsbaarheid in de Ad Hoc module, veroorzaakt door onjuiste inputneutralisatie, waardoor kwaadaardige scripts kunnen worden geïnjecteerd en uitgevoerd binnen de context van de applicatie.

Oplossingen

Progress heeft updates uitgebracht voor MOVEit Transfer om deze kwetsbaarheden te verhelpen, waaronder versies 25.0.8, 25.1.4 en 26.0.1. Zie bijgevoegde referenties voor meer informatie.

Referenties

- https://community.progress.com/s/article/MOVEit-Transfer-Critical-Security-Bulletin-June-2026

Kwetsbaarheden

CVE	CVSS Score
CVE-2026-10698	**6.9 MEDIUM**
CVE-2026-10699	**6.9 MEDIUM**
CVE-2026-11903	**5.3 MEDIUM**

CWE's

CWE	Beschrijving
CWE-79	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')
CWE-401	Missing Release of Memory after Effective Lifetime
CWE-707	Improper Neutralization
CWE-943	Improper Neutralization of Special Elements in Data Query Logic

Getroffen producten

Progress
MOVEit Transfer

Disclaimer

The Netherlands Cyber Security Center (henceforth: NCSC-NL) maintains this page to enhance access to its information and security advisories. The use of this security advisory is subject to the following terms and conditions: NCSC-NL makes every reasonable effort to ensure that the content of this page is kept up to date, and that it is accurate and complete. Nevertheless, NCSC-NL cannot entirely rule out the possibility of errors, and therefore cannot give any warranty in respect of its completeness, accuracy or continuous keeping up-to-date. The information contained in this security advisory is intended solely for the purpose of providing general information to professional users. No rights can be derived from the information provided therein. NCSC-NL and the Kingdom of the Netherlands assume no legal liability or responsibility for any damage resulting from either the use or inability of use of this security advisory. This includes damage resulting from the inaccuracy of incompleteness of the information contained in the advisory. This security advisory is subject to Dutch law. All disputes related to or arising from the use of this advisory will be submitted to the competent court in The Hague. This choice of means also applies to the court in summary proceedings.