Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

NCSC-2024-0267

Kwetsbaarheden verholpen in Progress MOVEit

NCSC Advisory
Prioriteit: Normaal
Gepubliceerd op: 26-06-2024
Revisie: 1.0.1

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

Update Revisie 1

Addendum in verband met een recent ontdekte kwetsbaarheid in Third-Party component. Beveiligingsadvies is bijgewerkt met mitigerende maatregelen

Feiten

Progress heeft kwetsbaarheden verholpen in MOVEit Transfer en MOVEit Gateway. Tijdens het onderzoek naar de kwetsbaarheden is ook een kwetsbaarheid ontdekt in een niet nader benoemde Third-Party component dat in gebruik is door MOVEit Transfer.

Duiding

De kwetsbaarheden bevinden zich in de SFTP-module van de betreffende applicaties en stellen een kwaadwillende in staat om authenticatie te omzeilen en zo zonder voorafgaande authenticatie toegang te krijgen tot de bestanden die via de SFTP-dienst worden vrijgegeven.

Tijdens het onderzoek is een kwetsbaarheid ontdekt in een niet nader benoemde Third-Party component, dat in gebruik is bij MOVEit Transfer. Voor deze kwetsbaarheid is (nog) geen update beschikbaar. Wel zijn mitigerende maatregelen gepubliceerd om het risico op misbruik weg te nemen tot de update beschikbaar is. Deze kwetsbaarheid is niet aanwezig in MOVEit Gateway, omdat MOVEit Gateway geen gebruik maakt van deze Third-Party component.

Oplossingen

Progress heeft updates uitgebracht om de kwetsbaarheden te verhelpen in MOVEit Transfer en MOVEit Gateway.

Voor de (nog) niet verholpen kwetsbaarheid in de Third-Party component zijn mitigerende maatregelen vrijgegeven:

- Blokkeer inkomend RDP verkeer naar de MOVEit server(s) vanaf publieke netwerken.
- Beperk uitgaand verkeer vanaf de MOVEit server(s) tot uitsluitend vertrouwde endpoints.

Zie verder de bijgevoegde referenties voor meer informatie.

Referenties

› https://community.progress.com/s/article/MOVEit-Gateway-Critical-Security-Alert-Bulletin-June-2024-CVE-2024-5805
› https://community.progress.com/s/article/MOVEit-Transfer-Product-Security-Alert-Bulletin-June-2024-CVE-2024-5806

Kwetsbaarheden

CVE	CVSS Score
CVE-2024-5806	9.1 CRITICAL
CVE-2024-5805	9.1 CRITICAL

CWE's

CWE	Beschrijving
CWE-287	Improper Authentication

Getroffen producten

ipswitch
moveit
progress
moveit_gateway
moveit_transfer

Disclaimer