Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

NCSC-2025-0233

ZeroDay kwetsbaarheid ontdekt in Microsoft SharePoint Server

NCSC Advisory

PRIORITEIT: HOOG

Gepubliceerd op: 20-07-2025

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

Microsoft heeft informatie vrijgegeven over een actief misbruikte ZeroDay kwetsbaarheid in on-premises Microsoft SharePoint Server. Sharepoint Online (Microsoft 365) is niet geraakt.

Duiding

De ZeroDay kwetsbaarheid, geïdentificeerd als CVE-2025-53770, stelt een aanvaller in staat om ongeautoriseerde code uit te voeren op de kwetsbare SharePoint Server. Dit kan leiden tot ernstige beveiligingsrisico's. Microsoft ontwikkelt momenteel een update om deze kwetsbaarheid te verhelpen, maar biedt in de tussentijd mitigaties aan om gebruikers te helpen hun omgevingen te beschermen.

De kwetsbaarheid is een variant van de eerder actief misbruikte kwetsbaarheid met kenmerk `CVE-2025-49706`. Voor deze kwetsbaarheid heeft het NCSC beveiligingsadvies NCSC-2025-0215 uitgebracht, waarvoor op 19 juli een update is verschenen met kans en inschaling HIGH/HIGH [1]

Er is vooralsnog geen publieke exploit bekend, maar er wordt wel actief misbruik waargenomen. Wanneer Proof-of-Concept-code (PoC) of exploitcode publiek beschikbaar komt, verwacht het NCSC een significante toename in scanverkeer en pogingen tot misbruik.

[1] https://advisories.ncsc.nl/advisory?id=NCSC-2025-0215

Oplossingen

Microsoft werkt op dit moment aan updates om de kwetsbaarheid te verhelpen. Vooralsnog zijn uitsluitend mitigerende maatregelen beschikbaar om de risico's zo veel mogelijk te beperken. Het NCSC adviseert om met spoed onderstaande stappen te zetten in afwachting van een definitieve update:

- Zet de meest recente updates in, waaronder de updates van juli 2025 waarvoor het NCSC beveiligingsadvies NCSC-2025-0215 heeft gepubliceerd.
- Configureer de integratie met de Anti Malware Scan Interface (AMSI) binnen SharePoint. AMSI integratie is sinds september 2023 standaard actief, maar het is zinvol te controleren of integratie niet is uitgeschakeld in de tussentijd. Wanneer AMSI integratie actief is, is de kwetsbaarheid wel nog aanwezig, maar is misbruik niet mogelijk volgens Microsoft.
- Zet Defender AV in op alle sharepoint omgevingen.
- Indien AMSI uitgeschakeld is, en niet ingezet kan worden, adviseert Microsoft om de Sharepoint server **los te koppelen van het internet** en te wachten op de update om deze zo spoedig mogelijk in te zetten.

Zie verder bijgevoegde referenties voor meer informatie.

Referenties

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-53770
- https://msrc.microsoft.com/blog/2025/07/customer-guidance-for-sharepoint-vulnerability-cve-2025-53770/
- https://learn.microsoft.com/en-us/sharepoint/security-for-sharepoint-server/configure-amsi-integration

Kwetsbaarheden

CVE	CVSS Score
CVE-2025-53770	9.8 CRITICAL

CWE's

CWE	Beschrijving
CWE-502	Deserialization of Untrusted Data

Getroffen producten

Microsoft
Microsoft SharePoint Enterprise Server 2016
Microsoft SharePoint Server 2019
Microsoft SharePoint Server Subscription Edition

Disclaimer