Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

NCSC-2025-0233

Zeroday-kwetsbaarheden ontdekt in Microsoft SharePoint Server

NCSC Advisory

PRIORITEIT: HOOG

Gepubliceerd op: 23-07-2025
Revisie: 1.0.3

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 3

Microsoft heeft beveiligingsupdates beschikbaar gesteld om de kwetsbaarheden te verhelpen in SharePoint Server Subscription Service en SharePoint Server 2019. Voor SharePoint Server 2016 zijn vooralsnog geen beveiligingsupdates beschikbaar. Lees het handelingsperspectief voor meer informatie. Daarnaast is een ontbrekende CVE (CVE-2025-53771) en is informatie over actief misbruik aan dit beveiligingsadvies toegevoegd.

Feiten

Microsoft heeft informatie vrijgegeven over actief misbruikte zeroday-kwetsbaarheden in on-premises versies van Microsoft SharePoint Server. Sharepoint Online (onderdeel van Microsoft 365) is niet getroffen.

Duiding

De zeroday-kwetsbaarheden, met kenmerk CVE-2025-53770 en CVE-2025-53771, stellen een kwaadwillende in staat om willekeurige code uit te voeren op SharePoint Server-systemen. Kwaadwillenden kunnen op deze manier toegang krijgen tot gevoelige gegevens of verdere aanvallen op het netwerk van het slachtoffer uitvoeren.

Het NCSC heeft signalen ontvangen dat de kwetsbaarheden actief worden misbruikt. Naast Microsoft heeft onder andere beveiligingsbedrijf Eye Security hier op hun website over bericht. Tevens is proof-of-conceptcode (PoC) gepubliceerd waarmee de kwetsbaarheid met kenmerk CVE-2025-53770 kan worden misbruikt. Het NCSC heeft de werking van dit PoC niet geverifieerd, maar acht het aannemelijk dat het PoC functioneel is. Het is daarom de verwachting dat het aantal pogingen tot misbruik verder toeneemt.

De kwetsbaarheden zijn varianten van de eerder actief misbruikte kwetsbaarheden CVE-2025-49704 en CVE-2025-49706. Voor deze kwetsbaarheden heeft het NCSC beveiligingsadvies NCSC-2025-0215 uitgebracht, waarvoor op 19 juli een update is verschenen met kans en inschaling HIGH/HIGH.

Oplossingen

Microsoft heeft beveiligingsupdates uitgebracht voor SharePoint Server 2016, SharePoint Server 2019 en SharePoint Server Subscription Edition. Het NCSC adviseert dringend om de updates zo snel mogelijk te installeren. Op de website van Microsoft lees je hoe je dit doet. Let er hierbij op dat je je ASP.net-machinekeys roteert nadat je de updates hebt geïnstalleerd. Dit voorkomt dat een kwaadwillende eventuele eerder buitgemaakte machinekeys in de toekomst kan misbruiken en op die manier toegang tot de SharePoint-omgeving houdt.

Indien het niet mogelijk is om de beveiligingsupdates te installeren op de manier die Microsoft voorschrijft, adviseert het NCSC om de mitigerende maatregelen toe te passen zoals uitgelegd op de website van Microsoft. Let er ook hierbij op dat je je machinekeys roteert. Als het ook niet mogelijk is om de mitigerende maatregelen

toe te passen, adviseert het NCSC om de SharePoint-omgeving tijdelijk los te koppelen van het internet totdat de beveiligingsupdates op de juiste wijze zijn uitgevoerd.

Naast het installeren van de beveiligingsupdates, is het raadzaam om je SharePont-omgeving en netwerklogs op aanwezigheid van indicators-of-compromise (IOC's) te controleren. Hiermee kun je bepalen of je systeem mogelijk is gecompromitteerd. Verschillende cybersecuritybedrijven hebben IOC's gedeeld. Kijk in je netwerklogs of er netwerkverbindingen met de genoemde IP-adressen zijn opgezet, en controleer op je SharePoint-systeem of de genoemde malafide bestanden aanwezig zijn. IOC's zijn onder andere op de volgende websites te vinden:

- https://research.eye.security/sharepoint-under-siege/
- https://www.microsoft.com/en-us/security/blog/2025/07/22/disrupting-active-exploitation-of-on-premises-sharepoint-vulnerabilities/
- https://unit42.paloaltonetworks.com/microsoft-sharepoint-cve-2025-49704-cve-2025-49706-cve-2025-53770/
- https://www.bitdefender.com/en-us/blog/businessinsights/bitdefender-advisory-rce-vulnerability-microsoft-sharepoint-server-cve-2025-53770ce

Zie de 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
› https://research.eye.security/sharepoint-under-siege/

Kwetsbaarheden

CVE	CVSS Score
› CVE-2025-53770	9.3 CRITICAL
› CVE-2025-53771	5.3 MEDIUM

CWE's

CWE	Beschrijving
› CWE-502	Deserialization of Untrusted Data

CWE-707	Improper Neutralization
CWE-22	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')
CWE-20	Improper Input Validation

Getroffen producten

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

Disclaimer