Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

NCSC-2026-0004

Kwetsbaarheden verholpen in Trend Micro Apex Central

NCSC Advisory
Prioriteit: Normaal
Gepubliceerd op: 09-01-2026

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

Trend Micro heeft kwetsbaarheden verholpen in Trend Micro Apex Central.

Duiding

De kwetsbaarheden bevinden zich in de manier waarop Trend Micro Apex Central omgaat met bepaalde invoer. Een aanvaller kan een Denial-of-Service (DoS) veroorzaken zonder authenticatie door gebruik te maken van een ongecontroleerde NULL-retourwaarde. Daarnaast kunnen kwaadwillenden ongeauthenticeerde toegang krijgen om kwaadaardige DLL's in een cruciale uitvoerbare bestand te laden, wat kan leiden tot de uitvoering van willekeurige code met SYSTEM-rechten. Dit kan de integriteit en beveiliging van de getroffen systemen in gevaar brengen.

Oplossingen

Trend Micro heeft updates uitgebracht om de kwetsbaarheden te verhelpen. Zie bijgevoegde referenties voor meer informatie.

Referenties

- https://success.trendmicro.com/en-US/solution/KA-0022071

Kwetsbaarheden

CVE	CVSS Score
CVE-2025-69259	8.7 HIGH
CVE-2025-69260	8.7 HIGH
CVE-2025-69258	9.3 CRITICAL

CWE's

CWE	Beschrijving
CWE-120	Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')
CWE-290	Authentication Bypass by Spoofing

CWE-346	Origin Validation Error
CWE-427	Uncontrolled Search Path Element

Getroffen producten

Trend Micro
Apex Central

Disclaimer