Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

NCSC-2026-0387

Kwetsbaarheid verholpen in Check Point Security Management en Log Servers

NCSC Security Advisory
Prioriteit: Normaal
Gepubliceerd op: 23-09-2026

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

Check Point heeft een kwetsbaarheid verholpen in Security Management en Log Servers.

Duiding

De kwetsbaarheid betreft een pre-authentication directory-traversal-kwetsbaarheid in de Check Point Management Web Service, waarmee ongeauthenticeerde aanvallers scripts vanaf een willekeurig pad kunnen uitvoeren. De kwetsbaarheid kan leiden tot remote code execution en treft meerdere Check Point Management- en Logging-componenten. Check Point meldt dat de kwetsbaarheid actief wordt geëxploiteerd en heeft deze als zero-day aangemerkt. Volgens Check Point is sinds 23 juli 2026 actief misbruik waargenomen. Omdat de kwetsbaarheid vóór authenticatie kan worden uitgebuit, is het belangrijk dat de managementinterface niet rechtstreeks vanaf het internet toegankelijk is. Check Point adviseert specifiek om toegang tot TCP/19009 uitsluitend vanaf vertrouwde IP-adressen toe te staan.

Oplossingen

Check Point heeft updates uitgebracht om de kwetsbaarheden te verhelpen. Er is actief misbruik van de kwetsbaarheid waargenomen en Check Point heeft Indicators of Compromise (IoC's) gepubliceerd om mogelijke compromittering te detecteren. Raadpleeg de bijgevoegde referentie voor meer informatie, de beschikbare updates en de gepubliceerde IoC's.

Dreigingsinformatie

zie https://support.checkpoint.com/results/sk/sk1000171/ voor indicators of compromise.

Referenties

- https://blog.checkpoint.com/security/security-advisory-action-required-active-exploitation-of-cve-2026-85102-and-a-management-pre-authentication-vulnerability-cve-2026-93616/
- https://support.checkpoint.com/results/sk/sk1000171

Kwetsbaarheden

CVE	CVSS Score
CVE-2026-93616	9.8 CRITICAL

CWE's

CWE	Beschrijving
CWE-22	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')

Getroffen producten

Check Point
Multiple Products

Disclaimer