Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

NCSC-2026-0264

Kwetsbaarheden verholpen in Check Point Security Management producten

NCSC Security Advisory
Prioriteit: Normaal
Gepubliceerd op: 24-07-2026

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 kwetsbaarheden verholpen in SmartConsole, Gaia Portal, Security Management en Multi-Domain Security Management.

Duiding

De kwetsbaarheden betreffen authenticatiebypasses en privilege-escalaties binnen verschillende Check Point managementcomponenten.

- In SmartConsole kunnen niet-geauthenticeerde externe aanvallers administratieve login tokens verkrijgen, waardoor zij volledige administratieve toegang krijgen en beveiligingsbeleid kunnen aanpassen. Deze kwetsbaarheid vereist internettoegang tot de Management Server en een permissieve Trusted Clients configuratie.
- In Gaia Portal kan een geauthenticeerde gebruiker met alleen leesrechten commando's uitvoeren met root privileges, wat toegangsbescherming omzeilt.
- In Security Management en Multi-Domain Security Management kunnen niet-geauthenticeerde externe aanvallers met netwerktoegang tot de Management Server administratieve commando's uitvoeren, wat kan leiden tot controle over beheerde Security Gateways, afhankelijk van firewall- en Trusted Client-instellingen.

Checkpoint meldt dat van de kwetsbaarheid met kenmerk CVE-2026-16232 actief misbruik is waargenomen bij een beperkt aantal gebruikers die de kwetsbare tooling incorrect geconfigureerd hadden en publiek beschikbaar hadden op internet. Deze gebruikers zijn reeds geïnformeerd. Er is op dit moment nog geen verder misbruik waargenomen.

De genoemde applicaties zijn niet bedoeld om zonder additionele maatregelen publiek toegankelijk te hebben, maar af te steunen in een separate omgeving. Met name publiek toegankelijke systemen lopen een hoog risico op actief misbruik.

Oplossingen

Check Point heeft updates uitgebracht om deze kwetsbaarheden te verhelpen. Zie bijgevoegde referenties voor meer informatie.

Referenties

- https://support.checkpoint.com/results/sk/sk185152
- https://support.checkpoint.com/results/sk/sk185153
- https://support.checkpoint.com/results/sk/sk185169

Kwetsbaarheden

CVE	CVSS Score
CVE-2026-16232	10.0 CRITICAL
CVE-2026-62145	9.4 CRITICAL
CVE-2026-62144	10.0 CRITICAL

CWE's

CWE	Beschrijving
CWE-269	Improper Privilege Management
CWE-287	Improper Authentication

Getroffen producten

Check Point
Multi-Domain Security Management Server
Quantum Security Gateway, Quantum Security Management
Quantum Security Management, Multi-Domain Security Management
Security Management Server
SmartConsole

Disclaimer