



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

The Netherlands Cyber Security Center (henceforth: NCSC-NL) maintains this page to enhance access to its information and security advisories. The use of this security advisory is subject to the following terms and conditions: NCSC-NL makes every reasonable effort to ensure that the content of this page is kept up to date, and that it is accurate and complete. Nevertheless, NCSC-NL cannot entirely rule out the possibility of errors, and therefore cannot give any warranty in respect of its completeness, accuracy or continuous keeping up-to-date. The information contained in this security advisory is intended solely for the purpose of providing general information to professional users. No rights can be derived from the information provided therein. NCSC-NL and the Kingdom of the Netherlands assume no legal liability or responsibility for any damage resulting from either the use or inability of use of this security advisory. This includes damage resulting from the inaccuracy of incompleteness of the information contained in the advisory. This security advisory is subject to Dutch law. All disputes related to or arising from the use of this advisory will be submitted to the competent court in The Hague. This choice of means also applies to the court in summary proceedings.