

Alert Bulletin

Bulletin N.: 103

Publication Date: 18/09/2026

Subject: Alert 2026-103 Critical RCE Vulnerability as root in Check Point Security Management and Log Servers

Traffic Light Protocol (TLP): White

Affected product(s):

Product / component	Status
Check Point Security Management Server	Affected
Check Point Multi-Domain Security Management Server	Affected
Check Point Log Server	Affected
Check Point Multi-Domain Log Server	Affected
Standalone Deployments (Management + Gateway on the same machine)	Affected
Smart-1 Cloud	Not affected; the fix has already been deployed by Check Point

A server is considered vulnerable if it runs any of the following branches with the indicated **Jumbo Hotfix Take** or an earlier version:

Branch	Affected range	Recommended fix
R82.20	All builds	Install the <i>LivePatch</i> / urgent update available for R82.20
R82.10	Jumbo Hotfix Take 44 or earlier	Install the <i>LivePatch</i> or update to a later fixed Take
R82	Jumbo Hotfix Take 126 or earlier	Install the <i>LivePatch</i> or update to a later fixed Take
R81.20	Jumbo Hotfix Take 166 or earlier	Install the <i>LivePatch</i> or update to a later fixed Take
R81.10	Jumbo Hotfix Take 190 or earlier	EoS branch; request fix from Check Point Support or plan priority migration

Description

A vulnerability has been published in Check Point, labeled as **CVE-2026-91843**, a critical *stack-based buffer overflow* vulnerability in the login process of its management and log servers. The flaw has a **CVSS 9.8** score and could allow an unauthenticated remote attacker to execute arbitrary code with **root** privileges.

CVE-2026-91843 is a stack-based buffer overflow vulnerability, classified as **CWE-121**, in the login process of Security Management Server and Log Server. The vulnerable condition occurs **before authentication**: a remote attacker can send a login request with an excessively long username and trigger the overflow.

The vulnerable path is associated with the **Trusted Clients** mechanism, which defines which machines can connect to the management server via SmartConsole. According to Check Point, the vulnerability is reachable only through this trusted clients configuration. A permissive configuration, especially if it uses the **"Any"** value or allows access from the Internet, significantly increases the attack surface.

A successful compromise of a Management Server is especially serious because this component controls security policies, gateway configuration, network objects, credentials, and administrative access for the Check Point ecosystem. Execution as root could allow modifying firewall policies, introducing unauthorized access rules, altering logs, extracting configurations, and using the server as a pivot point toward gateways and other managed assets.

The vendor recommends immediately applying the fix via **Check Point LivePatch** or the corresponding offline update package. At the time of publication, Check Point indicated that it had no evidence of active exploitation and CISA recorded the exploitation status as "none"; however, because this is a pre-authentication, remote flaw with root execution on management infrastructure, remediation should be considered the highest priority.

Solution

The main solution is to apply the *LivePatch* indicated in advisory **sk1000155**. Machines with automatic updates enabled per Check Point configuration may receive the fix automatically, but administrators should verify its installation using *cplp list*.

<https://support.checkpoint.com/results/sk/sk1000155>

For environments without LivePatch or automatic updates, Check Point provides urgent offline update packages. **Take 29** packages are reported for R82.20 and **Take 28** for R82.10, R82, and R81.20; confirm the exact applicable package from the support portal and the advisory before deploying it.

There is no mitigation that replaces applying the patch. Restricting Trusted Clients, removing "Any", and closing direct Internet access are important compensating controls, but the *LivePatch* must be installed as a priority.

Additional information:

- <https://support.checkpoint.com/results/sk/sk1000155>
- <https://www.cve.org/CVERecord?id=CVE-2026-91843>
- <https://thehackernews.com/2026/09/critical-check-point-management-server.html>