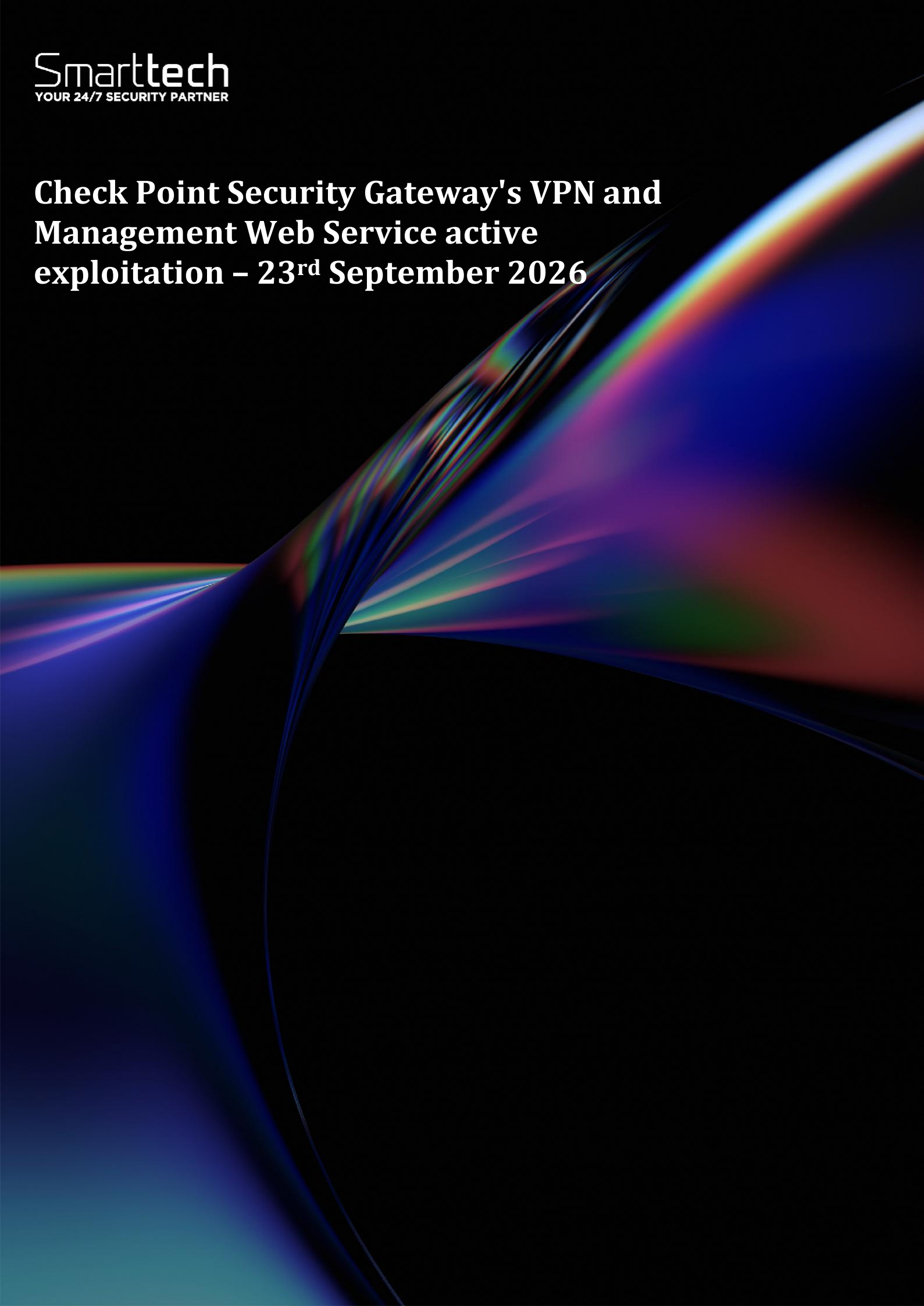


# **Check Point Security Gateway's VPN and Management Web Service active exploitation – 23<sup>rd</sup> September 2026**



|                 |                                                                                                       |
|-----------------|-------------------------------------------------------------------------------------------------------|
| Document ID     | SMA-Threat Report                                                                                     |
| Document status | ISSUED                                                                                                |
| Issue Number    | 170                                                                                                   |
| Authors         | Alex Ciuta < <a href="mailto:alexandru.ciuta@smarttech247.com">alexandru.ciuta@smarttech247.com</a> > |
| Verified by     | Alin Curcan < <a href="mailto:alin.curcan@smarttech247.com">alin.curcan@smarttech247.com</a> >        |
| Last modified   | 2026-09-23                                                                                            |
| Issue Date      | 2026-09-23                                                                                            |

**Threat Reports** are reports created by Smarttech247 based on high and critical severity vulnerabilities that may have a high potential to be exploited in the wild i.e. vulnerabilities that are present in most used products by companies and do not have an auto-update option or they are usually not automatically updated in case that could lead to some service disruption. This report is usually created as soon as the vulnerability is released, therefore we strongly recommend that the information is reviewed, tests are performed and patches are applied before the first proof-of-concept is released. Even though certain vulnerabilities may not have an active exploit in the wild at the time that we report on them, we take into consideration the wider risk and the impact it could have on systems, should an exploit like that be available after a while. Our duty is to report them on time and we recommend enterprises that, in order to keep critical business systems protected, they should consider, on average, ten working days to check whether or not the new vulnerability affects them, and if so, to implement actions in order to remove the risk.

## Overview:

Multiple critical vulnerabilities have been identified in Check Point Quantum Security Gateway, Security Management Server, and Spark Firewall. CVE-2026-85102 is a pre-authentication remote code execution vulnerability caused by improper validation of certificate data during VPN negotiation, while CVE-2026-93616 is a pre-authentication path traversal vulnerability in the management web service that can allow arbitrary script execution and Java class loading on affected management servers. Both vulnerabilities carry a CVSS score of 9.8 and have been observed in exploitation activity, with CVE-2026-85102 targeting VPN-enabled devices and CVE-2026-93616 exploited in limited targeted attacks.

## Risk

Government:

- Large and medium government entities: **Critical**
- Small government entities: **Critical**

Businesses:

- Large and medium business entities: **Critical**
- Small business entities: **Critical**

## Technical summary

More details related to this vulnerability are as follows:

| CVE ID                                               | Description                                                                                                                             |
|------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------|
| <b>CVE-2026-85102</b><br><b>CVSS Base Score: 9.8</b> | Improper validation of certificate data during VPN negotiation allows unauthenticated remote code execution                             |
| <b>CVE-2026-93616</b><br><b>CVSS Base Score: 9.8</b> | Pre-authentication path traversal in Check Point management web service, leading to arbitrary-path script execution and Java class load |

## Affected Products

- Security Gateway, Spark Firewall (Centrally Managed),
- Spark Firewall (Locally Managed),
- Spark Firewalls:
  - R80.20.X (EOS),
  - R81.10.X,
  - R82.00.X
- Security Management

## Observed Attacks

### CVE-2026-85102

Starting September 12, 2026, CheckPoint observed a wave of exploitation attempts against Spark customers. The attempts originated from anonymization infrastructure, including VPN services and proxies, and used certificates with the following subjects:

CN=vpn,OU=users,O=global

CN=vpn-user,OU=users,O=global

CN=vpnuser,OU=users,O=global

### CVE-2026-93616

## Symptoms

### CVE-2026-85102

- Issue: Improper validation of certificate data during VPN negotiation may allow an unauthenticated remote attacker to execute arbitrary code on the Security Gateway.
- This issue received the ID CVE-2026-85102 with CVSS: 9.8.
- For Site-to-Site VPN, the issue affects Security gateways that use or allow certificate-based authentication.  
Note: VPN with Dynamic IP Gateways (DAIP) or Large Scale VPN (LSV) Gateways in the community enables certificate authentication. Gateways that participate only in encryption communities where authentication is based on a Pre-Shared Key are not vulnerable.
- Update (September 20, 2026): This vulnerability is actively exploited on Spark Firewalls as of September 12, 2026.
- Update (September 14, 2026): Important notification for customers who installed the Offline LivePatch Package and are running:
  - R82.10 Jumbo Hotfix Take 24 or lower
  - R82 Jumbo Hotfix Take 107 or lower
  - R81.20 Jumbo Hotfix Take 146 or lower
- Following additional research, we identified a rare scenario in which customers must install Check Point Live Patch Take 26, which provides enhanced coverage for this CVE.

- Affected Products: Security Gateway, Check Point Spark Firewall using Site to Site VPN or Remote Access VPN
- Affected Versions:
  - R81.20, R82, R82.10
  - R80, R80.10, R80.20, R80.30, R80.40, R81, R81.10 (all EoS)
  - R81.10.x, R82.00.x
- Not Affected Versions: R82.20

## **CVE-2026-93616**

- A directory traversal and file upload vulnerability allows an unauthenticated attacker to upload and execute arbitrary scripts on the Check Point Management Server.
- This vulnerability is exploited in the Wild. Check Point is aware of a handful of customers who have been attacked.
- This issue received the ID CVE-2026-93616 and a CVSS score of 9.8.
- Affected Products: Security Management Server, Multi-Domain Security Management Server, Log Server, Multi-Domain Log Server, SmartEvent.
- Not Affected Products: Smart-1 Cloud (fix is already applied), Check Point Firewall Appliances, Check Point Spark Firewall.
- Affected Versions:
  - R82.20
  - R82.10 Jumbo Hotfix Take 44 or lower
  - R82 Jumbo Hotfix Take 126 or lower
  - R81.20 Jumbo Hotfix Take 166 or lower
  - R81.10 Jumbo Hotfix Take 190 or lower (EoS)
  - R80, R80.10, R80.20, R80.30, R80.40, R81 (all EoS)
- Note: Check Point LivePatch Take 28/29 does not address this issue.

## **Mitigation**

### **CVE-2026-85102**

Use this mitigation only if the affected system cannot be updated through Jumbo Hotfix Accumulator or Check Point LivePatch. Exercise caution when disabling VPN implied rules and configuring explicit rules, as an incorrect configuration can cause connectivity issues.

**For Site to Site VPN**, disable implied rules for VPN and manually define VPN access for UDP/500 and UDP/4500 for the specific peer IP addresses. Refer to sk179346.

#### **For Remote Access VPN:**

Disable the Remote Access VPN implied rules. Create explicit Access Control rules that allow the required Remote Access VPN services to the Security Gateway:

- UDP/500 (IKE), UDP/4500 (NAT-T), TCP/443 (SSL), TCP/80 (when applicable)
- Specify the source of the Remote Access clients' IP address ranges if applicable.

Note: These mitigation options are not applicable to the locally managed Spark Firewall.

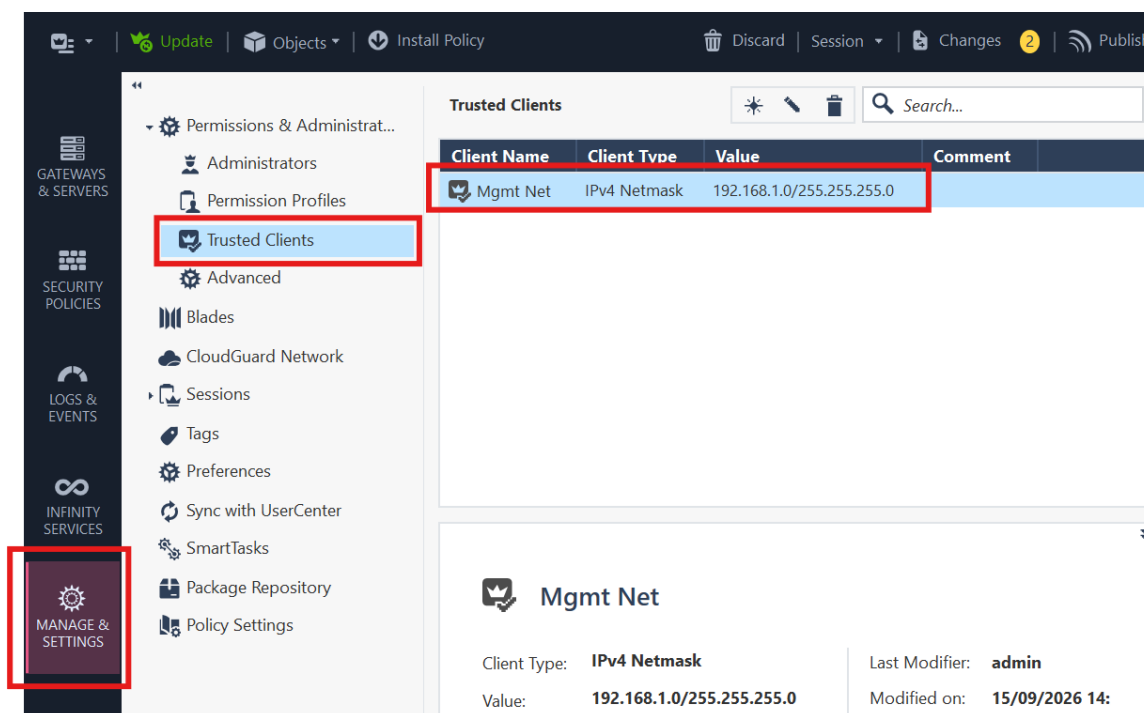
## CVE-2026-93616

Limit access to your Management Servers behind a Security Gateway/Check Point Firewall according to the Check Point Gateway and Management Hardening Administration Guide.

- Make sure that access to port TCP/19009 is only possible from Trusted IP addresses.
- If you already have a Security Gateway / Check Point Firewall with implied rules enabled, make sure your Trusted Clients are limited to trusted internal IP addresses. This will create an Implied rule limiting access.

To do so:

1. In SmartConsole, go to Manage & Settings > Permissions & Administrators > Trusted Clients.
2. Double-click the client you want to edit.
3. In the Trusted Client configuration window that opens, change the settings as needed.
4. Click OK.



## Solution

## CVE-2026-85102

Option 1: The fix is included in Check Point LivePatch

## Automatic installation

If you have enabled automatic installation of Check Point LivePatch, the protection will be applied automatically.

## Manual installation

Download the offline package.

To validate that LivePatch is properly installed and active, run the `cpinfo -y CPupdates` command on the Security Gateway / ClusterXL member in Expert mode and validate that you have `BUNDLE_URGENT_SECURITY_UPDATE_R82_AUTOUPDATE` Take 26

### Example:

```
[Expert@Host:0]# cpinfo -y CPupdates
[CPupdates]
    BUNDLE_URGENT_SECURITY_UPDATE_R82_AUTOUPDATE    Take: 26
```

### For LivePatch validation, run in Expert mode:

On a Security Gateway / ClusterXL member: `cppl list`  
On a Scalable Platform Security Group: `g_all cppl list`

### Expected output:

```
cpcert:cpca*      CVE-2026-85102 CVE-2026-85103
cpcert:iked*      CVE-2026-85102 CVE-2026-85103
cpcert:vpn*       CVE-2026-85102 CVE-2026-85103
cpcert:vpnrad*    CVE-2026-85102 CVE-2026-85103
cpcert_cpriid:cprid* CVE-2026-85102 CVE-2026-85103
```

### Option 2: The fix is also included in:

- Jumbo Hotfix Accumulator for R82.10 starting from Take 44
- Jumbo Hotfix Accumulator for R82 starting from Take 126
- Jumbo Hotfix Accumulator for R81.20 starting from Take 166
- Jumbo Hotfix Accumulator for R81.10 starting from Take 190
- Check Point Spark Firewalls R82.00.10 starting from Build 2325
- Check Point Spark Firewalls R81.10.17 starting from Build 4968

## CVE-2026-93616

This problem was fixed.

- Download the R82.20 Security Hotfix (TAR)

The fix is also included in:

- Jumbo Hotfix Accumulator for R82.10 starting from Take 45
- Jumbo Hotfix Accumulator for R82 starting from Take 127
- Jumbo Hotfix Accumulator for R81.20 starting from Take 170

- Jumbo Hotfix Accumulator for R81.10 starting from Take 192

Notes:

- These Jumbo Hotfix Accumulators also include the fix for CVE-2026-91843 (sk1000155).
- Because of the nature of the fix, a LivePatch is not be available for this issue.

## Recommendations

**Smarttech247 team** recommend the following actions be taken:

- Apply the appropriate patches, hotfixes or appropriate mitigations provided by Check Point to vulnerable systems immediately after appropriate testing.
- Upgrade software and operating systems, applications, and firmware on network assets in a timely manner for prevention.
- Use the right Vulnerability Management Tools to assess endpoint, networks or applications for known weaknesses.
- Apply the Principle of Least Privilege to all systems and services.
- Apply advanced application control and protection to enforce granular control over all application access, communications, and privilege elevation attempts.
- Kindly ensure that your Endpoint Security and Perimeter security products are updated with the latest signatures to detect these threats.

## References

<https://blog.checkpoint.com/security/security-advisory-action-required-active-exploitation-of-cve-2026-85102-and-a-management-pre-authentication-vulnerability-cve-2026-93616/amp>  
<https://support.checkpoint.com/results/sk/sk1000171/>  
<https://support.checkpoint.com/results/sk/sk1000117>

## CVE

CVE-2026-85102  
CVE-2026-93616

