



Your IT Company

Boletim de Inteligência - Vulnerabilidades Críticas no Check Point

	Boletim de Inteligência - Vulnerabilidades Críticas no Check Point Cyber Threat Intelligence	Código
		SGSI-081
		Página
		2 de 6

ÍNDICE

1. Descrição da vulnerabilidade.....	3
2. Exploração.....	3
3. Impactos potenciais.....	3
4. IOCs e artefatos	4
5. Mitigação e prevenção	5
8. Considerações finais	5
9. Referências Técnicas	6

	Boletim de Inteligência - Vulnerabilidades Críticas no Check Point Cyber Threat Intelligence	Código
		SGSI-081
		Página
		3 de 6

1. Descrição da vulnerabilidade

A Check Point confirmou a exploração ativa de duas vulnerabilidades críticas de pré-autenticação em sua infraestrutura de segurança. A CVE-2026-85102 afeta o processamento de certificados durante negociações VPN e pode permitir execução remota de código sem autenticação. A CVE-2026-93616, por sua vez, afeta o serviço web do Security Management e permite exploração de path traversal e upload de arquivos/scripts, também sem autenticação. Ambas possuem uma avaliação crítica CVSS 9.8.

A situação é especialmente relevante porque a Check Point confirmou atividade maliciosa real: tentativas contra Spark Firewall começaram em 12 de setembro de 2026, enquanto a CVE-2026-93616 foi explorada em ataques direcionados já em 23 de julho de 2026, antes da disponibilização da correção.

2. Exploração

A exploração dessas vulnerabilidades pode gerar impactos críticos para o ambiente corporativo:

- **CVE-2026-85102 - VPN:** A vulnerabilidade ocorre durante o processamento de certificados utilizados na negociação de conexões VPN. Um atacante remoto pode enviar dados especialmente manipulados para explorar a falha antes da autenticação. Em caso de exploração bem-sucedida, o atacante pode obter execução de código no equipamento, utilizar o gateway comprometido para realizar reconhecimento da rede interna e tentar acessar outros serviços.
- **CVE-2026-93616 - Security Management:** A falha está relacionada a um problema de Path Traversal no serviço web do Check Point Security Management. Um atacante não autenticado pode manipular requisições para acessar locais indevidos no sistema e carregar arquivos ou scripts controlados por ele, podendo resultar em execução de código no servidor de gerenciamento. Por ser um componente responsável pelo gerenciamento centralizado da infraestrutura Check Point, seu comprometimento pode ampliar significativamente o impacto de um ataque.

3. Impactos potenciais

A exploração pode permitir:

- Execução remota de código;
- Comprometimento de gateways e servidores de gerenciamento;

	Boletim de Inteligência - Vulnerabilidades Críticas no Check Point Cyber Threat Intelligence	Código
		SGSI-081
		Página
		4 de 6

- Acesso não autorizado à infraestrutura;
- Alteração de configurações e políticas de segurança;
- Criação ou modificação de arquivos e scripts;
- Reconhecimento da rede interna;
- Movimentação lateral;
- Comprometimento de credenciais;
- Possível comprometimento de outros dispositivos administrados pelo Management Server.

4. IOCs e artefatos

1. CVE-2026-85102

Durante a investigação, recomenda-se verificar:

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

• Também devem ser analisadas:

- Sessões VPN não reconhecidas;
- Autenticações por certificados desconhecidos;
- Conexões originadas de VPNs, proxies ou redes incomuns;
- Atividades de varredura realizadas após uma conexão VPN.

2. CVE-2026-85102

Buscar nos logs e artefatos por:

```
../
ReflectionUtils
allResourceFiles
cpm.elg
```

- Também devem ser investigados **arquivos, scripts, processos ou alterações administrativas inesperadas** no Security Management Server.

	Boletim de Inteligência - Vulnerabilidades Críticas no Check Point Cyber Threat Intelligence	Código
		SGSI-081
		Página
		5 de 6

5. Mitigação e prevenção

As seguintes medidas devem ser priorizadas:

- Aplicar imediatamente os hotfixes de segurança disponibilizados pela Check Point;
- Identificar todos os equipamentos que utilizam versões vulneráveis;
- Restringir o acesso ao Security Management Server somente às redes administrativas necessárias;
- Evitar a exposição direta do Management Server à Internet;
- Restringir portas e serviços administrativos a endereços autorizados;
- Revisar configurações de VPN e autenticação por certificados;
- Monitorar os logs em busca de autenticações e atividades anômalas.

Recomendações para administradores:

- Realizar um inventário das versões e *Jumbo Hotfix Takes* instalados;
- Priorizar equipamentos expostos à Internet;
- Revisar sessões e autenticações VPN recentes;
- Verificar alterações não autorizadas em políticas, usuários e configurações;
- Correlacionar eventos do Check Point com SIEM, firewall, VPN e demais fontes de logs;
- Investigar arquivos e processos desconhecidos no Management Server;
- Preservar evidências caso seja identificada atividade suspeita;
- Avaliar a rotação de credenciais administrativas caso haja indícios de comprometimento.

8. Considerações finais

As vulnerabilidades apresentam alta relevância para organizações que utilizam produtos Check Point, devido à combinação de severidade crítica, exploração pré-autenticação e evidências de exploração ativa.

A CVE-2026-85102 representa um risco direto aos serviços VPN, enquanto a CVE-2026-93616 merece atenção especial por atingir o servidor responsável pelo gerenciamento centralizado da infraestrutura.

Recomendação principal: aplicar as correções disponibilizadas pela Check Point com prioridade, reduzir a exposição dos equipamentos e realizar análise retrospectiva dos logs para verificar possíveis sinais de comprometimento anteriores à aplicação das correções.

	Boletim de Inteligência - Vulnerabilidades Críticas no Check Point Cyber Threat Intelligence	Código
		SGSI-081
		Página
		6 de 6

9. Referências Técnicas

Para saber informações mais detalhadas sobre este tema, acesse:

- <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://gbhackers.com/hackers-exploit-check-point-0-day-flaw/>
- https://cybersecuritynews.com/hackers-exploit-critical-check-point-vpn-flaws/#google_vignette
- <https://thehackernews.com/2026/09/check-point-warns-of-management-server.html>

Esta publicação tem como objetivo orientar a equipe interna e os nossos clientes sobre ameaças emergentes no ambiente cibernético, possibilitando assim ações proativas de prevenção para tornar a infraestrutura de nossas empresas cada vez mais segura.

Produzido por: Equipe de Cyber Threat Intelligence