GT13 campaign compromises Check Point management servers at 22 organizations



GreyNoise reports an ongoing campaign, tracked as GT13, that compromised 24 Check Point security management servers at 22 organizations in 17 countries. Attackers used the SmartConsole authentication bypass CVE-2026-16232, disclosed in July.

- 22 organizations across 17 countries were affected, including government, financial services, energy, transportation, mining and manufacturing.
- Attackers used CVE-2026-16232, a SmartConsole authentication bypass that yields administrator access; Check Point disclosed it in July as exploited in the wild.
- Activity included theft of firewall databases, credentials, configuration data and internal certificate authority files, and unloading of security policies.
- GreyNoise lost visibility on November 2 but believes the campaign may still be active, and has

shared indicators of compromise.

- Check Point states the vulnerability and protections are not new and that the exploit adapts a public Metasploit module.

Threat intelligence firm GreyNoise has described an ongoing campaign, which it tracks as GT13, in which attackers compromised 24 Check Point security management servers belonging to 22 organizations. The victims are spread across 17 countries and show no clear sign of specific targeting. They include government bodies, financial services providers, and companies in energy, transportation, mining and manufacturing.

What was observed

GreyNoise confirmed activity between October 17 and November 2, when its visibility ended, and believes the campaign may still be running because the actor retains access. During post-compromise stages it saw exploitation of **CVE-2026-16232**, an authentication bypass in Check Point SmartConsole that lets an attacker obtain a login token and authenticate as an administrator. GreyNoise could not establish when or how the servers were first breached.

Recorded actions included stealing firewall databases, credentials, configuration data and internal certificate authority files, generating a new certificate in one environment, unloading security policies so that firewall protection was effectively disabled, and internal reconnaissance with attempted lateral movement. The attackers also probed other enterprise products, including Citrix NetScaler, Ivanti, VMware vCenter, Microsoft Exchange and Netlogon.

Vendor position

Check Point says the flaw was publicly disclosed in July 2026 with a note that exploitation had been seen in the wild, so the vulnerability and available protections are not new. It adds that the attackers used an adaptation of a public Metasploit module. GreyNoise has notified government partners and CERTs and published indicators of compromise. It assesses that an AI-powered tool may have been used, but this is unconfirmed.

Implications

A compromised management server can expose policies, credentials and certificate trust across an estate, so institutions running SmartConsole should confirm patching and review for signs of misuse.

What to do now

1. Confirm that Check Point SmartConsole and management servers have the fixes for CVE-2026-16232 applied, and restrict management interface access to trusted networks.
2. Hunt for the GreyNoise indicators of compromise in firewall, VPN and management logs, including the

listed IP addresses.

3. Review management servers for unexpected administrator sessions, newly generated certificates, unloaded security policies and configuration exports.
4. If compromise is suspected, rotate credentials and review the internal certificate authority and its issued certificates.
5. Check patch status of other exposed products named in the report, such as Citrix NetScaler, Ivanti, VMware vCenter and Microsoft Exchange.
6. Report confirmed incidents to the National Cybersecurity Authority and your sector regulator as required.