AI-assisted campaign compromises Check Point Security Management servers, GreyNoise reports



GreyNoise reports that actor GT13 used AI-enabled tools against Check Point Security Management servers, affecting at least 22 organizations. The firm believes the campaign is likely ongoing because the actor kept persistent access.

- GreyNoise tracks the actor as GT13, active since early October, using 99 IP addresses linked to ExpressVPN egress or compromised Check Point devices.
- At least 22 organizations were targeted, across energy, finance, government, manufacturing, mining, transport and other sectors in many countries.
- GreyNoise believes agentic systems automated vulnerability weaponization, scanning and exploitation, supported by hands-on-keyboard work.
- The actor held access to the Check Point servers before compromising a separate HFS server; how

that first access was gained is unknown.

- Activity was observed between October 17 and November 2, but persistent access suggests the campaign may continue.

GreyNoise, a threat intelligence firm, has described a campaign against Check Point Security Management servers by an actor it calls GreyNoise Threat 13 (GT13). The firm began tracking it in early October and believes it is likely still ongoing.

What was observed

GT13 ran scanning, exploitation and control activity from 99 IP addresses, all of which were either ExpressVPN egress points or compromised Check Point devices. GreyNoise counted more than 1,400 network sessions, more than 800 command-line artifacts and more than 1,200 files downloaded, uploaded or created. At least 22 organizations were targeted.

In one case, the actor forged a signed admin session cookie to gain administrative access to an HFS server, then obtained SSH access, scanned the environment and exfiltrated data. Tools included Nmap, Chisel, Impacket and Paramiko, used for reconnaissance, lateral movement and privilege escalation. One victim's server served as a hop holding data taken from 24 compromised Check Point Security Management servers.

Why it matters

GreyNoise believes separate agentic systems weaponize vulnerabilities, find exposed assets and exploit them automatically, with operators working by hand alongside. The actor had access to the Check Point servers before the HFS compromise, and GreyNoise could not determine when or how. Because GT13 kept persistent access, the campaign may continue even though observation stopped on November 2.

The source lists many CVEs used or attempted in one victim's environment, across Rejetto HFS, Citrix NetScaler, Ivanti, Check Point SmartConsole, Linux, Windows NetLogon, Microsoft Exchange and VMware vCenter. Security management servers hold high-value administrative control, so institutions running them should check their exposure calmly and methodically.

What to do now

1. Check whether Check Point Security Management servers are reachable from the internet and restrict management access to trusted networks.
2. Review logs on these servers for unexpected SSH keys, bulk certificate-management tasks and outbound scp transfers.
3. Hunt for the tools named by GreyNoise (Nmap, Chisel, Impacket, Paramiko) and unexpected Python scripts on management and adjacent servers.
4. Verify patch status for the CVEs listed in the source across HFS, Citrix, Ivanti, Check Point SmartConsole,

Windows, Exchange and vCenter.

5. Rotate administrative credentials, session secrets and SSH keys if any compromise indicator is found, and follow your incident process and NCA notification duties.