Unpatched Check Point Gateways Targeted in PHP2Shell Attacks Delivering TSGA Backdoor



Check Point reports an unknown actor exploiting PHP2Shell flaws on unpatched Security Gateways, then a Gaia OS privilege escalation flaw, to deploy the TSGA backdoor. Activity began on October 30, 2026.

- The attacker targets unpatched Check Point Security Gateways for initial access through the PHP2Shell vulnerabilities.
- A previously reported local privilege escalation flaw in Gaia OS is then used to deploy the TSGA backdoor.
- Check Point says the activity began on October 30, 2026, and first targeted Israeli organizations.
- A broader follow-up wave has been observed; the headline also refers to wiping of ESXi files.
- The actor has not been identified.

Check Point has detailed an intrusion campaign in which an unknown threat actor targets Security Gateways that have not been patched. Initial access is obtained through the PHP2Shell vulnerabilities, after which the attacker uses a previously reported local privilege escalation flaw in Gaia OS to install a backdoor called TSGA.

What is known

According to Check Point, the activity began on October 30, 2026 and initially targeted Israeli organizations. A broader follow-up wave was observed afterwards. The source headline also states that ESXi files were wiped, but the excerpt available to us does not explain how or in which environments, so we do not draw conclusions on that point.

The excerpt does not provide CVE identifiers, patch versions or indicators of compromise. These should be taken directly from Check Point's own advisory.

Why it matters for Saudi institutions

Security gateways sit at the network edge and are trusted components. A compromised gateway gives an attacker a strong position, and the reported mention of ESXi file wiping points to possible impact on virtualized infrastructure. Institutions running Check Point gateways should treat this as a prompt to verify patch status rather than as a cause for alarm.

Recommended approach

Confirm which gateways are in use, compare them against Check Point's published fixes, and review recent activity for signs of the TSGA backdoor. Keep the work within existing change and incident-handling procedures.

What to do now

1. Inventory all Check Point Security Gateways and their Gaia OS versions.
2. Apply the fixes Check Point has published for the PHP2Shell vulnerabilities and the Gaia OS privilege escalation flaw.
3. Hunt for TSGA indicators using Check Point's published guidance and review gateway logs since late October 2026.
4. Verify ESXi backups are recent, offline or immutable, and restorable.
5. Restrict management access to gateways and brief your incident response team on this campaign.