Reported: Check Point gateways abused via PHP2Shell to deliver a VMware ESXi wiper



BleepingComputer reports that Check Point gateways were compromised using PHP2Shell to deploy a wiper aimed at VMware ESXi. Only the headline was readable, so institutions should verify details with the vendor.

- BleepingComputer reports Check Point gateways were hacked using something called PHP2Shell.
- The reported end goal was deploying a wiper against VMware ESXi.
- The article text was not readable on our side, so technical details, affected versions and scope are unconfirmed.
- Gateways and hypervisors are both high-value infrastructure for regulated institutions.

What was reported

BleepingComputer published a report under the headline "Check Point gateways hacked via PHP2Shell to deploy VMware ESXi wiper". According to that headline, attackers compromised Check Point gateways using PHP2Shell and used that access to deploy a wiper targeting VMware ESXi.

What we could not confirm

The body of the source article was not readable when we prepared this item. We therefore cannot state which products or versions are affected, how the gateways were accessed, who is behind the activity, how many organisations are involved, or whether a fix or CVE exists. We have not filled these gaps with assumptions. Please consult the original article and Check Point and Broadcom (VMware) advisories directly.

Why it matters

Perimeter gateways are exposed by design, and ESXi hosts often run many business-critical virtual machines. A destructive tool aimed at the hypervisor layer, if delivered as described, would threaten availability and recovery rather than only confidentiality. This makes recovery readiness as important as patching.

A calm, proportionate response is to confirm your exposure, check vendor guidance, and validate that your backups and segmentation would hold up if a gateway were compromised. No panic measures are needed until the vendors publish specifics.

What to do now

1. Identify all Check Point gateways in your estate and confirm owners, versions and management exposure.
2. Monitor Check Point and Broadcom (VMware) security advisories and apply guidance as soon as it is published.
3. Review gateway and ESXi host logs for unusual administrative activity or unexpected files, and escalate findings to your SOC.
4. Verify that ESXi backups are offline or immutable and that a restore test has succeeded recently.
5. Confirm that ESXi management interfaces are segmented from gateways and not reachable from untrusted networks.
6. Update incident response and BCM plans with a scenario for destructive attacks on virtualisation infrastructure.