

Check Point Management Products Vulnerable to Unauthenticated Path Traversal Attack



Check Point Security Management Server and related products contain a path traversal vulnerability allowing unauthenticated attackers to upload and execute arbitrary scripts.

- Multiple Check Point management products affected including Security Management Server, Multi-Domain Security Management Server, Log Server, Multi-Domain Log Server, and SmartEvent
- Vulnerability permits unauthenticated attackers to upload and execute arbitrary scripts via path traversal
- CISA requires federal agencies to apply vendor mitigations by 25 September 2026
- Organizations must evaluate internet exposure of affected assets and prioritize patching
- Discontinuation of product use recommended if vendor mitigations are unavailable

Vulnerability Overview

CISA has disclosed **CVE-2026-93616**, a path traversal vulnerability affecting multiple Check Point management products. The flaw impacts Check Point Security Management Server, Multi-Domain Security Management Server, Log Server, Multi-Domain Log Server, and SmartEvent. The vulnerability allows an **unauthenticated attacker** to upload and execute arbitrary scripts on affected systems, presenting a significant risk to organizations relying on these platforms for security management.

Risk to Saudi Institutions

Path traversal vulnerabilities enable attackers to access files and directories outside the intended scope, and in this case, to execute malicious code without authentication. For regulated institutions in the Kingdom operating Check Point management infrastructure, this represents a critical exposure, particularly for systems accessible from the internet. The vulnerability could allow adversaries to compromise security management platforms that control broader network defenses.

Remediation Guidance

CISA guidance references its BOD 26-04 framework for prioritizing security updates based on risk and forensics triage requirements. Organizations are instructed to apply vendor-supplied mitigations immediately. Where mitigations are unavailable, discontinuation of the affected product is recommended. Federal agencies in the United States face a remediation deadline of 25 September 2026, providing a reference timeline for urgency.

Institutions must assess which Check Point management assets are exposed to the internet and prioritize patching accordingly. Cloud service deployments require particular attention to ensure applicable guidance is followed.

What to do now

1. Identify all Check Point Security Management Server, Multi-Domain Security Management Server, Log Server, Multi-Domain Log Server, and SmartEvent deployments in your environment
2. Assess internet exposure of each affected Check Point management asset and document external accessibility
3. Contact Check Point immediately to obtain vendor-supplied patches or mitigations for CVE-2026-93616
4. Apply vendor mitigations to all affected systems prioritizing internet-facing assets first
5. Review logs for indicators of compromise including unexpected file uploads or script execution on management platforms
6. If vendor mitigations are unavailable, prepare contingency plans to discontinue use of affected products or isolate them from internet access