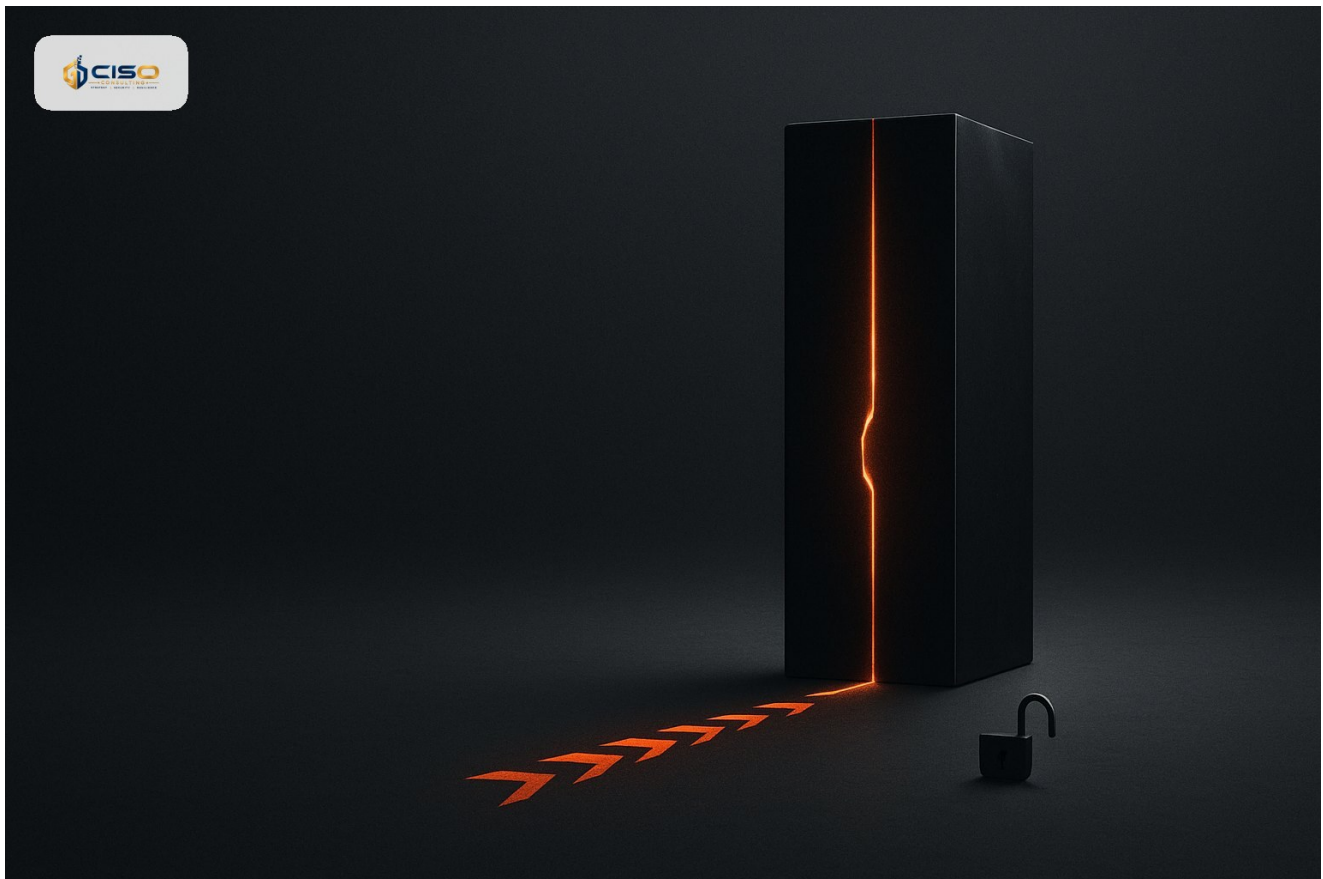


Public exploit released for critical FortiSIEM flaw CVE-2026-106173



A proof-of-concept exploit is now public for CVE-2026-106173 (CVSS 9.4), a patched path traversal flaw in Fortinet FortiSIEM that can let an unauthenticated attacker run unauthorized code or commands.

- Researchers have published a proof-of-concept exploit for a recently patched FortiSIEM flaw.
- The flaw is tracked as CVE-2026-106173 and rated CVSS 9.4 (critical).
- It is a path traversal issue that an unauthenticated attacker could use to execute unauthorized code or commands.
- A public PoC generally makes unpatched systems easier targets.

Researchers have released a proof-of-concept (PoC) exploit for a critical vulnerability in Fortinet FortiSIEM

that the vendor has recently patched. The flaw is tracked as CVE-2026-106173 and carries a CVSS score of 9.4.

What is known

The issue is a path traversal weakness. According to the report, an unauthenticated attacker could use it to execute unauthorized code or commands on an affected system. No credentials are needed, which is why the rating is critical.

The source excerpt does not list affected versions, fixed versions, or any confirmed exploitation in the wild. Those details should be taken from the official Fortinet advisory.

Why it matters

FortiSIEM often sits at the centre of security monitoring, collecting logs from across the estate. A compromise of such a platform can affect visibility and trust in the data it holds. Once a working PoC is public, the time between patch release and attempted abuse tends to shrink, so organisations that have not yet applied the fix should treat it as a priority.

What to do next

Confirm whether FortiSIEM is deployed in your environment, check the version against Fortinet's advisory, and schedule the patch through your emergency change process. Until it is applied, limit network access to the platform's interfaces to trusted management networks only.

What to do now

1. Inventory all FortiSIEM instances, including test and disaster-recovery systems.
2. Compare installed versions with the Fortinet advisory for CVE-2026-106173 and apply the patch through emergency change control.
3. Restrict access to FortiSIEM interfaces to trusted management networks until patched.
4. Review FortiSIEM and network logs for unusual requests or unexpected commands since the patch was released.
5. Record the exposure and remediation in your vulnerability management and risk register for regulator review.