Hive Pro

Threat Level

Red

Hiveforce Labs

THREAT ADVISORY

VULNERABILITY REPORT

Path Traversal in FortiSIEM Gives Attackers a Direct Route to Command Execution

Date of Publication	Admiralty Code	TA Number
October 21, 2026	A1	TA2026307

Summary

First Seen: October 13, 2026
Affected Products: Fortinet FortiSIEM 7.5.0
Impact: Fortinet disclosed CVE-2026-106173 on October 13, 2026, a critical path traversal flaw in FortiSIEM that lets an unauthenticated attacker write files anywhere on the appliance and turn that into code execution. The weakness sits in the phQueryMaster gRPC service, which listens on TCP port 27918 and does not ask connecting clients for a certificate, so anyone who can reach the port can talk to it. A week later, on October 20, 2026, a detailed technical breakdown and a working proof-of-concept exploit were made public, putting reliable attack code within reach of anyone who wants it. Only FortiSIEM 7.5.0 is affected; version 7.6 and FortiSIEM Cloud are not. With a public exploit already in circulation, upgrading to 7.5.1 or later is urgent and should not wait for the next scheduled maintenance window.

CVE

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2026-106173	Fortinet FortiSIEM Path Traversal Vulnerability	Fortinet FortiSIEM	✗	✗	✓

Vulnerability Details

#1

CVE-2026-106173 is a path traversal flaw, tracked as CWE-22, in the FortiSIEM component called phQueryMaster. In simple terms, someone who has never logged in can send the appliance specially crafted packets and get it to run their own commands.

#2

The problem starts with a service that FortiSIEM leaves open. phQueryMaster listens on TCP port 27918 across every network interface, and the setting that would make it ask callers for a certificate is switched off, so anyone who can reach the port is allowed to send it requests. One of those requests is meant to save query results to disk. The service works out where to save the file by taking a name supplied by the caller and sticking it onto a fixed folder path, without ever checking what that name contains. By putting "..[/]" sequences in the name, an attacker can climb out of the results folder and point the write at almost anywhere on the system, and whatever data they send becomes the contents of that file.

#3

That by itself would only get an attacker halfway, because the service adds its own ending to the filename, including a number that only the server sets. The way around it is that the service copies the caller's text using the length the caller claims, which means a null byte can be slipped into the middle of the name. When the finished path is handed to the operating system, the null byte looks like the end of the text, so everything after it is thrown away, including the ending the service added. The file lands on exactly the path the attacker chose. If a file is already sitting there, it is replaced in place and keeps its original owner and permissions, so nothing looks obviously wrong afterwards.

#4

Turning that into code execution is the easy part. FortiSIEM runs several scripts on a timer, and the researchers aimed the attack at a Redis health-check script that a cron job runs every sixty seconds and that the service is allowed to write to. Replace what is inside it, and the attacker's commands run within a minute, with nothing else required. Everyday tools such as curl and standard gRPC libraries refuse to put a null byte in a header, so the request has to be built by hand, but the public proof-of-concept now does that work for anyone who wants it. Fortinet says the flaw is not known to have been exploited in the wild and offers no virtual patch, although the CVSS vector already reflects mature exploit code, which matches the working exploit released on October 20, 2026. Only FortiSIEM 7.5.0 is affected, and the fix is in 7.5.1 and later; FortiSIEM 7.6 is not affected, FortiSIEM Cloud is out of scope, and blocking TCP port 27918 stops the attack where an upgrade has to wait.

Vulnerability

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2026-106173	Fortinet FortiSIEM (7.5.0, before 7.5.1)	cpe:2.3:a:fortinet:fortisiem:*:*:*:*:*:*:*:*	CWE-22

Recommendations

Upgrade FortiSIEM Immediately: Move any FortiSIEM 7.5.0 deployment to version 7.5.1 or above, which contains Fortinet's fix for CVE-2026-106173. Version 7.6 is not affected and FortiSIEM Cloud is out of scope, so the upgrade effort can be focused entirely on 7.5.0 appliances. Given that working exploit code is already public, this should be handled as an emergency change rather than waiting for the next maintenance window.

Restrict Access to TCP Port 27918: Where an immediate upgrade is not possible, apply Fortinet's documented workaround and block or tightly restrict access to TCP port 27918. The gRPC service binds to every interface by default, so this port should never be reachable from untrusted networks or the internet. Limit it to the specific internal hosts that genuinely need to talk to phQueryMaster, and verify the restriction from an external vantage point rather than assuming it holds.

Hunt for Tampered Scripts: FortiSIEM produces no application logs that clearly show this vulnerability being exploited, so detection must rely on the filesystem. Review the creation and modification timestamps of scripts and binaries the platform executes on a schedule, and treat any file whose timestamp doesn't align with the surrounding files as suspicious. The Redis health-check script and the phLicenseTool binary are the two files the researchers called out specifically, but the same logic applies to any recurring executable on the appliance.

Vulnerability Management: Maintain an accurate inventory of security-tooling versions, including the products that monitor the rest of the estate, and subscribe to vendor PSIRT feeds so that advisories such as FG-IR-26-180 are picked up on the day they publish. Build a process that distinguishes flaws with public exploit code from routine patches, since that distinction is what determines how quickly a fix needs to ship. Extend the same review to third-party and appliance-based products, which are frequently excluded from standard patching cycles.

Potential MITRE ATT&CK TTPs

Tactic	Technique	Sub-technique
Initial Access	T1190: Exploit Public-Facing Application	
Execution	T1059: Command and Scripting Interpreter	
Persistence	T1053: Scheduled Task/Job	T1053.003: Cron
Resource Development	T1588: Obtain Capabilities	T1588.006: Vulnerabilities

Patch Link

https://fortiguard.fortinet.com/psirt/FG-IR-26-180

References

https://fortiguard.fortinet.com/psirt/FG-IR-26-180

https://horizon3.ai/attack-research/cve-2026-106173-deep-dive-fortisiem-grpc-path-traversal-file-write-rce/

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a Demo of **HivePro**.

REPORT GENERATED ON

October 21, 2026 • 07:30 AM

© 2026 All Rights are Reserved by Hive Pro

More at www.hivepro.com