Hive Pro

Threat Level

Red

Hiveforce Labs

THREAT ADVISORY

VULNERABILITY REPORT

Fortinet2Shell: Critical FortiClient Flaw Turns a Website Visit into Code Execution

Date of Publication	Admiralty Code	TA Number
November 11, 2026	A1	TA2026333

Summary

First Seen: November 10, 2026
Affected Products: Fortinet FortiClientMac, Fortinet FortiClientWindows, Fortinet FortiClientWindowsPAM
Impact: CVE-2026-121529, dubbed "Fortinet2Shell", is a critical origin validation error in FortiClientMac, FortiClientWindows, and FortiClientWindowsPAM. According to the researcher who discovered it, a CORS misconfiguration lets a malicious website run arbitrary code through a local FortiClient service, so a victim only has to visit the site. Fortinet rates the issue Critical with a CVSSv3 score of 9.1. Successful exploitation can give attackers full control of the endpoint with elevated privileges, exposing credentials and sensitive data. Through the user's trusted VPN or FortiPAM access, attackers can also reach the corporate network and privileged accounts. Fortinet reports no known exploitation and has released fixes. However, the publicly disclosed root cause makes exploit development likely, leaving unpatched organisations at serious risk of data breaches and operational disruption.

CVE

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2026-121529	Fortinet2Shell (Fortinet FortiClient Origin Validation Error Vulnerability)	Fortinet FortiClientMac, FortiClientWindows, FortiClientWindowsPAM	✗	✗	✓

Vulnerability Details

#1

CVE-2026-121529 is an origin validation error in a local API endpoint shipped with FortiClient. The component runs locally on the endpoint and is meant to accept requests only from trusted sources, but it fails to properly verify where incoming requests originate. According to the researcher who discovered it, the root cause is a CORS misconfiguration that permits attacker-controlled web pages to communicate with the local service and reliably execute arbitrary code.

#2

In practice, an attacker hosts or injects malicious content into a web page and lures a FortiClient user to visit it. The victim's browser then issues cross-origin requests to the local FortiClient service, which processes them as trusted and executes the attacker's code or commands. The researcher notes that vulnerable Windows installations may expose a service listening on TCP port 9191 and run the FortiVRS.exe process, and that the issue was found in FortiClient with FortiPAM enabled.

#3

Fortinet rates the vulnerability Critical with a CVSSv3 score of 9.1 and lists its impact as escalation of privilege, while the CNA score shown on NVD and GitHub is 9.6 Critical. The severity reflects how little an attacker needs: a single successful lure can give full control of the endpoint, and that compromise can extend beyond the FortiClient component itself.

#4

Fortinet marks the flaw as not known to be exploited and offers no virtual patch, but its CVSS vector (CVSS:3.1) rates exploit maturity as Proof of Concept. Combined with the researcher's public naming of the issue and disclosure of its root cause, this gives attackers enough direction to build working exploits.

Vulnerability

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2026-121529	Fortinet FortiClientMac (7.4.0 through 7.4.7); Fortinet FortiClientWindows (7.4.0 through 7.4.7, 7.2.0 through 7.2.14); Fortinet FortiClientWindowsPAM (7.4.0 through 7.4.7, 7.2.0 through 7.2.14)	cpe:2.3:a:fortinet:forticlient:*:*:*:*:*:macos:*:*, cpe:2.3:a:fortinet:forticlient:*:*:*:*:*:windows:*:*, cpe:2.3:a:fortinet:forticlient_pam:*:*:*:*:*:windows:*:*	CWE-346

Recommendations

Upgrade FortiClient Immediately: Upgrade FortiClientMac 7.4, FortiClientWindows 7.4, and FortiClientWindowsPAM 7.4 to 7.4.8 or above, and FortiClientWindows 7.2 and FortiClientWindowsPAM 7.2 to 7.2.15 or above, as directed by Fortinet. Push the update through EMS or your software distribution tooling and confirm completion across every endpoint, prioritising privileged-access workstations running FortiPAM.

Identify Exposed Endpoints: Build an inventory of all FortiClient installations and their versions. On Windows hosts, the researcher notes that a service listening on TCP port 9191 and a running FortiVRS.exe process may indicate a vulnerable installation, so use EDR or configuration management queries for these alongside version checks to find systems still at risk.

Hunt for Suspicious Child Processes: Review endpoint telemetry for unusual processes spawned by FortiClient components, such as command shells, scripting engines, or unsigned binaries, especially shortly after browser activity. Treat any such activity on unpatched hosts as a potential compromise and isolate the endpoint for investigation.

Reduce Web-Borne Exposure Until Patched: Where patching is delayed, tighten web filtering to block uncategorised, newly registered, and known-malicious sites, and consider restricting browsing on unpatched privileged-access workstations. Because the attack relies on a victim visiting a malicious page, limiting untrusted browsing directly reduces the opportunity for exploitation.

Enforce Least Privilege on Endpoints: Limit local administrator rights and segment privileged-access workstations from general user networks so that code execution on one endpoint does not easily lead to lateral movement or credential theft across the environment.

Potential MITRE ATT&CK TTPs

Tactic	Technique	Sub-technique
Resource Development	T1608: Stage Capabilities	T1608.004: Drive-by Target
Initial Access	T1189: Drive-by Compromise	
Execution	T1203: Exploitation for Client Execution	
	T1204: User Execution	T1204.001: Malicious Link
Privilege Escalation	T1068: Exploitation for Privilege Escalation	

Patch Link

https://www.fortiguard.com/psirt/FG-IR-26-194

References

https://www.fortiguard.com/psirt/FG-IR-26-194

https://github.com/advisories/GHSA-qgwm-rpp4-xv5g

https://www.linkedin.com/posts/kevin-joensen_cve-2026-121529-or-fortinet2shell-as-we-activity-7526030567436345345-NP-H

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

November 11, 2026 • 05:00 AM

© 2026 All Rights are Reserved by Hive Pro

More at www.hivepro.com