



TLP: CLEAR

CALIFORNIA CYBERSECURITY INTEGRATION CENTER



CYBER ADVISORY UPDATE

Wednesday, September 16, 2026

CAL-CSIC-202609-A-007

Update to New Exploitation of F5 BIG-IP Access Policy Management Environments using Malicious Linux Root Kit

Linux Root Kit

Fileless Web Shell Delivery

Dual Access Channeling

Process-level Compromise

The California Cybersecurity Integration Center (Cal-CSIC) has become aware of new method of exploitation involving F5 BIG-IP Access Policy Management (APM) environments. This activity has been linked to the exploitation of CVE-2025-53521, an unauthenticated remote code execution vulnerability that impacts BIG-IP APM when an access policy is configured on a virtual server.¹ The Cal-CSIC issued an advisory addressing this exploit on October 2025 (Cal-CSIC-202510-A-004) that also references MyF5's quarterly security notification.²

According to Sophos analysis, a Linux rootkit is believed to have given attackers a way to hide shells inside compromised F5 BIG-IP APM environments using Apache and PHP components. The rootkit appears to be specifically tailored to BIG-IP APM webtop environments as opposed to a generic Apache or PHP attack.

The implant hooks Apache's PHP-loading process and modifies the way selected PHP files are presented to the running process. When PHP attempts to memory-map one of these files as part of the routine PHP runtime, the rootkit intercepts the operation and creates a modified in-memory version containing the malicious web shell alongside the legitimate script while the file on disk remains unchanged. Additionally, the root kit establishes a second access mechanism through a local UNIX socket. After authentication, the socket can provide an interactive `"/bin/bash"` session to give an attacker another way into the system while avoiding network-based detection.³

Defenders are recommended to re-investigate systems that were vulnerable before patching and use F5's IOCs along with memory and behavioral telemetry for threat hunting since files scans alone may not detect the compromise.⁴

For additional details regarding the Linux root kit analysis, please use this link:

<https://www.sophos.com/en-us/blog/dissecting-a-php-web-server-rootkit>

WARNING: This document is the property of the California Cybersecurity Integration Center (CAL-CSIC) and follows Traffic Light Protocol (TLP) standards. Except for **TLP: CLEAR**, all TLP designations require recipients to control, store, handle, transmit, and dispose of this product accordingly. Do not release to the public, media, or unauthorized personnel without prior CAL-CSIC approval. This document may contain information exempt from public release under the California Public Records Act (Govt. Code Sec. 7920.000 et seq.). CAL-CSIC does not guarantee the completeness or accuracy of the information.

TLP: CLEAR

Cal-CSIC services are provided at no cost to assist organizations in strengthening their cybersecurity defenses. If you need assistance or wish to verify this communication, please contact us at (833) REPORT-1, or (916) 636-2997. Visit our website for more details: [California Cybersecurity Integration Center | California Governor's Office of Emergency Services](#)

References

-
- ¹ CSO; "Stealth rootkit targeting F5 BIG-IP could expose enterprise identity gateways"; <https://www.csoonline.com/article/4220693/stealth-rootkit-targeting-f5-big-ip-could-expose-enterprise-identity-gateways.html>; accessed 16 September 2026
- ² MyF5; "K000156572: Quarterly Security Notification (October 2025)"; <https://my.f5.com/manage/s/article/K000156572>; accessed 16 September 2026; accessed 16 September 16, 2026
- ³ Sophos; "Dissecting a PHP web server rootkit"; <https://www.sophos.com/en-us/blog/dissecting-a-php-web-server-rootkit>; accessed 16 September 16, 2026
- ⁴ HackRead; "F5 BIG-IP APM Linux Malware Hides PHP Web Shell in Apache Memory"; <https://hackread.com/f5-big-ip-apm-linux-malware-php-web-shell-apache-memory/>; accessed 16 September 16, 2026

WARNING: This document is the property of the California Cybersecurity Integration Center (CAL-CSIC) and follows Traffic Light Protocol (TLP) standards. Except for **TLP: CLEAR**, all TLP designations require recipients to control, store, handle, transmit, and dispose of this product accordingly. Do not release to the public, media, or unauthorized personnel without prior CAL-CSIC approval. This document may contain information exempt from public release under the California Public Records Act (Govt. Code Sec. 7920.000 et seq.). CAL-CSIC does not guarantee the completeness or accuracy of the information.

TLP: CLEAR