CYBER ADVISORY

Thursday, May 07, 2026

CSIC-ADVISORY-202605-A-004

Buffer Overflow Vulnerability Impacting PAN-OS User-ID Authentication Portal (Captive Portal)

Unauthenticated Attacker	Zero-Day	Arbitrary Code Execution	Workaround Available

The California Cybersecurity Integration Center (Cal-CSIC) has become aware of a critical vulnerability that targets the User-ID Authentication Portal service of Palo Alto Networks PAN-OS software. CVE-2026-0300 carries a CVSS 3.1 score of 9.3. The vulnerability allows an unauthenticated attacker to execute arbitrary code with *root* privileges on the PA-Series and VM-Series firewalls by sending specially crafted packets.

Successful exploitation allows for full control over that target network's edge security infrastructure.[1] The attacker does not need credentials to exploit if the portal is accessible, and user interaction is not required. The vendor has observed limited exploitation, and due to the vendor's patching approach, CVE-2026-0300 can be considered a zero-day exploit.

Palo Alto has issued a temporary workaround instruction to address the exploit and plan to develop firmware updates to permanently address the vulnerability. Customers can either Restrict User-ID Authentication Portal access to only trusted zones and if possible – disable the User-ID Authentication Portal entirely until the vendor issues the patches in a staggered rollout between 13-28 May.[2]

The Cal-CSIC recommends following Palo Alto Network's guidance on temporary workarounds. For more technical vulnerability details for CVE-2026-0300, please use this link:

https://security.paloaltonetworks.com/CVE-2026-0300

Affected Product and Version:

Products	Version
PAN-OS 12.1	<12.1.4-h5 <12.1.7
PAN-OS 11.2	< 11.2.4-h17 < 11.2.7-h13 < 11.2.10-h6 < 11.2.12
PAN-OS 11.1	< 11.1.4-h33 < 11.1.6-h32 < 11.1.7-h6 < 11.1.10-h25 < 11.1.13-h5 < 11.1.15
PAN-OS 10.2	< 10.2.7-h34 < 10.2.10-h36 < 10.2.13-h21 < 10.2.16-h7 < 10.2.18-h6

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] Palo Alto Networks; “CVE-2026-0300 PAN-OS: Unauthenticated user-initiated Buffer Overflow Vulnerability in User-ID™ Authentication Portal”; https://security.paloaltonetworks.com/CVE-2026-0300; accessed 06 May 2026
[2] Cyber Press; “Critical Palo Alto Firewall Flaw Exploited to Gain Root Access”; https://cyberpress.org/critical-palo-alto-firewall-flaw-exploited-to-gain-root-access/; accessed 06 May 2026