BLACKSWAN CYBERSECURITY

THREAT ADVISORY

Palo Alto Firewall Zero-Day

May 7, 2026

Background/Summary

On May 6, 2026, Palo Alto Networks disclosed **CVE-2026-0300**, a critical buffer overflow vulnerability in the User-ID Authentication Portal (also known as Captive Portal) service of PAN-OS. The flaw allows unauthenticated remote code execution (RCE) with **root privileges** on affected PA-Series and VM-Series firewalls via specially crafted network packets. Exploitation is limited but confirmed in the wild, primarily targeting instances with the Captive Portal exposed to the public internet or untrusted networks. Prisma Access, Cloud NGFW, and Panorama are **not affected**. Patches are scheduled in phases starting May 13, 2026, with additional fixes by May 28.

Unit 42 is tracking related activity as **CL-STA-1132**, consistent with sophisticated (likely state-sponsored) threat actors. CISA has added the CVE to its Known Exploited Vulnerabilities (KEV) catalog.

Threat

- **Actors**: Sophisticated operators (CL-STA-1132), likely state-sponsored, focused on edge device compromise for network access, espionage, and persistence.
- **Vector**: Unauthenticated buffer overflow (CWE-787) in the Captive Portal service. Exploitation requires the portal to be enabled and exposed.
- **Objective**: Gain root access to firewalls for traffic interception, lateral movement, credential harvesting, and long-term persistence with minimal footprint.

This continues a pattern of nation-state targeting of network edge devices (firewalls, routers, VPNs) for high-privilege footholds.

Risk

- **High** for organizations with internet-exposed Captive Portals on PA/VM-Series firewalls.
- **Medium-High** broadly for PAN-OS users due to the prevalence of these firewalls in enterprise and government environments.
- Successful compromise provides root-level control, enabling traffic manipulation, policy bypass, and pivoting into internal networks.
- Low risk if the portal is restricted to trusted internal IPs or disabled (per Palo Alto best practices).

Impact

- Root-level RCE on compromised firewalls.
- Potential for traffic interception, backdoor installation, credential theft (e.g., service accounts), and AD enumeration.
- Log tampering and anti-forensics to evade detection.
- Broader supply-chain and perimeter defense erosion for affected organizations.

IOCs

Network / C2 Indicators (from Unit 42):

- 67.206.213.86
- 136.0.8.48
- 146.70.100.69 (C2 staging)
- 149.104.66.84

Download / Tooling URLs:
- hxxp://146.70.100.69:8000/php_sess (EarthWorm)
- hxxps://github.com/Acebond/ReverseSocks5/releases/download/v2.2.0/ReverseSocks5-v2.2.0-linux-amd64.tar.gz

File Hashes & Paths:
- SHA256: e11f69b49b6f2e829454371c31ebf86893f82a042dae3f2faf63dcd84f97a584 (EarthWorm)
- /var/tmp/linuxap, /var/tmp/linuxda, /var/tmp/linuxupdate
- /tmp/.c (Python script)
- /tmp/R5, /var/R5 (ReverseSocks5)

Behavioral:
- Attacker User-Agent: Safari/532.31 Mozilla/5.5 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/138.0.0.0 Safari/537.36 Edg/138.0.0.0
- Log deletion: Crash kernel messages, nginx crash entries, core dumps, audit logs (ptrace), SUID binaries.
- AD enumeration targeting domain root and DomainDnsZones using firewall service account credentials.
- Deployment of open-source tunneling tools (EarthWorm, ReverseSocks5).

TTPs

- **Initial Access**: Unauthenticated RCE via crafted packets to exposed Captive Portal (buffer overflow → shellcode injection into nginx worker).
- **Execution & Persistence**: Deploy tunneling tools; use legitimate credentials for AD enumeration.
- **Defense Evasion**: Immediate log cleanup, anti-forensics (delete crash files, ptrace evidence); intermittent/low-volume activity; reliance on open-source/living-off-the-land tools.
- **Discovery & Lateral Movement**: AD enumeration; SOCKS tunneling and port forwarding for pivoting.
- **Command & Control**: Reverse/outbound tunnels (EarthWorm, ReverseSocks5) to attacker infrastructure.

MITRE ATT&CK:
- T1190 (Exploit Public-Facing Application)
- T1068 / T1548 (Privilege Escalation)

- T1070 (Indicator Removal on Host / Log Clearing)
- T1090 / T1572 (Proxy / Protocol Tunneling)
- T1087 (Account Discovery)

Recommendations

1. **Immediate**:
    - Restrict Captive Portal (User-ID Authentication Portal) access to trusted internal IPs only. Disable Response Pages on untrusted interfaces.
    - Disable the portal entirely if not required.
    - Enable Threat ID 510019 (Advanced Threat Prevention, content 9097-10022+; requires PAN-OS 11.1+).
    - Scan for listed IOCs and anomalous tunneling traffic.
2. **Detection & Hunting**:
    - Use Cortex Xpanse or external scanners to identify exposed portals.
    - Monitor for suspicious packets to Captive Portal endpoints, nginx crashes, and unusual root processes.
    - Review firewall logs (where available) for AD queries from the appliance and tunneling tool artifacts.
3. **Patching & Hardening**:
    - Apply patches as released (starting May 13).
    - Follow Palo Alto best practices for management interface and portal security.
    - Minimize internet exposure of all management services.
4. **Longer-Term**:
    - Adopt Zero Trust principles for edge devices.
    - Regular attack surface management and credential hygiene.
    - Engage Unit 42 IR if compromise is suspected.

References: Official advisory, Unit 42 Threat Brief. Monitor Palo Alto and CISA channels for updates. Organizations should treat exposed PAN-OS Captive Portals as high-priority risks until mitigated.

Contact Blackswan Cybersecurity at 855-BLK-SWAN or
Contact@BlackswanCybersecurity.com