**TLP: CLEAR**

*UNIFIED THREAT ADVISORY*

# *Exploited CVE-2026-0300 PAN-OS Unpatched for 7-days*

*2026-05-06T01:35:42.106Z*

RANSOM-ISAC [DEFUSED] detections.ai

---

## *Introduction*

*The Unified Threat Advisory is a coordinated Cyber Intelligence effort co-authored by* **Ransom-ISAC** *an Information Sharing and Analysis Center dedicated to emerging ransomware analysis, collective defense strategies, and global threat intelligence sharing.* **Defused** *a sophisticated cyber deception platform detecting early warning emerging threats such as 0/N-day vulnerabilities, and* **Detections.ai** *a community driven platform for sharing high-fidelity detection rules across integrated environments.*

## *Overview*

*The* **Unified Threat Advisory** *group is dessiminating a vulnerability advisory published by Palo Alto Networks affecting* **PA-Series hardware appliances and VM-Series**. *The flaw results in a* **CWE-787** *Out-of-bounds* **Buffer Overflow** *CAPEC-100 targeting* **USER-ID** *auth portals from a specific endpoint and Inbound port. Versions affected include* **PAN-OS 12.1, PAN-OS 11.2, PAN-OS 11.1, PAN-OS 10.2**. *Limited exploitations have been reported with organizations detected in Education, Healthcare, and Internet Service Provider allowing attackers with* **unauthenticated actors with root access privileges.**

**May 13 Patch (CVSS 9.3)**
*CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:L/SI:L/SA:N/E:A/AU:Y/R:U/V:C/RE:M/U:Red*

**May 28 Patch (8.7)**
*CVSS:4.0/AV:A/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:L/SI:L/SA:N/E:A/AU:Y/R:U/V:C/RE:M/U:Red*

**Note:** *No current patches are available until* **May 13** *and secondary patches until* **May 28**

## *Mitigation & Detection*

*We encourage affected* **PAN-OS** *customers to* **monitor connections to Inbound :6080, 6081,6082** *HTTP POST request for malicious anomaly traffic or* **request with long content-length** *targeting Captive* **USER-ID** *portal via* **/php/uid.php** *exceeding* **>1000 byte headers** *triggering the memory corruption overflow. Isolate inbound network traffic and allow list where possible. Defenders should monitor for suspicious* **outbound connections made from the firewall** *appliance* **initiating reverse shell code** *after executing the classic buffer overflow. This typically floods the content-headers with* **long concatenated strings such as "A" or padded non-binary strings.** *Detecting this exploit it is best to look for network anomalies with oversized payloads designed to exhaust memory buffer forcing the return pointer to a specific memory location by the attacker. PAN-OS customers should update their* **Threat Prevention Signatures.** *We publish* **detection.ai** *rules in our* **ThreatCluster community.**

## *Indicators & C2 domains*

*d349df35218709e8b4763ad72ce431702aca91263ec06f3ed76fd1164b62f689* **research_poc.py**
*shellcode = b"\x90" * 32 + b"\xcc" * 32*
*payload = padding + ret_addr + shellcode*