مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Vulnerability in Palo Alto Networks User-ID Credential Agent

Tracking #:432317696

Date:12-09-2025

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed that Palo Alto Networks disclosed a vulnerability in the User-ID Credential Agent for Windows, which may expose service account passwords in cleartext under certain non-default configurations.

TECHNICAL DETAILS:

A vulnerability in the Palo Alto Networks User-ID Credential Agent on Windows systems can expose service account passwords in cleartext under certain non-default configurations. Local attackers with unprivileged access could exploit this flaw to compromise network security policies, escalate privileges, or disrupt the agent service.

Vulnerability Details

- **CVE-2025-4235**
- CVSS v3.1 Base Score: 4.2 (Medium)
- The User-ID Credential Agent collects and manages service account credentials for integrating Active Directory user mappings into firewall policies. Under specific custom configurations, an unprivileged domain user can retrieve service account passwords in cleartext from agent files or memory.

Impact:

- Minimal privileges: Disrupts credential agent operations, weakening phishing prevention and URL filtering.
- Elevated privileges: Full control over domain controllers, including shutdown, restart, and domain manipulation.
- Network policies may be bypassed or degraded, increasing exposure to lateral movement and reconnaissance.

Affected Versions

- User-ID Credential Agent 11.0.0
  - >= 11.0.2-133 on Windows
  - < 11.0.3 on Windows

Fixed Versions:

- User-ID Credential Agent 11.0 on Windows
  - Upgrade to 11.0.3 or later

RECOMMENDATIONS:

The UAE Cyber Security Council recommends updating the affected versions to the fixed or latest versions released by Palo Alto Networks.

Kindly circulate this information to your subsidiaries and partners as well as share with us any relevant information and findings.

The UAE Cyber Security Council extends its appreciation for the continued collaboration.

REFERENCES:

- https://security.paloaltonetworks.com/CVE-2025-4235