

Alert Bulletin

Bulletin N.:

Publication Date: 22/04/2026

Subject: Alert 2026-41 Multiple vulnerabilities in ManageEngine

Traffic Light Protocol (TLP): Amber

Affected product(s):

- ManageEngine Password Manager Pro: versions 8600 to 13230.
- ManageEngine PAM360: versions prior to build 8531.
- ManageEngine Log360: versions build 13000 to 13013.

Description

Two critical vulnerabilities have been identified, cataloged as CVE-2026-3324 and CVE-2026-5785, which could allow an attacker to compromise affected systems depending on the implementation context.

Below are the vulnerabilities and their details:

- **CVE-2026-3324:** Corresponds to a vulnerability of criticality 8.2, which could allow code execution or manipulation of internal processes by leveraging insufficient validations in exposed components. Successful exploitation could lead to the execution of arbitrary commands or unauthorized access to system resources.
- **CVE-2026-5785:** This is an additional vulnerability with criticality 8 that could be chained with other weaknesses to increase the impact, allowing privilege escalation, access to sensitive information, or alteration of the affected system's behavior.

Both vulnerabilities represent an elevated risk, especially in environments where vulnerable services are exposed to external networks, remote access exists without robust controls, and segmentation or hardening controls have not been applied.

Potential impact includes remote code execution (RCE), privilege escalation, total system compromise, and lateral movement within the network.

Solution and mitigations:

Organizations are recommended to immediately implement the following actions, prioritizing first the Log360, PAM360, and Password Manager Pro instances exposed to the Internet or accessible from less trusted networks:

- Apply without delay the specific security patches and updates for CVE-2026-3324 and CVE-2026-5785, following the official ManageEngine guides for Log360/EventLog Analyzer (<https://www.manageengine.com/products/eventlog/advisory/CVE-2026-3324.html>) and Password Manager Pro/PAM360 (<https://www.manageengine.com/products/passwordmanagerpro/advisory/cve-2026-5785.html>)
- Strictly restrict access to vulnerable services through segmentation and network controls (ACL, VPN, and Zero Trust approaches), limiting administrative access only from controlled networks and jump hosts
- Enable and enforce strong authentication (MFA) for all accounts with access to administration consoles and reporting modules; review and strengthen remote access policies ensuring the use of individual accounts, least privilege principles, and audited sessions
- Intensively monitor application, database, and operating system logs for anomalous activity or signs of exploitation, especially unusual queries or changes to privileged accounts
- Run updated vulnerability scans to identify Log360, PAM360, and Password Manager Pro instances still unpatched, verifying the effective application of the fixed versions (Log360 > 13013, PAM360 ≥ 8531, Password Manager Pro > 13230 according to the manufacturer's guide).

Additional information:

- <https://www.cert.gov.py/vulnerabilidades-en-productos-manageengine/>
- <https://www.cve.org/CVERecord?id=CVE-2026-3324>
- <https://horizon3.ai/attack-research/vulnerabilities/cve-2026-3324/>
- <https://www.rapid7.com/db/vulnerabilities/zoho-manageengine-pam360-cve-2026-5785/>
- <https://asec.ahnlab.com/en/93437/>