NATIONAL CSIRT-CY

High-Severity Vulnerability
ManageEngine Log360

17 April 2026

[Cyber Threat Intelligence]

EXECUTIVE SUMMARY:

The Digital Security Authority (DSA) wants to bring to your attention a high-severity authentication bypass vulnerability in ManageEngine Log360. This flaw may allow unauthorized users to access sensitive data and perform restricted operations through exposed APIs.

TECHNICAL DETAILS:

Vulnerability Details

The vulnerability exists due to improper authorization checks in exposed V1 APIs. An attacker can exploit this flaw to bypass authentication mechanisms, potentially gaining unauthorized access to system data and functionality.

- **CVE ID:** CVE-2026-3324
- **Score:** 8.2
- **Severity:** High
- **CWE-288: Authentication Bypass Using an Alternate Path or Channel**

Affected Products

- **Zohocorp ManageEngine Log360**
- Builds **13000 to 13013**

Fixed Version

- Upgrade to build 13017 or later version using the service pack.

RECOMMENDATIONS:

The Digital Security Authority (DSA) recommends applying the mitigation or workaround provided by ManageEngine.

Please ensure to distribute this information among your subsidiaries and partners and provide us with any pertinent information or findings you may have (such as Indicators of Compromise, Tactics, Techniques, and Procedures, etc.).

The Digital Security Authority (DSA) extends its appreciation for the continued collaboration.

REFERENCES:

1. https://nvd.nist.gov/vuln/detail/CVE-2026-3324 · Security Note
2. https://twitter.com/CVEnew/status/2045102673997787333 · Twitter Post
3. https://manageengine.com/log-management/advisory/CVE-2026-3324.html · Note
4. https://twitter.com/infoflowcloud/status/2045105091913412629 · Twitter Post

DISCLAIMER:

The information presented in this report is based on available data up to the 18th of April 2024.

Organizations are advised to consult with relevant cybersecurity professionals and follow best practices for their specific environments.