NATIONAL CSIRT-CY

Critical Path Traversal Vulnerability in **CrowdStrike LogScale**

22 April 2026

[Cyber Threat Intelligence]

EXECUTIVE SUMMARY:

The Digital Security Authority (DSA) wants to bring to your attention a critical vulnerability (CVE-2026-40050) has been identified in CrowdStrike LogScale affecting specific self-hosted versions.

TECHNICAL DETAILS:

A critical vulnerability (CVE-2026-40050) has been identified in CrowdStrike LogScale affecting specific self-hosted versions. This flaw allows unauthenticated remote attackers to perform path traversal attacks, potentially exposing sensitive files on the underlying server.

The vulnerability carries a CVSS v3.1 score of 9.8 (Critical), indicating severe risk if left unpatched. While LogScale SaaS and Next-Gen SIEM customers are not affected, self-hosted deployments must take immediate remediation action.

Vulnerability Details

- CVE ID: CVE-2026-40050
- Type: Unauthenticated Path Traversal
- Severity: **Critical (CVSS 9.8)**
- Affected Product: CrowdStrike LogScale (**Self-Hosted only**)

Affected Products

- LogScale Self-Hosted (GA): Versions 1.224.0 → 1.234.0 (inclusive)
- LogScale Self-Hosted (LTS): Versions 1.228.0, 1.228.1

Fixed Version

- 1.235.1 or later
- 1.234.1 or later
- 1.233.1 or later
- 1.228.2 (LTS) or later

Weakness Enumerations

- CWE-22 Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')
- CWE-306 Missing Authentication for Critical Function

RECOMMENDATIONS:

Upgrade Immediately: Upgrade LogScale to a patched version.

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.

[Cyber Threat Intelligence]

REFERENCES:

1. https://www.crowdstrike.com/en-us/security-advisories/cve-2026-40050/
2. https://nvd.nist.gov/vuln/detail/CVE-2026-40050

DISCLAIMER:

The information presented in this report is based on available data up to the 22nd of April 2026.

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