مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

# Critical Path Traversal Vulnerability in CrowdStrike LogScale

Tracking #:432318826

Date:22-04-2026



TLP: WHITE

## EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed 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 Versions:**

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

**Fixed Versions:**

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

## RECOMMENDATIONS:

**Upgrade Immediately:** Upgrade LogScale to a patched version

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://www.crowdstrike.com/en-us/security-advisories/cve-2026-40050/