Critical CrowdStrike LogScale Vulnerability Lets Attackers Read Server Files Without Login

TLDR;

There is a vulnerability in CrowdStrike LogScale (CVE-2026-40050, CVSS 9.8) that allows a remote, unauthenticated attacker to access sensitive files from the server by abusing a path traversal flaw in a cluster API endpoint.

This issue impacts self-hosted deployments only. SaaS environments are already protected, and there is no confirmed exploitation at this time.

Overview

There is a vulnerability in CrowdStrike LogScale (CVE-2026-40050, CVSS 9.8) that allows a remote attacker to access sensitive files on the server without authentication. The issue is in a cluster API endpoint that does not properly validate user input, allowing directory traversal outside of intended paths.

Affected Products

- LogScale Self-Hosted (GA) – versions 1.224.0 through 1.234.0
- LogScale Self-Hosted (LTS) – versions 1.228.0 through 1.228.1

Because authentication is not required, an attacker can directly query the exposed endpoint and steal files from the underlying system. This vulnerability lets an attacker manipulate file paths to access data outside of the intended directory. Because no authentication is required, they can do this without logging in.

If exploited, this could expose configuration files, credentials, log data, or other sensitive information stored on the host. In some environments, that data could be used to pivot further into the network.

CVE-2026-40050 only affects self-hosted LogScale deployments. CrowdStrike-managed SaaS environments have been mitigated at the network level, and there is no current evidence of active exploitation. Because the vulnerability requires no authentication and is easy to exploit, Aspire recommends patching immediately.

Aspire Protects

- **Patch** – Upgrade immediately to a patched version. Please see CrowdStrike's advisory for more details.
- Restrict external access to LogScale cluster API endpoints.
- Review logs for unusual file access activity or API abuse.
- Treat exposed systems as potentially compromised if they were internet-facing.
- Rotate credentials stored or processed on affected systems.

TTPs to Watch

Initial Access

- Exploit Public-Facing Application [T1190] – The attacker may exploit the exposed LogScale API endpoint to access the system without authentication.

Discovery

- File and Directory Discovery [T1083] – The attacker may enumerate directories and files through the path traversal vulnerability to locate sensitive data.

IoCs

There are no known IoCs at this time. Aspire is actively monitoring and will notify customers if any are found. For more details on how we can help protect your organization, contact Aspire's Customer Success Management team.

Targeted Industries

Organizations using self-hosted log management platforms, particularly CrowdStrike LogScale, may be affected if instances are exposed to the internet.

- Education
- Energy
- Finance
- Healthcare
- Legal
- Manufacturing
- Government
- Retail

Aspire Service Offerings

- **Aspire Managed XDR (MXDR)**
  - Aspire Managed XDR (MXDR) combines next-generation eXtended Detection and Response (XDR) technology, a 24x7 security operations center (SOC), and the expertise of a US-based team of security professionals to identify and respond to threats across a broader attack surface.
  - Building on the existing capabilities of Managed Detection and Response (MDR), Aspire Managed XDR integrates and correlates telemetry from endpoints, network, cloud, email, identity, and more. This advanced platform creates valuable context enabling end-to-end visibility across all threat vectors.
  - Experienced security analysts and incident responders deliver 24x7 threat detection, analysis, and investigations – with both automated and human-led response actions to quickly mitigate cyber attacks.
- **Aspire Incident Response**
  - The ability to respond effectively to data breaches is critical to every organization. When attacks occur, IT leaders need a process that will ultimately maintain business continuity, protect the company reputation, and avoid fines, legal fees, and remediation costs.
  - Aspire offers incident response services to help you prepare for, manage, and recover from data breaches and network attacks. An experienced team uses industry-leading threat intelligence and the most current security technology to quickly respond to attacks, reduce damage, and minimize exposure.

Supporting Documentation

CVE-2026-40050 — CrowdStrike LogScale Unauthenticated Path Traversal

CWE - CWE-22: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') (4.19.1)

CWE - CWE-306: Missing Authentication for Critical Function (4.19.1)