Logstash 8.19.14, 9.2.8, 9.3.3 Security Update (ESA-2026-29)

ismisepaul (Paul) 1 April 8, 2026, 4:32pm

Improper Limitation of a Pathname to a Restricted Directory in Logstash Leading to Arbitrary File Write

Improper Limitation of a Pathname to a Restricted Directory (CWE-22) in Logstash can lead to arbitrary file write and potentially remote code execution via Relative Path Traversal (CAPEC-139). The archive extraction utilities used by Logstash do not properly validate file paths within compressed archives. An attacker who can serve a specially crafted archive to Logstash through a compromised or attacker-controlled update endpoint can write arbitrary files to the host filesystem with the privileges of the Logstash process. In certain configurations where automatic pipeline reloading is enabled, this can be escalated to remote code execution.

Affected Versions:

- 8.x: All versions from 8.0.0 up to and including 8.19.13
- 9.x:
  - All versions from 9.0.0 up to and including 9.2.7
  - All versions from 9.3.0 up to and including 9.3.2

Affected Configurations:

Deployments with the GeoIP database downloader enabled and configured to use an external update endpoint are affected. The risk is elevated in configurations where automatic pipeline configuration reloading is enabled and the pipeline configuration directory is writable by the Logstash process.

Solutions and Mitigations:

The issue is resolved in versions 8.19.14, 9.2.8, and 9.3.3.

For Users that Cannot Upgrade:

- Disable the GeoIP database downloader by setting `xpack.geoip.downloader.enabled: false` in the Logstash configuration.
- Ensure the GeoIP downloader endpoint uses HTTPS and points to a trusted source.
- Disable automatic pipeline configuration reloading to prevent code execution via written files.
- Restrict filesystem write permissions for the Logstash process to only necessary directories.

Indicators of Compromise (IOC)

Check for unexpected files written outside the GeoIP database directory. Review the filesystem for files that should not exist in pipeline configuration directories or other sensitive locations.

- Monitor Logstash logs for GeoIP database download activity, particularly downloads from unexpected endpoints.
- Check for unexplained pipeline configuration files or changes to existing pipeline configurations.
- Review file integrity monitoring alerts for writes to directories outside the expected GeoIP data path.

Severity: CVSSv3.1: High (8.1) - CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H
CVE ID: CVE-2026-33466
Problem Type: CWE-22 - Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')
Impact: CAPEC-139 - Relative Path Traversal

Related topics

Topic	Replies	Activity
Logstash File Output Vulnerability CVE-2015-4152	1	July 6, 2017
Logstash 8.11.1 Security Update (ESA-2023-26)	0	November 15, 2023
Logstash 8.19.10, 9.1.10, 9.2.4 Security Update (ESA-2026-06)	0	March 19, 2026
Change the logfilepath for internal logstash files	1	December 12, 2019
Logstash 7x not reading from log file, same working for 6x versions	3	October 25, 2019