INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-04-14 06:04 UTC

Pillow FITS GZIP Decompression Bomb Vulnerability (CVE-2026-40192)

CVE VULNERABILITY | MEDIUM | CVSS 5.5

SCC Item ID	SCC-CVE-2026-0039
Type	CVE Vulnerability
CVE ID	CVE-2026-40192
Severity	MEDIUM
CVSS Base Score	5.5
Affected Products	pillow (PyPI), specific affected versions not confirmed from available source data
Published	2026-04-13T19:22:35Z
Discovery Source	Osv

Executive Summary

A denial-of-service vulnerability (CVE-2026-40192) has been identified in Pillow, a widely used Python imaging library, affecting its processing of FITS files compressed with GZIP. An attacker who can supply a maliciously crafted image file to an application using Pillow can trigger excessive memory or CPU consumption, crashing or degrading the affected service. Organizations running Python-based applications that process user-supplied image files, including AI/ML pipelines that commonly depend on Pillow, carry the highest operational risk.

Technical Analysis

CVE-2026-40192 is a decompression bomb vulnerability (CWE-400: Uncontrolled Resource Consumption; CWE-409: Improper Handling of Highly Compressed Data) in the Pillow Python imaging library (PyPI). The flaw resides in Pillow's handling of FITS (Flexible Image Transport System) files that use GZIP compression. A specially crafted FITS file with an extreme compression ratio can cause the library to expand the payload into memory, exhausting RAM or CPU until the process is killed or the host becomes unresponsive. This maps to MITRE ATT&CK T1499.004 (Endpoint Denial of Service: Application or System Exploitation). CVSS base score is 5.5 (Medium). EPSS score and percentile are not yet populated, indicating limited observed exploitation activity at time of publication. Affected versions are documented in GHSA-whj4-6x5x-4v2j and NVD entry CVE-2026-40192. The vulnerability is not listed in CISA KEV. Patch status should be verified against the upstream advisory, as fix availability was not confirmed in source data at configuration time.

Action Checklist

1. Step 1: Containment. Identify all Python environments and applications in your organization that import Pillow (search requirements.txt, pyproject.toml, Pipfile, and installed packages via 'pip list' or 'pip show pillow'). Prioritize services that accept user-uploaded or externally sourced image files. Temporarily restrict FITS file upload capability in affected services until patched.
2. Step 2: Detection. Query your software asset inventory and CI/CD dependency manifests for Pillow installations. Check SBOM records if available. Review application logs for memory or CPU spike events tied to image processing jobs, particularly any involving FITS file handling. Monitor host-level metrics (RAM exhaustion, OOM-killer events, process crashes) on systems running Pillow-dependent workloads.
3. Step 3: Eradication. Upgrade Pillow to the patched version. Consult GHSA-whj4-6x5x-4v2j for the specific version number and PyPI release notes for installation guidance. Update all virtual environments, container images, and deployment pipelines. Note: Patch version was not confirmed from available sources at time of publication - verify against upstream advisory before deployment.
4. Step 4: Recovery. After patching, validate that Pillow's installed version matches the patched release across all environments ('pip show pillow'). Re-enable FITS file processing only after version verification. Monitor application memory and CPU utilization for 24-48 hours post-patch to confirm stability. Rebuild affected container images from updated base dependencies.
5. Step 5: Post-Incident. Review whether your dependency management process surfaces decompression-class vulnerabilities proactively. Implement file-type validation and size limits on image uploads at the application layer to reduce exposure to future decompression attacks. Evaluate adding Pillow to your software composition analysis (SCA) tooling watchlist.

Detection Guidance

Search all Python dependency manifests (requirements.txt, pyproject.toml, Pipfile.lock, setup.cfg) and runtime environments for any version of Pillow (package name: Pillow or PIL on PyPI). Use 'pip list | grep -i pillow' or query your SCA/SBOM tooling. For runtime detection, monitor for sudden memory growth or OOM-killer events in services that process images, particularly any that accept FITS file input. Application logs showing repeated process restarts or memory-limit errors in image-processing workers are a behavioral indicator. There are no network-layer IOCs; this is a file-content attack relying on dependency inventory, runtime monitoring, and log analysis for detection.

Framework Mappings

MITRE-ATTACK

- **T1499.004** — Application or System Exploitation

NIST-800-53R5

- **SC-5** — Denial-of-Service Protection

CIS-V8

- **13.8** — Deploy a Network Intrusion Prevention Solution

ISO-27001-2022

- **A.8.8** — Management of technical vulnerabilities

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1499.004	Application or System Exploitation	Impact

Sources

Source	URL	Tier
osv	https://osv.dev/vulnerability/GHSA-whj4-6x5x-4v2j	T3
FITS GZIP decompression bomb in Pillow · CVE-2026-40192 - GitHub	https://github.com/advisories/GHSA-whj4-6x5x-4v2j	T3
Ubuntu Pro FIPS-updates 24.04 LTS : Linux kernel (Azure ... - Tenable	https://www.tenable.com/plugins/nessus/306094	T3
Amazon Linux Security Center - CVE List	https://explore.alas.aws.amazon.com/	T3
Ubuntu Linux Kernel Multiple Vulnerabilities - HKCert	https://www.hkcert.org/security-bulletin/ubuntu-linux-kernel-multip...	T3
NVD	https://nvd.nist.gov/vuln/detail/CVE-2026-40192	T1

Generated 2026-04-14 06:04 UTC by TJS Security Command Center