CVE-2025-8194

Descriere	**CVE-2025-8194** este o vulnerabilitate de severitate înaltă (CVSS 7.5) în modulul ***tarfile*** din *CPython*. Ea permite atacatorilor să creeze arhive TAR malitioase cu offset-uri negative în anteturile de fișiere. Când acestea sunt procesate de către API-urile ***TarFile.extract()*** sau ***TarFile.iter(),*** se declanșează o buclă infinită, blocând aplicația și provocând un atac de tip Denial-of-Service (DoS).
Scor	7.5 **(HIGH)**
CVSS	3.1
CWE - ID	**CWE - 835** Loop with Unreachable Exit Condition ('Infinite Loop')
Versiuni vulnerabile	CPython: Toate versiunile anterioare 3.14.0. Sisteme dependente: Orice aplicație Python ce utilizează ***tarfile.extract(), tarfile.open()*** sau ***tarfile.iter().***
Impacturi principale	• Consumul resurselor: CPU și memorie sunt epuizate până la blocarea procesului. • Disponibilitate redusă: Aplicațiile care procesează arhive TAR din surse nevalidate (de ex., sisteme de upload, instrumente CI/CD) devin inoperabile. • Fără compromitere a confidențialității sau integrității: Vulnerabilitatea afectează doar disponibilitatea.

Cauza principală	Modulul ***tarfile*** nu validează câmpul ***offset*** din anteturile TAR. Atacatorii pot seta acest câmp la valori negative (de ex., ***-1***), determinând funcția ***TarInfo._block()*** să intre într-o buclă fără condiție de ieșire:
	„# Codul vulnerabil (simplificat)
	def _block(self, count):
	while count > 0:
	# Procesează blocuri de date...
	count -= 1 # Dacă count este negativ, incrementarea devine infinită ”
	Un fișier TAR malitios conține o intrare cu ***offset = -1***, transformând bucla într-un ciclu nesfârșit.

Vectorul de atac	• Cerințe: Aplicația trebuie să deschidă sau să enumere fișierele dintr-un arhivă TAR primită de la surse neautentificate (de ex., upload de utilizatori, cereri HTTP). • Complexitate: Scăzută. Exploatarea necesită doar crearea unui TAR cu antet corupt.
Recomandări de Securitate	• Validarea arhivelor: Verificați fișierele TAR primite de la surse necunoscute cu instrumente precum ***tar -tf <file>*** înainte de procesare. • Limitarea resurselor: Rulați extracția TAR în containere cu limite stricte de CPU/memorie (de ex., prin cgroups sau Docker). • Timeouts: Adăugați timeout-uri pentru operațiunile cu arhive: „import signal

	def handler(signum, frame):
	raise TimeoutError("Procesarea TAR a depășit timpul alocat")
	signal.signal(signal.SIGALRM, handler)
	signal.alarm(30) # 30 de secunde
	try:
	with tarfile.open("file.tar") as tar:
	tar.extractall()
	finally:
	signal.alarm(0) ”
	• Monitorizare: Utilizați tool-uri precum ***Sentry*** sau ***New Relic*** pentru a detecta blocări în procese.

Soluții	• Actualizare CPython: Upgrade la versiunea 3.14.0 sau ulterioară.
	• Patch aplicabil:
	„import tarfile
	def _block_patched(self, count):
	if count < 0:
	raise tarfile.InvalidHeaderError("offset invalid")
	return _block_patched._orig_block(self, count)
	# Aplică patch-ul la runtime
	_block_patched._orig_block = tarfile.TarInfo._block
	tarfile.TarInfo._block = _block_patched ”
	Acest patch introduce o validare a offset-urilor negative.

Referință	https://feedly.com/cve/CVE-2025-8194 https://github.com/python/cpython/pull/137027 https://nvd.nist.gov/vuln/detail/CVE-2025-8194 https://securityonline.info/python-tarfile-vulnerability-cve-2025-8194-allows-dos-via-malicious-archives/ https://cvetodo.com/cve/CVE-2025-8194