

NEW CRITICAL VULNERABILITY ADVISORY: CVE-2026-68770

Summary

CVE-2026-68770 is a newly disclosed Critical vulnerability. It is not yet on CISA's actively-exploited list; treat it as proactive patching before it is weaponised. sentence-transformers contains a security control bypass vulnerability that allows attackers to achieve arbitrary code execution by exploiting a logic flaw in the `import_module_class` helper within `sentence_transformers/util/misc.py`, where the guard condition includes an `'or os.path.exists(model_name_or_path)'` clause that satisfies the trust gate whenever the supplied path exists on the local filesystem, regardless of the `trust_remote_code=False` argument. Attackers who can control or influence the contents of a model directory on disk can place malicious Python files such as `modeling_*.py` referenced via `modules.json`, causing the code to execute at import time when an application loads the model with `SentenceTransformer(path, trust_remote_code=False)`, bypassing the documented security contract and achieving code execution within the loading process.

What we know

- **CVE:** CVE-2026-68770
- **Status:** Newly disclosed, not yet known-exploited (not on CISA KEV)
- **Severity:** CVSS 9.8 Critical, Network-exploitable, no privileges required, no user interaction (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)
- **Exploitation likelihood (EPSS):** 1%

Recommended action

Patch as a fix becomes available, prioritised by the exposure and EPSS above. Until then, restrict network access to the affected service now (segment it, put it behind a VPN, or take it offline) until you can patch. This does not yet trigger CRA 24-hour reporting, which requires active exploitation, but patching ahead of exploitation is the whole point.

Sources: NIST NVD. Public data; an advisory of a newly disclosed vulnerability, not an incident report. Verify applicability to your estate before acting.