nesquena / **hermes-webui** Public

Code | Issues 82 | Pull requests 4 | Actions | Projects | Security and quali

Commit 3cc5839

3 people authored last week · 1 / 4 · Verified

```
[security] fix(sessions): validate session_id before deleting session files
(#412)

* fix(sessions): validate session_id before deleting files

* fix: remove premature session index invalidation before validation check

* docs: v0.50.32 release — version badge and CHANGELOG

---------

Co-authored-by: hinotoi-agent <paperlantern.agent@gmail.com>
Co-authored-by: Nathan Esquenazi <nesquena@gmail.com>
```

master (#412) · v0.50.133 ••• v0.50.32

1 parent 539501e commit 3cc5839

4 files changed +35 -2 lines changed ↑ Top

Filter files…

- CHANGELOG.md
- api
  - routes.py
- static
  - index.html
- tests
  - test_sprint3.py

4 files changed +35 -2 lines changed Search within code

CHANGELOG.md

```
@@ -1,5 +1,14 @@
# Hermes Web UI -- Changelog

+ ## [v0.50.32] fix(sessions): validate session_id before deleting session files [SECURITY] (#409)
+
+ `/api/session/delete` accepted arbitrary `session_id` values from the request body and built the delete path directly as `SESSION_DIR / f"{sid}.json"`. Because pathlib discards the prefix when `sid` is an absolute path, an attacker could supply `/tmp/victim` and cause the server to unlink `victim.json` outside the session store. Traversal-style values (`../../etc/target`) were also accepted. CVSS 8.1 High (AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:H/A:H).
+
+ - `api/routes.py`: validate `session_id` against `[0-9a-z_]+` allowlist (covers `uuid4().hex[:12]` WebUI IDs and `YYYYMMDD_HHMMSS_hex` CLI IDs) before path construction; resolve candidate path and enforce `path.relative_to(SESSION_DIR)` containment before unlinking; only invalidate session index on successful deletion path, not on rejected requests
+ - `tests/test_sprint3.py`: 2 new regression tests — absolute-path payload rejected and file preserved, traversal payload rejected and file preserved
+ - Original PR by @Hinotoi-agent (cherry-picked; branch was 4 commits behind master)
+ - 1041 tests total (up from 1039)
+
## [v0.50.31] fix: delegate all live model fetching to agent's provider_model_ids()

`_handle_live_models()` in `api/routes.py` previously maintained its own per-provider fetch logic and returned `not_supported` for Anthropic, Google, and Gemini. Now it delegates entirely to the agent's `hermes_cli.models.provider_model_ids()` — the single authoritative resolver — and `_fetchLiveModels()` in `ui.js` no longer skips any provider.
```

api/routes.py

```
@@ -724,10 +724,16 @@ def handle_post(handler, parsed) -> bool:
            sid = body.get("session_id", "")
            if not sid:
```

```
726  726              return bad(handler, "session_id is required")
     727  +         if not all(c in '0123456789abcdefghijklmnopqrstuvwxyz_' for c in sid):
     728  +             return bad(handler, "Invalid session_id", 400)
727  729          # Delete from WebUI session store
728  730          with LOCK:
729  731              SESSIONS.pop(sid, None)
730       -         p = SESSION_DIR / f"{sid}.json"
     732  +         try:
     733  +             p = (SESSION_DIR / f"{sid}.json").resolve()
     734  +             p.relative_to(SESSION_DIR.resolve())
     735  +         except Exception:
     736  +             return bad(handler, "Invalid session_id", 400)
731  737          try:
732  738              p.unlink(missing_ok=True)
733  739          except Exception:
```

static/index.html

```
@@ -535,7 +535,7 @@ <h3 style="margin:0;font-size:18px">Control Center</h3>
535  535                  <div class="settings-section-title">System</div>
536  536                  <div class="settings-section-meta">Instance version and access controls.</div>
537  537                </div>
538       -              <span class="settings-version-badge">v0.50.31</span>
     538  +              <span class="settings-version-badge">v0.50.32</span>
539  539              </div>
540  540              <div class="settings-field" style="border-top:1px solid var(--border);padding-top:12px;margin-top:8px">
541  541                <label for="settingsPassword" data-i18n="settings_label_password">Access Password</label>
```

tests/test_sprint3.py

```
@@ -114,6 +114,24 @@ def test_session_delete_requires_session_id():
114  114      result, status = post("/api/session/delete", {})
115  115      assert status == 400
116  116
     117  +
     118  + def test_session_delete_rejects_absolute_path_payload(tmp_path):
```

```
119 +     victim = tmp_path / "victim.json"
120 +     victim.write_text("TOPSECRET", encoding="utf-8")
121 +     result, status = post("/api/session/delete", {"session_id":
      str(victim.with_suffix(""))})
122 +     assert status == 400
123 +     assert victim.exists(), "absolute-path payload must not delete arbitrary
      files"
124 +
125 +
126 + def test_session_delete_rejects_traversal_payload(tmp_path):
127 +     victim = tmp_path / "outside.json"
128 +     victim.write_text("TOPSECRET", encoding="utf-8")
129 +     traversal = f"../../../../{victim.with_suffix('').as_posix().lstrip('/')}"
130 +     result, status = post("/api/session/delete", {"session_id": traversal})
131 +     assert status == 400
132 +     assert victim.exists(), "traversal payload must not delete arbitrary files"
133 +
134 +
117 135   def test_chat_start_requires_session_id():
118 136       result, status = post("/api/chat/start", {"message": "hello"})
119 137       assert status == 400
```

Comments 0

Please sign in to comment.