NEW CRITICAL VULNERABILITY ADVISORY: CVE-2026-3141

Summary

CVE-2026-3141 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. The FormGent plugin for WordPress is vulnerable to unauthorized arbitrary file deletion due to a missing capability check on the /wp-json/formgent/responses/attachments REST API endpoint in all versions up to, and including, 1.9.2 This is due to the REST API route being registered without any authentication middleware in routes/rest/api.php. This makes it possible for unauthenticated attackers to delete arbitrary files within the formgent uploads directory. Additionally, on Linux servers where the wp-content/uploads/formgent directory does not yet exist (the default state after plugin installation), the path traversal protection can be bypassed, enabling deletion of arbitrary files including wp-config.php which can lead to complete site takeover via a fresh WordPress installation.

What we know

- **CVE:** CVE-2026-3141
- **Status:** Newly disclosed, not yet known-exploited (not on CISA KEV)
- **Severity:** CVSS 9.1 Critical, Network-exploitable, no privileges required, no user interaction (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:H)
- **Exploitation likelihood (EPSS):** 0%

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.