



Philippines: nuclear records taken through a flaw fixed three years ago

Researchers found an attacker's own server open on the internet and read what was on it: the tools and the loot from intrusions at a Philippine nuclear research body and a marine engineering firm serving the Navy.

INCIDENT DETAILS • 5WH

Who Assessed by Hunt.io as a Chinese speaker, from simplified Chinese in code and folder names. No group is named and no government has attributed it.

What An inventory records about 9 GB taken from the nuclear agency; researchers recovered 372 MB, so material was removed before discovery.

Where The Philippines; the staging server was in Amsterdam, holding 1,310 files.

When Open directory found 13 Aug 2026; published 25 Aug after victims were notified.

Why Collection. Fuel inventories and core components map a national programme; the supplier sits against the South China Sea dispute.

How Two known unpatched internet-facing flaws: an ownCloud authentication bypass from 2023, and a WordPress plugin flaw.

IMPACT

- Safeguards: reactor components, nuclear material accounting and fuel inventories describe a national programme, and cannot be recalled.
- Personnel: passports, travel records and a badge database covering an entire workforce, supporting impersonation and physical reconnaissance.
- Credentials: a password manager database, encrypted files and disk recovery keys were taken, extending the compromise beyond what left.
- Hygiene: both entry points were published flaws, one three years old and exploitable only because of a default setting.

SEQUENCE OF EVENTS

2023 The ownCloud flaw, patched since

2024 The WordPress plugin flaw

27 Aug 2026 Added to the US known-exploited catalogue

- 1 An attacker leaves their own server open
- 2 In through a 2023 flaw, no password needed
- 3 Reactor, fuel and safety records taken and sorted
- 4 A second victim through a WordPress flaw
- 5 A 192 MB badge and attendance database
- 6 Disclosure, then a belated patch deadline

ASSESSMENT, LESSONS, AND RECOMMENDATIONS

- A default configuration is what exposed a national nuclear programme.
- The personnel data is the part with a long tail - documents age, people do not.
- The attribution is careful and should be carried as carefully; language shows who wrote it, not who paid.
- The 9 GB figure describes what was taken, not what was found.