

# CVE-2026-98411

## Microsoft power: sequencing: fix NULL-pointer dereference in pwrseq\_device\_register()

In the Linux kernel, the following vulnerability has been resolved: power: sequencing: fix NULL-pointer dereference in pwrseq\_device\_register() If dev\_set\_name() fails in pwrseq\_device\_register(), we jump to the err\_put\_pwrseq label before initializing pwrseq->targets. pwrseq\_release() will try to iterate over targets unconditionally and subsequently dereference an invalid pointer. Move the call to dev\_set\_name() after the list head is initialized.

|                                                               |                                       |                                                          |                                                      |
|---------------------------------------------------------------|---------------------------------------|----------------------------------------------------------|------------------------------------------------------|
| <b>EVRS</b><br><b>0</b> /100<br><b>Informational</b> priority | <b>CVSS</b><br><b>—</b><br>Not scored | <b>EPSS</b><br><b>0.002</b><br>10.5th percentile · FIRST | <b>CISA DEADLINE</b><br><b>—</b><br>No CISA deadline |
|---------------------------------------------------------------|---------------------------------------|----------------------------------------------------------|------------------------------------------------------|

### Signals behind the score

☒ counted in the score ☐ not counted

evidence for 2 of 8 signals

|                                            |                                    |                                                                |                                                                                                    |
|--------------------------------------------|------------------------------------|----------------------------------------------------------------|----------------------------------------------------------------------------------------------------|
| <input type="checkbox"/> <b>CISA KEV</b>   | Not currently CISA KEV-listed      | <input type="checkbox"/> <b>Vendor exploitation</b>            | Active-exploitation status not yet checked - scored at the population base rate (none) until known |
| <input type="checkbox"/> <b>Ransomware</b> | Ransomware association unavailable | <input type="checkbox"/> <b>KEV recency</b>                    | CISA KEV listing date unavailable                                                                  |
| <input type="checkbox"/> <b>EPSS</b>       | 0.002 probability                  | <input type="checkbox"/> <b>Pre-patch disclosure</b>           | Disclosure status unavailable                                                                      |
| <input type="checkbox"/> <b>CVSS</b>       | CVSS base score unavailable        | <input type="checkbox"/> <b>Microsoft Exploitability Index</b> | Not a Microsoft CVE                                                                                |

### Remediation

**Monitor** Untagged reference available; patch status is not confirmed

NVD lists one or more references for this CVE that aren't tagged as a patch or vendor advisory. Review them directly to confirm patch availability and applicability before making a remediation decision.

Basis: NVD reference (untagged)

### Affected and fixed versions

| PACKAGE                                 | AFFECTED | FIXED IN                | SOURCE |
|-----------------------------------------|----------|-------------------------|--------|
| Not identified by the connected sources | —        | no fixed version listed | NVD    |

### Sources

|                             |                                                                                                                                                         |                             |                                                                                                                                                         |
|-----------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Reference</b>            | <a href="https://git.kernel.org/stable/c/242da4318d97380741516b595af3920207b2f0f1">git.kernel.org/stable/c/242da4318d97380741516b595af3920207b2f0f1</a> | <b>Additional reference</b> | <a href="https://git.kernel.org/stable/c/a2890c1eb96d1dd0bec1cce5fbc4ed5af1dfd55d">git.kernel.org/stable/c/a2890c1eb96d1dd0bec1cce5fbc4ed5af1dfd55d</a> |
| <b>Additional reference</b> | <a href="https://git.kernel.org/stable/c/a2fb51ec8920279e9e908010f37b448775f42eff">git.kernel.org/stable/c/a2fb51ec8920279e9e908010f37b448775f42eff</a> | <b>Additional reference</b> | <a href="https://git.kernel.org/stable/c/efe21a5c5bfe23bd30a8e4ba4e2b04ae265348bb">git.kernel.org/stable/c/efe21a5c5bfe23bd30a8e4ba4e2b04ae265348bb</a> |
| <b>NVD</b>                  | <a href="https://nvd.nist.gov/vuln/detail/CVE-2026-98411">nvd.nist.gov/vuln/detail/CVE-2026-98411</a>                                                   | <b>ENISA EUVD</b>           | <a href="https://euvd.enisa.europa.eu/vulnerability/EUVD-2026-101060">euvd.enisa.europa.eu/vulnerability/EUVD-2026-101060</a>                           |
| <b>Current data</b>         | <a href="https://evulnable.com/vulnerability-management/cve/CVE-2026-98411">evulnable.com/vulnerability-management/cve/CVE-2026-98411</a>               |                             |                                                                                                                                                         |

Snapshot at generation time. EPSS can move quickly. A public exploit module is not evidence of active exploitation.