Siemens RUGGEDCOM APE1808: Fortinet FortiOS double free flaw (CVE-2026-106175)



CISA relays a Siemens advisory on RUGGEDCOM APE1808 units running Fortinet NGFW, affected by a FortiOS double free flaw. Siemens advises updating Fortigate NGFW to V7.6.9 or later.

- All versions of RUGGEDCOM APE1808 with Fortinet NGFW are listed as known affected.
- CVE-2026-106175 is a Double Free flaw (CWE-415) in FortiOS, FortiProxy and FortiSwitch.
- A local authenticated attacker could crash the newcli daemon using crafted CLI commands.
- The CVSS v3 score listed is 2.3, a low rating.
- Siemens recommends updating Fortigate NGFW to V7.6.9 or later via its secure update procedure.

What was published

CISA has republished a Siemens advisory covering the RUGGEDCOM APE1808, an industrial product that can run Fortinet's next-generation firewall software. The advisory follows Fortinet's own disclosure of a Double Free vulnerability, tracked as CVE-2026-106175 (CWE-415), in FortiOS, FortiProxy and FortiSwitch.

Impact

According to the source, a local attacker who is already authenticated could use crafted CLI commands to crash the newcli daemon. The listed CVSS v3 score is 2.3, so the severity is low. All versions of RUGGEDCOM APE1808 with Fortinet NGFW are marked as known affected. Siemens is headquartered in Germany, and the advisory lists the Critical Manufacturing sector with worldwide deployment.

Recommended remediation

Siemens advises updating Fortigate NGFW to V7.6.9 or later, following its secure update recommendation procedure. Detailed information is available through Siemens customer support.

Given the low score and the need for local authenticated access, this is a matter for routine, planned patching rather than emergency action. Institutions operating these units in industrial or operational technology networks should still confirm exposure and schedule the update.

What to do now

1. Identify any RUGGEDCOM APE1808 units running Fortinet NGFW in your asset inventory.
2. Plan an update of Fortigate NGFW to V7.6.9 or later using Siemens' secure update procedure.
3. Contact Siemens customer support for the detailed update information.
4. Restrict CLI and local administrative access on these devices to authorised staff only.
5. Record the change through your OT change-management process.