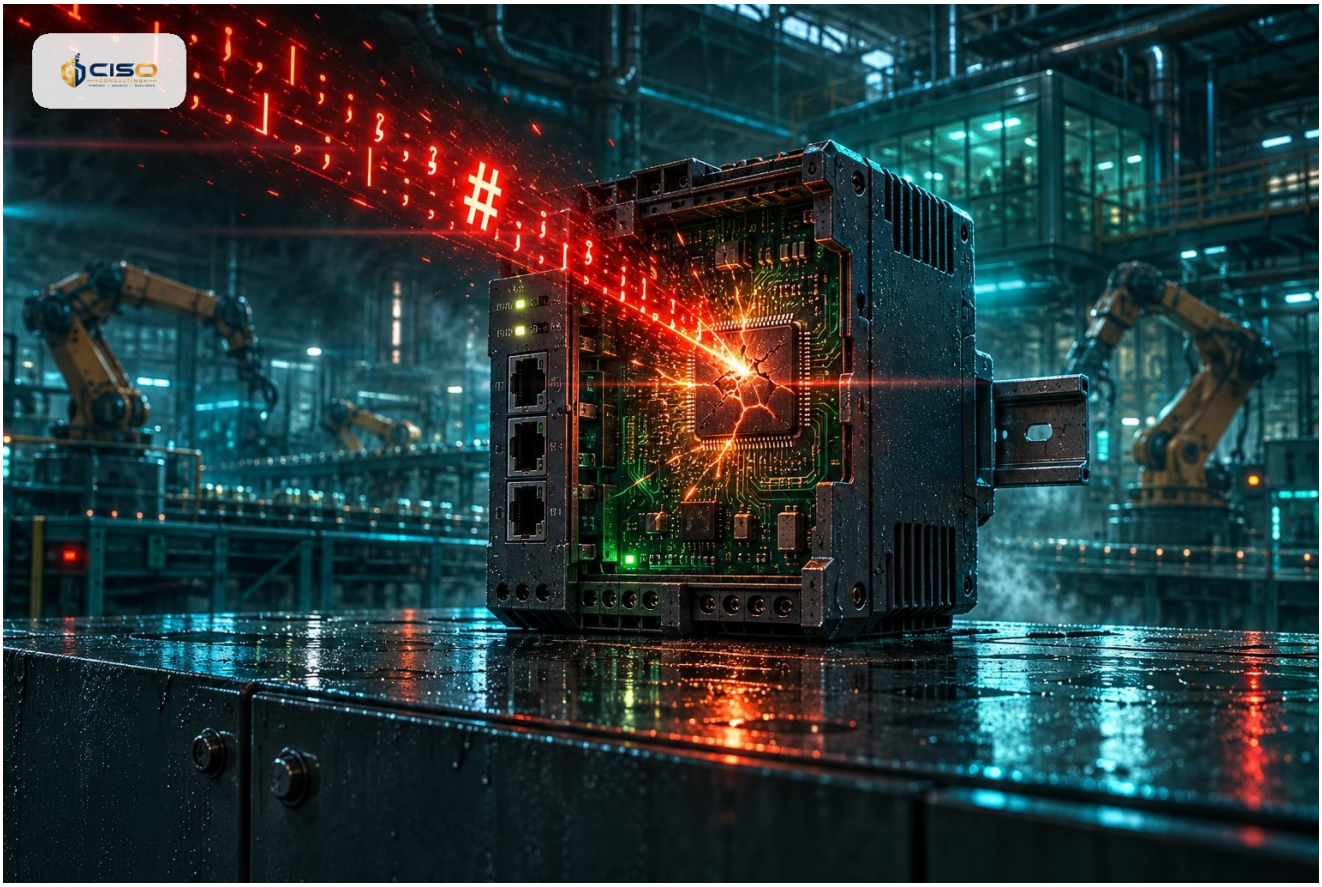
Siemens meta-iot2050 firmware update tool flaw allows root command execution (CVE-2026-109830)



CISA reports a command injection flaw (CVE-2026-109830, CVSS v3 7.3) in the meta-iot2050 firmware update tool from V01.03.01. Siemens is preparing fixes and advises mitigations meanwhile.

- Affected: Siemens meta-iot2050 from V01.03.01 onward.
- CVE-2026-109830 is an OS command injection in the firmware update tool, rated CVSS v3 7.3.
- An attacker able to alter a configuration file could run arbitrary commands as root.
- The tool executes parts of the configuration file without checking them.
- Siemens is preparing fixes; no remediation is listed as available yet, so mitigations apply.

CISA has published an industrial control systems advisory covering a vulnerability in Siemens meta-iot2050, the project behind software for the company's IOT2050 devices. The issue affects versions from V01.03.01 onward.

What the flaw is

The firmware update tool takes parts of a configuration file and executes them without validating them. This is an OS command injection weakness, tracked as **CVE-2026-109830** and scored 7.3 on the CVSS v3 scale. An attacker who is able to manipulate that configuration file could cause arbitrary commands to run as root on the device.

The advisory lists Critical Manufacturing, Energy and Information Technology as the affected sectors, with worldwide deployment. Siemens is headquartered in Germany.

Current status

The product status is listed as known affected, and the advisory shows no remediation available at this time. Siemens is preparing fixes and recommends mitigations for products where fixes are not yet available.

Exploitation depends on the attacker being able to alter the configuration file, so controlling who can write to it is a practical first line of defence. Organisations in the Kingdom that run these devices in operational or edge environments should confirm whether they are in use, identify versions, and follow the Siemens guidance as it is updated.

What to do now

1. Inventory devices running meta-iot2050 V01.03.01 or later, including OT and edge environments.
2. Restrict write access to the configuration file used by the firmware update tool to a minimal set of authorised administrators.
3. Apply the mitigations in the Siemens advisory where no fix is available, and monitor for the fixed release.
4. Monitor configuration files and update-tool activity for unexpected changes or commands run as root.
5. Record the exposure in your OT risk register and align treatment with NCA OTCC and ECC vulnerability management requirements.