

Inductive Automation Ignition: privilege escalation flaw (CVE-2026-92817) allows code execution



CISA reports an incorrect-authorization flaw in Ignition (CVE-2026-92817, CVSS 8.8) that lets a low-level authenticated user gain Designer-level privileges and run code on the Gateway. Versions 8.1.0–8.1.54 and 8.3.0–8.3.8 are affected.

- CVE-2026-92817 is an incorrect-authorization vulnerability with a CVSS v3 score of 8.8.
- Affected: Ignition 8.1.0 to 8.1.54 and 8.3.0 to 8.3.8.
- The Perspective module does not properly validate session privileges when determining Designer-level access.
- A user with access to a Vision project could use a valid Vision session identifier to gain Designer-level privileges.
- Exploitation could allow arbitrary code execution in the context of the Ignition Gateway process.

CISA has published an ICS advisory on Inductive Automation Ignition, an industrial software platform used in critical manufacturing, energy and information technology sectors worldwide.

What the flaw is

The issue, tracked as **CVE-2026-92817**, is an incorrect-authorization weakness rated 8.8 on the CVSS v3 scale. The Ignition Perspective module does not properly validate session privileges when it decides whether a user has Designer-level access. A user who is already authenticated and has access to a Vision project could present their own valid Vision session identifier and be granted Designer-level privileges.

With those elevated privileges, an attacker could execute arbitrary code in the context of the Ignition Gateway process.

Affected versions

- Ignition 8.1.0 through 8.1.54
- Ignition 8.3.0 through 8.3.8

The advisory notes that Inductive Automation has released version 8.3.9 as a mitigation. The source excerpt does not give further remediation detail, so teams should consult the full CISA advisory and the vendor's own notes.

What this means for operators

Exploitation requires a valid login, so the exposure depends on who holds accounts with Vision project access. Organisations running Ignition in operational environments should identify their versions, confirm which users can reach Vision projects, and plan the update through their normal change process for OT systems.

What to do now

1. Inventory all Ignition instances and identify any running versions 8.1.0–8.1.54 or 8.3.0–8.3.8.
2. Review the full CISA advisory and Inductive Automation's notes, then plan an update to a fixed version such as 8.3.9 through OT change control.
3. Review which accounts have access to Vision projects and remove access that is not needed.
4. Monitor Ignition Gateway hosts for unexpected Designer-level activity or unusual process behaviour.
5. Record the exposure and remediation status in your OT risk register in line with NCA OTCC requirements.