Siemens ROS# before 2.3.1: code injection flaw (CVE-2026-109097)



CISA reports a code injection flaw in Siemens ROS# versions before 2.3.1 (CVE-2026-109097, CVSS 8.2). Siemens advises updating to version 2.3.1 or later.

- Affected: Siemens ROS# versions earlier than 2.3.1.
- CVE-2026-109097, classed as CWE-94 (code injection), carries a CVSS score of 8.2.
- Message definition text is not properly escaped, so a crafted file could inject arbitrary code into the generated program.
- The vendor fix is to update to V2.3.1 or later.
- CISA lists the Critical Manufacturing sector; the vendor is headquartered in Germany.

What was reported

CISA has published an advisory on Siemens ROS#, noting that versions before 2.3.1 contain a code injection vulnerability tracked as CVE-2026-109097. The issue is classified as CWE-94, improper control of generation of code, and has a CVSS v3 base score of 8.2.

How the flaw works

Affected versions do not properly escape the text of message definition files. If an attacker can get a crafted message definition file to a user, that file could cause arbitrary code to be injected into the program that the tool generates. The advisory lists the Critical Manufacturing sector and states that the product is deployed worldwide.

Recommended response

Siemens has released a fixed version and recommends moving to V2.3.1 or later. The advisory does not describe any workaround or report of exploitation, so updating is the stated remediation.

Organisations with industrial or manufacturing environments should first establish whether ROS# is used anywhere, including by engineering or development teams, and which versions are in place. Where it is present, plan the update through normal change control and treat message definition files from outside sources with caution until the update is applied.

What to do now

1. Inventory any use of Siemens ROS# across engineering, development and OT teams and record the versions.
2. Update affected installations to V2.3.1 or later through change control.
3. Until updated, avoid using message definition files from untrusted or unverified sources.
4. Review programs generated from externally supplied message definition files for unexpected content.
5. Track the Siemens and CISA advisories for any revisions.