NEW CRITICAL VULNERABILITY ADVISORY: CVE-2026-58115

Summary

CVE-2026-58115 is a newly disclosed Critical vulnerability. It is not yet on CISA's actively-exploited list; treat it as proactive patching before it is weaponised. A vulnerability has been identified in SIMATIC IoT2050 Advanced (6ES7647-0BA00-1YA2) (All versions < V4.3.4.1 running Industrial OS with Node-RED installed). Affected devices do not enforce authentication on the Node-RED HTTP interface, allowing unauthenticated access to programming nodes that are capable of executing system commands on the server.

This could allow an unauthenticated remote attacker to create malicious flows through the HTTP interface in order to execute arbitrary code on the underlying server with maximum privileges.

What we know

- **CVE:** CVE-2026-58115
- **Status:** Newly disclosed, not yet known-exploited (not on CISA KEV)
- **Severity:** CVSS 10.0 Critical, Network-exploitable, no privileges required, no user interaction (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H)

Recommended action

Patch as a fix becomes available, prioritised by the exposure and EPSS above. Until then, restrict network access to the affected service now (segment it, put it behind a VPN, or take it offline) until you can patch. This does not yet trigger CRA 24-hour reporting, which requires active exploitation, but patching ahead of exploitation is the whole point.

Sources: NIST NVD. Public data; an advisory of a newly disclosed vulnerability, not an incident report. Verify applicability to your estate before acting.