

Cyber Resilience Act explained — scope, classes and deadlines

SECONDARY

Publisher CyberResilienceAct.eu

Published 2026-09-11

Retrieved 2026-10-06

Cite key cyberresili2026cyber

URL <https://www.cyberresilienceact.eu/explained.html>

Assessment. Secondary. Used only to corroborate the article number and the timeline already established from the Commission's own page; nothing rests on it alone.

Reporting articles. Articles 14 and 16 carry the reporting duties: 24 hours for an early warning on an actively exploited vulnerability or severe incident, 72 hours for the fuller notification with corrective measures, 14 days for the final report once resolved.

Timeline. 10 December 2024 entry into force. 11 June 2026, Chapter IV applies. 11 September 2026, reporting obligations begin. 31 October / 31 December 2026, core harmonised standards due. 11 December 2027, full application of most provisions.

Open source. Non-commercial open-source software developed outside a commercial activity is largely outside scope; open-source stewards have a lighter, tailored set of obligations.