TP-Link Systems Statement - EU Cyber Resilience Act

TP-Link Systems Inc. affirms its commitment to strengthening the security and resilience of its products throughout their lifecycle through efforts to align with the principles and requirements of the EU Cyber Resilience Act (CRA), including secure-by-design development, cybersecurity risk management, vulnerability handling, coordinated vulnerability disclosure, ongoing security maintenance, timely security updates, and transparency for customers and regulators.

Under the CRA implementation timeline, Article 14 reporting obligations will apply beginning September 11, 2026. The CRA's remaining requirements generally apply beginning December 11, 2027.

Article 14: Reporting of Actively Exploited Vulnerabilities and Severe Incidents

Beginning September 11, 2026, Article 14 requires manufacturers to report actively exploited vulnerabilities and severe incidents affecting the security of applicable products with digital elements.

TP-Link Systems supports coordinated vulnerability disclosure and welcomes good-faith vulnerability reports from security researchers, customers, industry partners, and other members of the security community. Potential security vulnerabilities may be submitted through TP-Link Systems' designated security reporting channels.
https://www.tp-link.com/us/press/security-advisory/

TP-Link Systems maintains a Product Security Incident Response Team that receives and evaluates vulnerability reports, coordinates remediation and security updates, and communicates with relevant stakeholders. TP-Link Systems continues to adapt these processes to support applicable CRA reporting and user-communication obligations and continues to prepare for the CRA requirements that apply beginning December 11, 2027.