DOT Europe statement

On Vulnerability Reporting Provisions in the Cyber Resilience Act

DOT Europe and its members[1] wish to add their voice to a growing and established concern surrounding the obligation to notify ENISA of unpatched vulnerabilities. We recognise the ambition of policymakers to harmonise cybersecurity requirements for digital products in the proposal for a Cyber Resilience Act (CRA) and understand the importance of increased cybersecurity worldwide, particularly in light of the war in Ukraine and the overall increase in instances of cyber-attacks by malicious actors.

Among others, the CRA outlines key provisions on vulnerability handling and reporting. In particular, Article 11 of the proposal provides for reporting obligations for manufacturers obliging them to notify any actively exploited vulnerability contained in the product with digital elements to ENISA. Unpatched vulnerabilities – referring to those security weaknesses in software, hardware, or systems that have not yet been addressed through an update or patch – pose significant threats to all types of organisations, including by acting as a primary avenue of attack for malicious actors.

The proposal has come a long way in the legislative process with both the Council and the European Parliament adopting their respective negotiating positions in view of the upcoming trilogues. DOT Europe welcomes the progress made by both institutions in further specifying the obligations outlined above with a view to aligning these with existing legislation and introducing further safeguards.

Whilst, however, recognising this progress made by co-legislators, DOT Europe maintains that, at its core, an obligation to report unpatched vulnerabilities would further weaken cybersecurity resilience levels in the Union as opposed to strengthening it. Requiring manufacturers to report unpatched vulnerabilities would, in practice, significantly harm the goals of the proposal and the overall cybersecurity level during a time in which it is needed most. In particular, DOT Europe would outline the following considerations:

1. Requiring manufactures to report unpatched vulnerabilities to which they have not yet found a solution **would further entice malicious actors to focus on these unmitigated vulnerabilities** as specific avenues of exploitation. It would align Europe with countries like China where similar problematic rules exist. The country's vulnerability reporting regulation (effective since September 2021) requires the reporting of vulnerabilities to a government authority for review prior to the vulnerability being shared with the product or service owner. Such rules can enable state actors to exploit such bugs. The EU risks being the second region moving in the same direction, setting a worrying global precedent and undoubtedly undermining, instead of reinforcing, cybersecurity.
2. The obligation for all manufacturers to report such unpatched vulnerabilities directly to ENISA would **furthermore result in ENISA becoming the primary target of attacks.** Government stockpiles in the past have leaked online or been stolen, resulting in global cybersecurity incidents that cost lives and billions of euros. Such a repository can only have added value for malicious actors trying to access and exploit its information for example, the Log4j

[1] DOT Europe is the voice of leading Internet companies operating in Europe. Our members: Airbnb, Amazon EU, Apple, Discord, Dropbox, eBay, Etsy, Expedia Group, Google, Indeed, King, Meta, Microsoft, Mozilla, Nextdoor, OLX, Shopify, Snap Inc., Spotify, TikTok, Twitter, Yahoo, Yelp.

Rue du Trône, 60, 1050
Brussels, Belgium
Tel: +32 (0) 472 26 83 02

WWW.DOTEUROPE.EU
Transparency Register: 53905947933-43
DOT Europe was formerly known as EDiMA

vulnerability. Sharing unpatched vulnerabilities with governments should be discouraged and, even if well intended, creates more problems than it solves.

3. Overall, we **further caution policymakers against expanding the list of actors that would have access to or knowledge of such vulnerabilities**. According to the CERT Guide to coordinated vulnerability disclosure, even a *"mere knowledge of a vulnerability's existence in a feature of some product is sufficient for a skillful person to discover it for themselves."* While recognising the need to share information and knowledge, expanding the pool of actors with access to this information would also expand the list of targets for malicious actors as well as, in practice, result in these institutions becoming beacons for cyber-attacks.

DOT Europe thus calls on policymakers to further consider and refine the elements above during trilogues to ensure that the very provisions of the text do not hinder the goals of a more cybersecure European Union. The CRA should not result in European institutions becoming repositories and lighthouses of potential entry points for malicious actors.

Rue du Trône, 60, 1050
Brussels, Belgium
Tel: +32 (0) 472 26 83 02

WWW.DOTEUROPE.EU
Transparency Register: 53905947933-43
DOT Europe was formerly known as EDiMA