Council of the European Union
General Secretariat

Interinstitutional files:
2022/0272 (COD)

Brussels, 06 March 2023

WK 2943/2023 REV 1

LIMITE

CYBER

This is a paper intended for a specific community of recipients. Handling and further distribution are under the sole responsibility of community members.

WORKING DOCUMENT

From:	General Secretariat of the Council
To:	Delegations
Subject:	Discussion Paper on automatic security updates in the Cyber Resilience Act (CRA)

Delegations will find attached discussion paper on the above subject submitted by BE, CZ, DK, DE, EE, FR, NL and PL. FR has decided to co-sign this discussion paper.

Discussion Paper on automatic security updates in the Cyber Resilience Act (CRA)

submitted by Belgium, Czech Republic, Denmark, Germany, Estonia, France, the Netherlands and Poland.

Automatic security updates are crucial to prevent cyberattacks on a growing number of products, thereby addressing a serious threat to our digital economy. This Discussion Paper aims to strengthen the Cyber Resilience Act (CRA) by arguing that:

1) **security updates** of products with digital elements should in principle, **by default**, be **installed automatically**
2) products should come with **clear instructions on how to turn off this default setting**, and
3) the **end date** until which updates are provided should be **clearly indicated** on the product.

1. The challenge

Almost 80% of cyberattacks that exploit vulnerabilities do so based on vulnerabilities that were already known for two years or more, and for which security patches were available.[1] Users simply did not install the available updates, either because they are unaware or have little incentive, time, or knowledge to do so. However, for most products with digital elements **patch management is still largely left to the responsibility of the user**.

Some **90% of connected devices are used in non-critical settings**, by millions of non-expert users. Who remembers to update their connected lawnmower, children's toy, home heating system, or even their router – let alone spends their weekends installing all the new updates? Yet, when a vulnerability occurs on a system and no intervention takes place, protection is no longer a given.

Every day, there are on average 50 new vulnerabilities discovered, for which patches are often quickly made available. Before 2030, there will be an **expected 25.4 billion devices connected to the internet**, each with life cycles often spanning several years. Adding Operating Systems, apps, and countless other types of products to the equation, results in an immense and ever increasing attack surface. It is, furthermore, highly **unrealistic to expect a sudden, and continuous change in behaviour of millions of non-expert users**, especially if products lack a simple user interface.

The current status-quo leaves our **connected digital society exposed to significant risk**. The CRA has the potential to remedy this threat.

Additional provisions should be introduced to the Commission Proposal, along three lines:

- **(a)** obliging manufacturers of products with digital elements to not only provide security updates, but to establish a **default setting, whereby *security* updates are installed automatically**, at least for products intended for consumer use or providing exceptions for some limited cases (e.g. products intended for industrial use)**;**
- **(b)** obliging manufacturers to provide **clear instructions alongside the product on how to turn off this default setting;**
- **(c)** obliging manufacturers, distributors and importers to very **clearly indicate, at the time of purchase, on the product and/or its packaging and/or via digital means, the final date until which security updates will be provided for.**

[1] Checkpoint Cybersecurity Report 2021, p. 55-56. A 2015 Verizon Data Breach Investigations Report equally stated that over 70% of successful cyberattacks exploited known security vulnerabilities that had patches available.

2. An opportunity in the CRA

It is an important principle of the CRA (especially in Annex I, section 1) that products with digital elements are **placed on the market in their most secure default state**. A default setting that pushes updates so that they are installed automatically clearly fits this philosophy. Moreover, this approach is fully aligned with the recent OECD Council Recommendation on the Digital Security of Products and Services[2] and ETSI standards, such as the ETSI IoT standard EN 303 645 v2.1.1 (2020-06), section 5.3.[3]

For **Operating Systems on smartphones and computers, it is already standard procedure** to push updates and to allow users to choose a good time to install them. If users keep postponing, the updates are installed automatically after a given period. This mechanism should be extended as a default setting – but that can be deactivated by the user - to all products with digital elements, with certain exceptions applying.[4]

Four important principles should be underlined in this proposal:

1) Security updates and other e.g. functional updates should be distinguished;
2) critical environments must not be disrupted;
3) users should be informed and given the option to postpone; and
4) the end date of support must be a concrete date.

First, the requirement to automatically install updates by default, should be **limited to *security* updates**. It should remain as much as possible up to users to decide whether they want a functionality update or not. Security updates and other e.g. functionality updates should be clearly separated as much as is technically possible. However, we acknowledge that in certain cases, additional functionalities may be required in order to deploy a given security update. In this scenario, and provided that the main objective and outcome of the update is to enhance or maintain the security of the product, the update containing functionality alterations can be considered a security update.

Second, it is highly undesirable that security updates are installed automatically on products which are used in **critical environments**, such as industrial settings, company networks, military, national security

---

[2] See OECD, *Recommendation of the Council on the Digital Security of Products and Services*, OECD/LEGAL/0481. This Recommendation was adopted on 26 September 2022 and states, among others, that suppliers should "take an appropriate level of responsibility for preconfiguring products and services and managing their digital security, rather than shifting this responsibility to users, and in particular (…)
(a) pre-configure and activate security features by default, while allowing users to opt-out to configure the security features themselves.
(b) provide users with information about preconfigured security settings and clear and simple instructions for security configuration;
(c) provide users with, at least until the product's EOS and if possible until the product's EOU, security updates which are:
– free of charge;
– distinct from functional updates or upgrades, where possible;
– automatically activated by default, where possible, in particular for critical vulnerabilities, while enabling users to opt out from automatic updates for example if they need to manage the potential digital security risk that updates can pose in their use context."
(d) provide users opting out from automatic updates with information and warnings about possible risk to themselves and third parties."

[3] Provision 5.3-4 in particular concerns automatic mechanisms to be used for software updates while provision 5.3-6 states: "If the device supports automatic updates and/or update notifications, these should be enabled in the initialized state and configurable so that the user can enable, disable, or postpone installation of security updates and/or update notifications."

[4] Some Operating Systems may prevent manufacturers from automatically updating their software when running on such OS. That said, this practice is likely to go against the CRA and we thus assume that for products placed on the EU market, such practice would remain only a theoretical option.

or hospitals, as well as dual-use goods. Unexpected automatic updates could significantly hinder these critical operations. This is why an exception must be foreseen whereby the requirement to deliver products with a default setting that automatically installs updates would not apply to products used in such critical settings, possibly limiting the requirement to products intended for consumer use. Products that do not fall under this exception should also come with **clear instructions on how to turn off the default setting** of automated updates. That said, the very first update of a critical product may be mandatory insofar as it relates to the first use or accessing a network for the first time.

Third, alongside the key principle of "duty to inform", it is important that **users are informed** that a security update is ready to be installed, and that users are provided the **option to delay** this update until a better moment if they so desire – yet with a clear end time by when, if not installed, the default setting – if not switched off by the user – will automatically install the update.

Fourth, in order for consumers to be aware and confident that new vulnerabilities of their products will be dealt with, the **end date until which the manufacturer guarantees as a minimum to provide security updates should be clearly indicated** on the product, its packaging or another easily findable place (at least) at the moment of sale. It should not just be mentioned somewhere in the often extensive documentation, which only expert users will read. The end of support should be marked by a clear date (**month and year**), rather than as a general period after placing on the market, which few users will know or desire to calculate; they will only consider the time of buying. Such a clearly indicated end-date also addresses the risks when distributors would sell products after the proposed five year period or shorter expected lifespan after placing on the market, as suggested in the Commission Proposal. A separate debate on the best way to determine the length of the support period is needed and goes beyond the scope of this paper.

We acknowledge that the automatic installation of updates may seem to amplify a **risk of malicious actors injecting malware with an update** (cf. supply chain attacks). Yet this risk is inherently present even when updates are not installed automatically and require an action by the user. It is a risk that should be mitigated by requiring that security updates always be sourced from legitimate sources, be securely developed and deployed. All in all, the security risk posed by an unpatched product used by non-expert users is currently much higher than the risk of an infection by a malicious update, even if the latter should be taken very seriously and prevented by all possible measures.

Regarding the **practical implementation** of the requirement to install security updates automatically by default, we acknowledge that some specific products and scenarios require further discussions to ensure CRA provisions are realistic and practical. For instance, some products with digital elements may require special delivery mechanisms for security updates, especially if they are not connected to the internet. Another example are connected products such as dolls, lawnmowers, or routers, for which it may not always be easy to find an appropriate channel for informing users that updates are about to be installed. For such products, the security support provided by manufacturers may sometimes need to be complemented by an action on the part of the user. Such implementation challenges could perhaps be addressed by harmonisation standards under the CRA.

Moreover, a safety procedure may need to be foreseen at the level of standards in case a power cut occurs or the product's battery dies during the update process, to avoid a sudden unexpected shutdown of the product, or any damages to the product.

Finally, the default setting for automatic updates should comply with existing privacy legislation and the future **ePrivacy Regulation** as regards consent.

3. Options for amendments

The proposed additions to the text of the European Commission proposal are in **bold and underlined**:

- Annex I,1 (3)a:
  be delivered with a secure by default configuration, including the possibility to reset the product to its original state**, and including a default setting that security updates be installed automatically according to requirements in Annex I,2 (9) and Annex II,(8a), with a clear and easy-to-use opt-out mechanism, [if the product is intended for consumer use] / [unless it would lead, by nature of the product, to disruptions in industrial processes or could result in damage, loss of life or severe injury];**[5]

  These amendment proposals are a first attempt and we acknowledge that it may need to be improved. Further work is needed on the best way to formulate an exemption for industrial / non-consumer use in legal terms.

- Annex I,1 (3)k: ensure that vulnerabilities can be addressed through security updates, including, where applicable, through automatic updates **by default, but with a clear and easy-to-use opt-out mechanism, and where applicable through** the notification of available updates to users, **and the option to temporarily postpone them**.

- Annex I,2 **(9): where applicable under Annex I,1 (3)a, set as a default setting – which can be switched off – that security updates are installed automatically on products with digital elements if not installed within a certain timeframe;**

- Annex II (8): the type of technical security support offered by the manufacturer and until when it will be provided, at the very least until when users can expect to receive security updates; **this earliest end date of support should also be clearly indicated at the time of purchase, in an easily accessible manner and where applicable on the product, its packaging and/or by digital means;**

- Annex II (**8a): simple and clearly understandable instructions on how the default setting of automatically installed updates, as required by Annex I,2(9) can be turned off;**

- Art.14(2)(b) the manufacturer and the importer have complied with the obligations set out respectively in Articles 10(10), **10(10a),** 10(11) and 13(4).

- **Recital (11a) Many cyberattacks exploit vulnerabilities that are known, often already for several years and for which patches exists. Findings show that security updates are not regularly applied by average users. This situation creates the risk of millions of unpatched and thereby vulnerable products, which poses a threat to the entire connected digital society. Manufacturers should therefore ensure that their products with digital elements that can be connected to the internet, include a default setting whereby security updates are not only offered to the user, but installed automatically, especially if the user does not install them within a reasonable timeframe. This default setting should, however, not be required for products for which consumers would not reasonably expect it, for instance in the case of products intended for use in industrial environments. Moreover, this obligation should only apply for security updates, not for other functionality or optimisation updates. Indeed, users should as far as possible be given the choice whether they wish to install non-security updates or not, and where applicable in accordance with Regulation [ePrivacy Regulation, COM(2017) 10 final]. Although security updates and other updates should ideally**

[5].

be clearly separated, this may not be possible in certain cases, such as when additional functionalities are required to deploy a given security update. In such cases, provided that the main objective and outcome of the update is to enhance or maintain the security of the product, or a security update is impossible to install without this functional update, the update containing some non-security alterations can be considered as a security update. Moreover, users should always be informed that an update will be automatically installed, with the possibility for them to opt out or temporarily postpone the update. The product should also come with clear instructions on how this default setting itself can be turned off, allowing users to install updates in a more controlled way, for example to avoid interference with operations in critical environments. When a user turns of the default setting for automatic updates, this action should not in any way affect the obligation of the manufacturer to keep offering security updates to this user. Manufacturers should also implement measures regarding the determination of the moment when security updates are automatically installed so as to reduce potential negative impacts on the user or the risk of damage to the product, which, for example, may occur if the update download or installation is initiated at an inappropriate time or is interrupted by insufficient product power or connectivity.

Moreover, we believe that **Art.10(6)** should be amended and a **new Article 10(10a)** should be added to require the **end of support date**, including at least the month and year, to be clearly and understandably indicated on the product, its packaging, and/or by digital means. A separate reflection is underway to provide concrete amendment suggestions in this respect and to address the broader issue of the length of the support period.