Cyber Resilience Act:
Vulnerability Handling

© ***Rob Hulsebos***

Version 2 (16 January 2024)

On 20 December 2023, three EU (European Union) institutions have agreed on the new proposal for the "Cyber Resilience Act", regulating "horizontal cybersecurity requirements for products with digital elements". In contrast to the NIS2, which focuses on "essential" and "important" ***users*** (called: entities) of products, the CRA is meant for ***vendors***.

In this article, we will focus on the part of the CRA related the handling of vulnerabilities discovered once the product is on the (EU) market.

Note: the author is active in OT cybersecurity, hence this article has a slight OT focus.

Why a CRA ?

The purpose of the CRA is to improve the cybersecurity posture of products, in both hardware and software. Today, many products are brought onto the market with many a vendor paying no (or minimal) attention to the cybersecurity of the hardware and the software in these products. The risks of using badly designed products are now at the users / product owners ("risk owners") while the benefits of developing bad products are at the manufacturer (less development and support effort, a competitive advantage).

The CRA will force the manufacturers to develop better cyber-secured products, execute a conformity assessment, do CE marking, inform customers about new vulnerabilities and develop patches during the support period, and inform (EU) authorities when needed.

Vulnerabilities

As stated earlier, many badly designed products (from a cybersecurity point-of-view) are brought on the market. But what about products that *are* properly designed? Still there is no guarantee that it is 100% cyber secure. Despite all efforts in architecting, designing, coding / implementing and testing a product to make it as cyber-secure as possible *before* it is put on the EU market, it is impossible to **not** have an architectural weakness, design flaw, or coding error (bug) in a product. Hackers abuse these vulnerabilities to gain unauthorized access to a product, install malware or ransomware, steal data, etc.

When a vulnerability becomes known (some 30000 yearly[1]), a vendor can make a "patch" (security update) which fixes the vulnerability. Users of the product must first download and then install the patch; from that moment on they are no longer vulnerable (until the moment a new vulnerability is discovered, and the cycle repeats).

Until the CRA, vendors had little obligations towards their customers in delivering products as cyber-secure as possible. The consequences of weak cybersecurity in products ended up at the customers – hacked products, malware, data theft, production loss, etc. Installation of patches also cost the customer money (and production loss).

[1] Based on statistics for the Common Vulnerability Enumerations (CVE) database. Note that these are only the publicly known vulnerabilities; there are many more vulnerabilities.

Some vendors even charge their customers for delivery of patches and/or its installation. Other vendors simply deliver no patches at all; they have already sold the product and no longer want to invest in something which brings no new income. Even worse are vendors that harass security researchers finding bugs in a product in their own time and at their own expense and report that to the vendor in good faith, sometimes being 'rewarded' with legal charges.

Does the CRA apply to *my* products?

The CRA specifically states that it applies to "products with digital elements":

> *… whose intended purpose or reasonably foreseeable use includes a direct or indirect logical or physical data connection to a device or network.*

There is a distinction between the category "products with digital elements" and "*important* products with digital elements" (art. 6). But for vulnerability handling there is no difference.

So the conclusion is that there is little escaping from the CRA, unless a product has no way to communicate over a network, or with another device; or the product is not brought onto the EU market. It also does not apply to products that are already on the market.

Legal pressure

The CRA wants vendors to deliver products as cyber-secure as possible. Only when all necessary obligations are fulfilled may the "CE" marking be attached to a product, a requirement to bring a product onto the EU market. The CRA thus also applies to non-EU vendors.

Conversely, if a product is found to have been brought onto the EU market without the vendor having fulfilled its obligations, the product may no longer be sold, or must be recalled, or must be fixed, and fines may be given (up to 15 million Euro's or up to 2.5% of the worldwide turnover, whichever is higher).

Vulnerability handling requirements

Annex I of the CRA describes the "Essential Cybersecurity Requirements" for products. Part I of this annex describes how products are to be *developed*. Part II of this annex describes the handling of *vulnerabilities:* vendors must develop and deliver security updates to customers, for the support period[2] of the product.

Below, we will take the literal text of Part II of Annex I of the CRA, and comment on each sentence. The original text is shown in **red**. The CRA lists 8 paragraphs, we show these in **blue**.

Paragraph 1

Identify and document vulnerabilities and components contained in the product …

It only looks logical to remove any known vulnerability *before* a product is brought onto the market. But sometimes this is just not possible. Software-components may be out of support, and hardware-components cannot be changed.

> Changing software looks simple, but often is not. For example, when an operating system (OS) is out of support: changing an OS in an application is a major undertaking.
>
> Changing hardware is also not trivial: for example, architectural flaws in Bluetooth or WiFi chips, and, AMD or Intel processors always cannot be resolved via a security. New hardware would be needed (if possible at all).

[2] According consideration 33a, the support period "should reflect the time the product is expected to be in use". Next, consideration 33b and 33d give guidance on what the minimum support period is.

The user must be informed about such vulnerabilities; it cannot be left to the user to "know" what is inside a product. It could be argued that such a product should not use such components, but sometimes there is just no alternative (also, the vulnerability could have been unknown at the time the hardware was designed).

Also, not all users may be affected by a vulnerability in (say) Bluetooth; perhaps this network is not needed in certain applications and can be shut off (in effect remediating the vulnerability). But a user should still know, and so can make an informed decision.

… including by drawing up a software bill of materials …

The "software bill of materials" (SBOM[3]) is a list of all used / integrated software libraries, components, drivers, etc. used by a product. It is to be provided by the vendor. The purpose of the SBOM is to provide a formal description containing details and supply-chain relationship of components in the product. Normally such information is only known to the vendor.

The value of an SBOM to an end-user is not so large, it is more intended for manufacturers "to ensure that their products do not contain vulnerable components developed by third parties" (consideration 37).

Note that the CRA states that manufacturers should not be required to make the SBOM public (annex II article 10). But it must always be provided as part of the technical documentation (Annex V) and it to be provided to a market surveillance authority upon request.

… in a commonly used and machine-readable format …

Import of SBOM in an asset-management tool helps to automate vulnerability management. The tool might warn for newly published vulnerabilities, so the user is (automatically) informed about it and might take mitigating measures while the vendor is working on a security update.

The asset-management tool must also be able to retrieve machine-readable information about (resolved) vulnerabilities. Currently there is no widely adopted standard for this; "CSAF" (Common Security Advisory Format) is a good standard, but at this moment (2024/1) only a few vendors support it.

In the current revision of the CRA, which SBOM format is to be used is not specified. This will be decided via an additional "implementing act" (consideration 15), taking into account European and international standards and best practices.

… covering at the very least the top-level dependencies of the product

For a software developer, the top-level dependencies of a product are always known, as these are the libraries / component / drivers / … connected to or used by the own software or hardware. Of course, there could be lower-level dependencies, but it is often impossible to know them in case of binaries. The suppliers for these should provide an SBOM of their own, so the whole dependency-tree can be drawn up[4].

Paragraph 2

Address and remediate vulnerabilities without delay, including by providing security updates

This enforces suppliers to actively support their product, and not silently ignore any new vulnerabilities (which would make the purpose of the CRA moot). Of course, the exact meaning of "without delay" might vary per vendor as the product development process and associated quality procedures might take time. People not familiar with product development are often surprised that a security update cannot be delivered the same day or in the same week. This very much depends on the availability of internal resources needed to execute the necessary steps. Sometimes, software needs to be pass a certification, which could take months.

[3] Well-known SBOM formats are CycloneDX and SPDX. The CRA has no preference (yet), but these 2 are approved under the US government's 2021 cybersecurity executive order.

[4] This will probably take some time to implement!

Of course, prioritization is possible depending on the severity of a certain vulnerability, but the CRA does not require it. However, customers could push their vendors to more quickly remediate a vulnerability.

… where technically feasible, new security updates shall be provided separately from functionality updates

Some vendors do currently not release patches for vulnerabilities, but include them together with functional updates. Sometimes this has unforeseen consequences as functional updates may require new hardware, or additional licensing, or force changes to the user's own application. This would make that the security update is not installed (or very much delayed) by customers, defeating the purpose of the CRA.

Also, some vendors have a quarterly / semi-annual / annual release cadence. This would make that a customer must wait for the next update to have a vulnerability remediated. When vulnerabilities are actively exploited by hackers, customers should not need to wait 3 / 6 / 12 months before being able to remediate a vulnerability.

Paragraph 3

Apply effective and regular tests and reviews of the security of the product

Vendors should incorporate test and review in their development procedures, for example formal reviews of changes to their own software, using vulnerability scanners (either static or dynamic), and/or performing penetration tests.

Paragraph 4

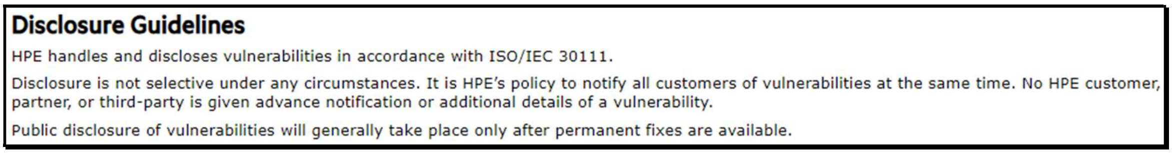
Once a security update has been made available, share and publicly disclose information about fixed vulnerabilities, including a description of the vulnerabilities, information allowing users to identify the product with digital elements affected, the impacts of the vulnerabilities, their severity and clear and accessible information helping users to remediate the vulnerabilities

Most users are not cybersecurity experts. Currently we see that information about vulnerabilities, security updates and remediations is highly technical, written by an expert in cybersecurity for another expert in cybersecurity. The CRA apparently wants more easily comprehensible documentation.

See paragraph 8 for an example of rather useless information.

In duly justified cases, where manufacturers consider the security risks of publication to outweigh the security benefits, they may delay making public information regarding a fixed vulnerability until after users have been given the possibility to apply the relevant patch.

Of course, hackers also read vendor information, providing too much detail about vulnerabilities too soon adds extra risk. Currently, it is already often seen that vulnerability details are published months after the security patch has been made available.



Disclosure Guidelines

HPE handles and discloses vulnerabilities in accordance with ISO/IEC 30111.

Disclosure is not selective under any circumstances. It is HPE's policy to notify all customers of vulnerabilities at the same time. No HPE customer, partner, or third-party is given advance notification or additional details of a vulnerability.

Public disclosure of vulnerabilities will generally take place only after permanent fixes are available.

Examples of a company's vulnerability disclosure guidelines

Paragraph 5

Put in place and enforce a policy on coordinated vulnerability disclosure

Security researchers who find a vulnerability in a product often report this to a vendor and give the vendor time to fix the vulnerability and release a patch, before the researchers go public with the vulnerability (for example in a cybersecurity conference, or publication). Often the vendor is given 90 days, in which time he can fix the vulnerability and start informing customers. This policy makes that by the time the vulnerability is made public, many users already have patched their products, keeping hackers out.

But: some vendors do not like to be informed about vulnerabilities in their products. Instead of fixing them, lot of time is spent arguing, dismissing the vulnerability, starting legal procedures, taking weeks to answer on emails, etc. If the CRA could bring a change here, that would be a big step forward.

Paragraph 6

Take measures to facilitate the sharing of information about potential vulnerabilities in their product …

Vendors should tell their customers what (potential) vulnerabilities are present in their product. Nowadays, this is seldom none. Users have no idea what they have to defend against; vendors don’t tell them (and perhaps often don’t even know). Why? Is it shame? Competitive pressure? Fear of legal procedures? Ignorance? Assuming that users don’t want to know?

There are examples of vendors who do publish information about (potential) vulnerabilities in their products, even when no security update is available. Users than at least know about it, and can take extra defensive measures until the security update is available (which may sometimes take months).

Of course, hackers also read vendor information, therefore I understand that providing too much detail about vulnerabilities adds extra risk (also addressed in paragraph 3). A balance should be found.

There are vendors (like Hewlett-Packard Enterprise) which never provide information about vulnerabilities in their products; luckily they *do* provide security updates.

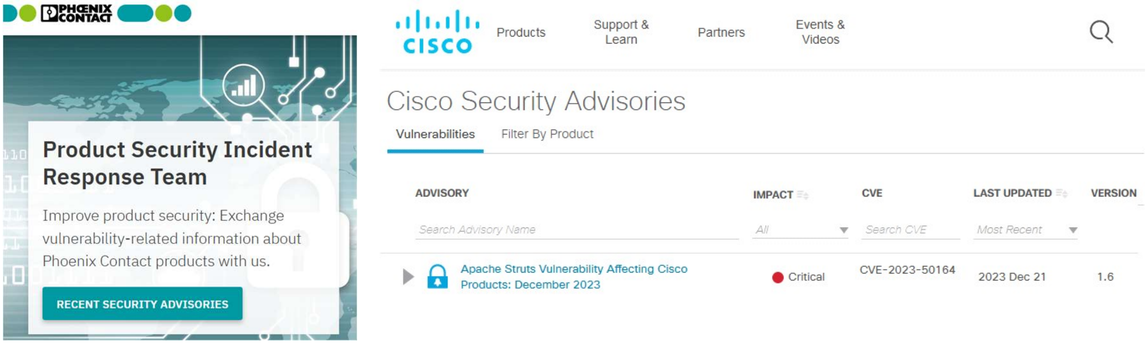
… as well as in third party components contained in that product

See the previous comment.
Providing details about which third party components are contained in a product is valuable information for hackers, which normally can only be obtained by an analysis of the software in a product. The CRA should not make life easier for hackers!

… including by providing a contact address for the reporting of the vulnerabilities discovered in the product

Many companies now have established a “ProductCERT[5]” or “PSIRT” (Product Security Incident Response Team) which is the central point of contact for all cybersecurity-related product issues.

Very large companies may even have multiple such teams (for different product ranges).
The usual way of communication is per email.



Product Security Incident Response Team

Improve product security: Exchange vulnerability-related information about Phoenix Contact products with us.

Cisco Security Advisories

ADVISORY	IMPACT	CVE	LAST UPDATED	VERSION
Apache Struts Vulnerability Affecting Cisco Products: December 2023	● Critical	CVE-2023-50164	2023 Dec 21	1.6

Two examples of a ProductCERT / PSIRT

[5] The term “CERT” is © copyright Carnegie-Mellon and must be licensed, hence some vendors uses “PSIRT”.

In case a company does not have a ProductCERT / PSIRT, an email contact could be used. The internet-standard for this is RFC-9116[6], in the file "security.txt" contacts can be given.

Paragraph 7

Provide for mechanisms to securely distribute updates for products …

Having an update available for a product is step 1, but such updates can be targeted by hackers as well. If an update is modified to include malware, every user who installs such an update automatically gets the malware as well. For a hacker, this is a very effective way of distributing malware: hack the vendor, and subsequently all its customers are hacked automatically when they download the (modified) security update.

So the website / servers who are used in distributing updates must be properly secured as well. Also, modifications by hackers to the security updates themselves must be prevented. For example, updates should be digitally signed. In turn this requires good protection of the certificates / keys on internal systems.

… to ensure that vulnerabilities are fixed or mitigated in a timely manner …

This is a requirement for the software development process of a vendor. The challenging part is that vulnerabilities "appear" at unpredictable moments, and this disrupt the regular software development process (planning, staffing, contractual obligations, 3rd-party involvement, etc.).

The CRA does not state how we should read "timely". Manufacturers now typically general respond within a week for high-criticality vulnerabilities[7], but otherwise count on (multiple) months[8].

… and where applicable for security updates, in an automatic manner.

Installing security updates is often not done by users, as they do not know about the existence of such updates, and/or are not knowledgeable about the necessity, do not know the procedure to update, or they just don't care. Having automatic updates is a way to work around this, as is done in many browsers for years.

However, it does require internet access, which in turn requires the vendor to set up an update server. Also the products must be designed to allow for automatic updates (i.e. have extra memory, outward connectivity). Manufacturers shouldn't forget that the update server and the security update installation software *themselves* need to be adequately protected against hackers.

In OT environments, automatic installation of security updates is often unwanted, as the installation process might take the device out of operation at an unwanted moment[9]. The user should then have the capability to either disable the automatic installation, or have the installation scheduled to only run at certain moments (i.e. on Saturday night).

The necessity to have internet access also requires a network to be properly protected, i.e. at least a firewall (and then this device needs to be secured and updated as well!).

So, a simple one-liner sentence in the CRA could mean a lot of work for manufacturers!

Paragraph 8

Where security updates are available to address identified security issues, they are disseminated without delay

Literally, I read here that as soon as a security update is available, it should be made available to users. The best way to prevent hacks is of course to patch ASAP, especially for high-risk vulnerabilities or exploited vulnerabilities.

[6] See https://www.rfc-editor.org/rfc/rfc9116

[7] Like with the "Log4J" vulnerabilities

[8] As an example, see vulnerability https://cert.vde.com/en/advisories/VDE-2023-026/, reported 31 July 2023, with a fix promised Q1 2024.

[9] Famous example is a drone vendor who allowed automatic updates while in-flight, causing the drone to crash because the CPU was busy with other tasks than flying.

In practice, many vendors follow a different cadence for publishing security updates, following the procedure started by Microsoft decades ago. At the time, the large amount of security updates in Windows made that sysadmins got multiple security updates *every day*, swamping them in work. Microsoft then started to accumulate all security updates, and publish them all together on the second Tuesday of each month. This "Patch Tuesday" (as it is now called) is a predictable moment, allowing for users to plan their work. Many other vendors also follow this monthly cadence (for example Siemens).

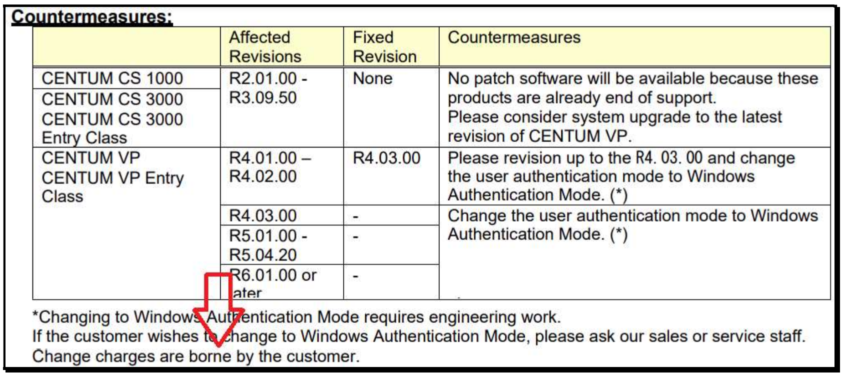
Out-of-band security updates can of course still be published at other moments, depending on the risk of the vulnerability, at the discretion of the vendor.

… unless otherwise agreed between manufacturer and business user in relation to a tailor-made product

This sounds logical.

… free of charge …

Vendors may not charge users for security updates, either directly or via a support contract. It is unclear whether vendors are allowed to charge you for *installing* a security update.



Countermeasures:

	Affected Revisions	Fixed Revision	Countermeasures
CENTUM CS 1000 CENTUM CS 3000 CENTUM CS 3000 Entry Class	R2.01.00 - R3.09.50	None	No patch software will be available because these products are already end of support. Please consider system upgrade to the latest revision of CENTUM VP.
CENTUM VP CENTUM VP Entry Class	R4.01.00 – R4.02.00	R4.03.00	Please revision up to the R4. 03. 00 and change the user authentication mode to Windows Authentication Mode. (*)
	R4.03.00	-	Change the user authentication mode to Windows Authentication Mode. (*)
	R5.01.00 - R5.04.20	-	
	R6.01.00 or later	-	

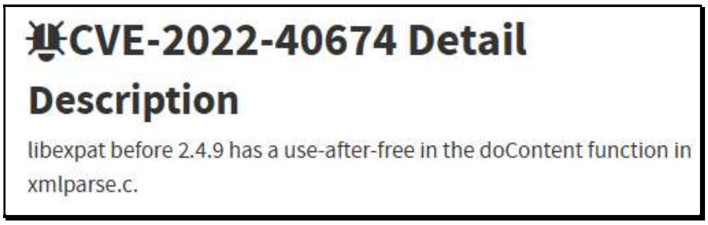
*Changing to Windows Authentication Mode requires engineering work.
If the customer wishes to change to Windows Authentication Mode, please ask our sales or service staff.
Change charges are borne by the customer.

From Yokogawa advisory YSAR-23-0001

… accompanied by advisory messages providing users with the relevant information, including on potential action to be taken.

The usual advice that comes with security updates is: install it as quickly as possible. Some vendors provide mitigations or recommendations – what to do if you don't want to (or cannot) install a security update.

In my personal experience, ordinary users do not have the same knowledge about root-causes of vulnerabilities as experts working in cybersecurity. For example, the descriptions in CVE's are often completely incomprehensible. And some vendors do not give any information about the root-cause vulnerabilities at all.

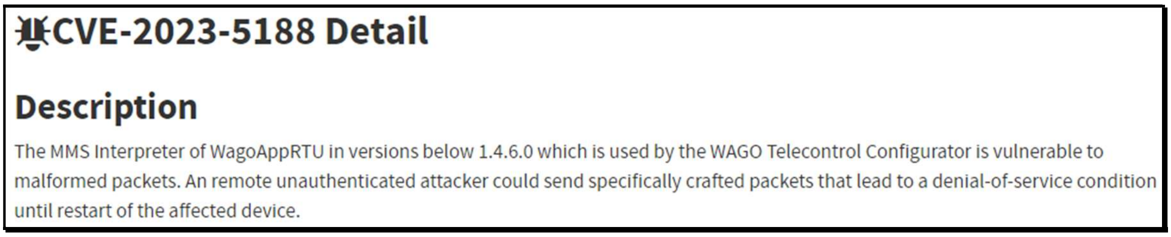


CVE-2022-40674 Detail

Description

libexpat before 2.4.9 has a use-after-free in the doContent function in xmlparse.c.

Example of an almost useless description (for users) of a vulnerability.



CVE-2023-5188 Detail

Description

The MMS Interpreter of WagoAppRTU in versions below 1.4.6.0 which is used by the WAGO Telecontrol Configurator is vulnerable to malformed packets. An remote unauthenticated attacker could send specifically crafted packets that lead to a denial-of-service condition until restart of the affected device.

A better example of a description, although you still need technical knowledge.

Summary

Although the vulnerability handling requirements are written down in just one page in the CRA, the consequences for the vendors of products are large. Development and support-procedures must be set up, legal and user documentation written, keeping watch over externally discovered vulnerabilities, generating security updates, changes to the products to allow for secure updating, etc.

For many (smaller) vendors this will be new, and the knowledge will not be available in-house. Luckily, the CRA is not info force yet, and once it is, there is a 21-month transition period (see article 57) after which reporting vulnerability requirements come into force (see article 11), and 36 months for all other requirements. So you still have some time to implement the requirements of the CRA.

The CRA is not final yet; the definitive version might be different from the draft version published on 20 December 2023 which is the base for this document.

The information above is my interpretation of the CRA draft text.
Consult a legal expert for advice on how the CRA might apply to your company.

If you have any suggestions, comments or additions,
please do not hesitate to contact me (email: rh[at]enodenetworks.com).

Version	Date	Changes
1	2 January 2024	Original text
2	16 January 2024	Updated after review and comments from LinkedIn: regarding certification, support period of products