

TLP - CLEAR



EUROPEAN UNION AGENCY
FOR CYBERSECURITY

ENISA Technical Advisory on security.txt, CVD Policies and Security Advisories

SME Vulnerability Kit

OCTOBER 2026

About ENISA

The European Union Agency for Cybersecurity, ENISA, is the Union's agency dedicated to achieving a high common level of cybersecurity across Europe. Established in 2004 and strengthened by the EU Cybersecurity Act, the European Union Agency for Cybersecurity contributes to EU cyber policy, enhances the trustworthiness of ICT products, services and processes with cybersecurity certification schemes, cooperates with Member States and EU bodies, and helps Europe prepare for the cyber challenges of tomorrow. Through knowledge sharing, capacity building and awareness raising, the Agency works together with its key stakeholders to strengthen trust in the connected economy, to boost resilience of the Union's infrastructure, and, ultimately, to keep Europe's society and citizens digitally secure. More information about ENISA and its work can be found here: www.enisa.europa.eu.

CONTACT

For contacting the authors please use product_security@enisa.europa.eu.
For media enquiries about this paper, please use press@enisa.europa.eu.

AUTHORS

ENISA

ACKNOWLEDGEMENTS

LEGAL NOTICE

This publication represents the views and interpretations of ENISA, unless stated otherwise. It does not endorse a regulatory obligation of ENISA or of ENISA bodies pursuant to the Regulation (EU) No 2019/881.

ENISA has the right to alter, update or remove the publication or any of its contents. It is intended for information purposes only and it must be accessible free of charge. All references to it or its use as a whole or partially must contain ENISA as its source.

Third-party sources are quoted as appropriate. ENISA is not responsible or liable for the content of the external sources including external websites referenced in this publication. Neither ENISA nor any person acting on its behalf is responsible for the use that might be made of the information contained in this publication. ENISA maintains its intellectual property rights in relation to this publication.

COPYRIGHT NOTICE

© European Union Agency for Cybersecurity (ENISA), 2026

This publication is licenced under CC-BY 4.0 "Unless otherwise noted, the reuse of this document is authorised under the Creative Commons Attribution 4.0 International (CC BY 4.0) licence (<https://creativecommons.org/licenses/by/4.0/>). This means that reuse is allowed, provided that appropriate credit is given and any changes are indicated".

Copyright for the image on the cover and on pages -: © Shutterstock

For any use or reproduction of photos or other material that is not under the ENISA copyright, permission must be sought directly from the copyright holders.

ISBN 000, DOI 000

Table of Contents

Scope and context	4
2. security.txt, CVD policy and Security Advisory	6
2.1 security.txt	6
2.2 CVD policy	7
2.3 Security advisory	7
3. Common mistakes	8
4. Good practices and templates	10
4.1 security.txt implementation guide	10
4.2 Coordinated Vulnerability Disclosure (CVD) Policy	13
4.3 Security advisory	17
Bibliography / References	19
Annex: 20	
A.1 How this package supports CRA obligations	20

Scope and context

Manufacturers of products with digital elements need practical ways to receive, assess and communicate information about vulnerabilities. Clear reporting channels, structured disclosure processes and timely security communications are important parts of effective vulnerability management. In this context, tools and practices such as **security.txt**, **Coordinated Vulnerability Disclosure (CVD)** and **security advisories** can help organisations handle vulnerability information in a consistent and transparent manner.

The Cyber Resilience Act (CRA) introduces new vulnerability management obligations for manufacturers of products with digital elements. **Micro-, small and medium-sized enterprises (SMEs)** may need practical guidance and support to put these obligations into practice, particularly where cybersecurity, compliance or legal resources are limited. This package provides practical, ready-to-use templates that organisations can adapt to their needs and level of maturity. It also supports the practical application of the CRA's vulnerability management requirements and the harmonised standard EN 40000-1-3 on Vulnerability Handling, under development by CEN/CLC/JTC13.

The purpose of this ENISA Technical Advisory is to provide practical support to manufacturers of products with digital elements, particularly SMEs, in implementing vulnerability reporting, coordinated disclosure and security communication practices in line with the CRA's vulnerability management requirements

In particular, this package:

- explains how **security.txt** can help external parties identify where and how to report vulnerabilities;
- supports the use of **CVD** practices for receiving, assessing and managing vulnerability reports;
- provides templates for **security advisories** to communicate vulnerabilities, mitigation measures and fixes to users; and
- helps organisations translate regulatory and standards-based expectations into practical steps.

The scope of this package is limited to the practical use of documentation and processes for vulnerability reporting, coordinated disclosure and external security communication. It focuses on how organisations can publish contact information, handle incoming reports, communicate with reporters, and inform users about relevant vulnerabilities and remediation.

This package does not provide legal advice and does not replace official guidance on the CRA. It also does not cover all aspects of vulnerability management or product security, such as secure development, internal remediation workflows, incident response, or vulnerability handling by third-party suppliers. These topics remain important but are outside the main scope of this package.

Relevance under NIS2: Certain manufacturers are also subject to Directive (EU) 2022/2555 (NIS2). As a general rule, medium- and large-sized enterprises listed as types of entities in the sectors set out

in Annex I and II are in scope of the NIS2. In particular, Annex II, point (5), covers the sector “manufacturing”. As part of the cybersecurity risk-management obligation, Article 21(2)(e) NIS2 requires entities in scope to address vulnerability handling and disclosure for their own network and information systems. One security.txt file and one monitored reporting channel can serve both the CRA and NIS2. The CVD policy should, however, make clear whether a report concerns the organisation's products with digital elements notified under Article 14 CRA or its network and information systems notified under Article 23 NIS2.

DRAFT

1. security.txt, CVD policy and Security Advisory

The CRA requires manufacturers of products with digital elements to establish processes for handling vulnerabilities during the product's support period. This includes putting in place and enforcing a coordinated vulnerability disclosure (CVD) policy, providing a contact mechanism for reporting vulnerabilities, and publicly disclosing information about fixed vulnerabilities. While the regulation establishes the applicable legal obligation and the upcoming harmonised standard (prEN 40000-1-3, currently under development) is intended to provide further technical requirements and guidance, this package aims to bridge the implementation gap by providing ready-to-use artifacts that support manufacturers, notably SMEs, in addressing and remediating vulnerabilities without delay, while also facilitating the future application of the harmonised standard.

Content	Why needed
security.txt	Practical means to provide the contact address for reporting vulnerabilities (CRA Annex I, Part II, point (6)) and to make the single point of contact easily identifiable (Article 13(17) CRA). Its publication is recommended by the draft prEN 40000-1-3. This document provides additional information, including the available fields.
Coordinated vulnerability disclosure (CVD) Policy	CRA Annex I, Part II on vulnerability handling requirements specifies that manufacturers shall put in place and enforce a policy that allows anyone to report vulnerabilities securely
Security advisory	CRA Annex I, Part II on vulnerability handling requirements requires manufacturers to share and publicly disclose information about fixed vulnerabilities, enabling users to know what was fixed and to take action if needed.

1.1 security.txt

A security.txt provides a standardised way for organisations to publish security contact information, making it easier for security researchers to report vulnerabilities. Defined in RFC 9116, it supports vulnerability reporting by providing a discoverable point of contact and links to relevant vulnerability disclosure policies where applicable. Section 4.1 of this document provides a ready-to-deploy security.txt template. To adapt and deploy the template:

- Copy the ready to deploy file provided, replace the placeholders with your real contact details and policy URL. Include the PGP key link only if a key has been set up.
- Use stable, role-based contact addresses and URLs (for example security@yourdomain.example and /security). The single point of contact also has to be stated in the information and instructions to the user (Annex II, point 2 CRA) and should remain valid for the lifetime of the product.

- Upload it to <https://yourdomain.example/.well-known/security.txt> and keep in mind that the `/well-known/` path is mandatory, not optional.
- Set the Expires field no more than 12 months out, and put a reminder in your calendar to renew it.

1.2 CVD policy

A Coordinated Vulnerability Disclosure (CVD) policy explains how an organisation receives, assesses and manages vulnerability reports from security researchers and other external parties. It sets out how to report a vulnerability, what reporters can expect from the organisation, and how information will be communicated throughout the disclosure process. Section 4.2. provides a ready-to-deploy CVD policy template. To adapt and deploy the template:

- Replace every bracketed placeholder: company name, in-scope products, contact email, and the response-time figures (defaults are provided; tighten or loosen based on your engineering capacity).
- Confirm the scope list matches your actual product range, including firmware/software versions still supported.
- Publish the finished policy on your website, and link to it from your security.txt file.
- Assign one named policy owner and at least one deputy, use a shared, role-based mailbox rather than a personal one, and set a calendar reminder for the annual review.
- Ensure the policy is implemented in practice through the necessary internal processes and responsibilities. Publication alone is not sufficient.

1.3 Security advisory

A security advisory informs users about a security vulnerability affecting a product, its potential impact, and the steps they can take to reduce the risk. It helps manufacturers communicate relevant security information clearly and promptly, including available fixes, updates or mitigation measures.

Unlike the other two artefacts, the advisory template is not customised once, it is reused every time a vulnerability is fixed and disclosed. There is nothing to fill in ahead of time beyond confirming the format works for your team. Each individual advisory is filled in at the point of disclosure using the fields in Section 4.3:

- Agree internally who is responsible for publishing an advisory once a fix is released.
- Decide how affected customers will be informed. Where customers are known, inform them directly, for example via a customer portal, service channels or direct notification. Where they are not known, publish advisories on a dedicated page of your website. In both cases, maintain a public index of all published advisories. The chosen channel should be suitable, taking into account the effort and the risk associated with the product.
- Use the customised and agreed template (for generic template see Section 4.3) for every resolved vulnerability going forward.

2. Common mistakes

A few simple mistakes can make vulnerability reporting and handling less effective. The following table highlights common problems SMEs may encounter when setting up security.txt, handling vulnerability reports and communicating security issues to customers, together with practical ways to avoid them.

Common mistake	What can go wrong?	How to avoid it
security.txt¹		
File in the wrong location	Researchers cannot find the file.	Publish it at /.well-known/security.txt.
File cannot be accessed	A login, CAPTCHA or firewall blocks access.	Make sure the file is publicly accessible.
Incorrect format or missing fields	Tools may not read the file correctly, or it may not meet RFC 9116 requirements.	Use plain text, UTF-8 encoding, and valid Contact and Expires fields.
Broken links or HTTPS errors	Researchers cannot access the file or follow its links.	Test the file and links using HTTPS.
Expired or incorrect contact details	Reports may never reach the right person.	Use a monitored contact address and update the file regularly.
Unclear or broken policy link	Researchers do not know how to report vulnerabilities or what systems are covered.	Link to a clear, accessible vulnerability disclosure policy.
No assigned owner	The file becomes outdated or reports go unanswered.	Assign someone to maintain the file and monitor reports.
Assuming the file is enough	Reports arrive, but the organisation does not know how to handle them.	Establish a process for assessing, fixing and tracking vulnerabilities.
Coordinated Vulnerability Disclosure (CVD)		
No clear reporting channel	Researchers do not know where to report a vulnerability.	Provide a clear, monitored reporting channel.
No acknowledgement	Researchers do not know whether their report was received.	Acknowledge reports and explain the next steps.
No assigned responsibility	Reports are missed or left unresolved.	Assign responsibility for managing each report, with a backup if possible.
No prioritisation	Serious vulnerabilities may not be addressed quickly enough.	Assess severity and potential impact, and prioritise accordingly.

¹ <https://www.rfc-editor.org/rfc/rfc9116.html>

No coordination with the reporter	Vulnerability details may be disclosed before users can protect themselves.	Keep the reporter informed and agree on a reasonable disclosure timeline.
No remediation process	Vulnerabilities are reported but remain unfixed.	Assign responsibility for investigating, fixing and verifying the issue.
No records or follow-up	Actions and deadlines are forgotten, and reports remain open.	Track reports, decisions, actions and their status.
Report not checked for active exploitation	The early warning within 24 hours under Article 14 CRA is missed.	Check every incoming report for signs of active exploitation and define who submits the notification via the Single Reporting Platform.
Vulnerability in a third-party component not reported to the supplier	The supplier is not informed and the fix is delayed.	Forward the report to the manufacturer or maintainer of the component, following its CVD policy where available (Article 13(6) CRA).
Security Advisories		
Unclear vulnerability description	Users do not understand the issue or its potential impact.	Explain the vulnerability in clear, simple language.
Affected versions not identified	Users cannot tell whether their product is affected.	List affected and, where known, unaffected versions.
No severity or impact information	Users cannot judge how urgently they need to act.	Explain the impact and indicate severity where appropriate.
No fix or mitigation instructions	Users know about the issue but cannot protect themselves.	Provide update instructions or a workaround if no fix is available.
Broken links or missing contact details	Users cannot find the fix or ask for help.	Include working links to updates and a contact for questions.
Advisory not updated	Users may rely on outdated information or remediation advice.	Update the advisory when new information or fixes become available.
Too much technical jargon	Users may misunderstand the issue or ignore the warning.	Use plain language and explain technical terms where necessary.
Premature or delayed publication	Early disclosure may increase risk, while delays can leave users unprotected.	Coordinate publication to give affected users timely, actionable information.

3. Good practices and templates

3.1 security.txt implementation guide

Publishing a security.txt file is a recommended practice that enables security researchers to quickly identify how to report vulnerabilities to an organisation. This simple text file, published on your website and containing the relevant security contact information, provides security researchers from around the world with a standardised way to find the appropriate reporting channel. This helps reduce delays in vulnerability reporting by ensuring that valuable time is not lost trying to find the appropriate communication channel.

Even with its simple implementation, the adoption of security.txt remains limited. Recent measurements by the German Federal Office for Information Security² (BSI) and the French public data platform³ (datagouv) found valid files on only a small proportion of surveyed websites, highlighting a clear opportunity for wider uptake.

While the draft prEN 40000-1-3 recommends publishing a security.txt file, it does not delve into detail about what belongs in it. security.txt is actually a formal IETF standard in its own right - RFC 9116⁴, so the field list already exists; it needs to be filled in and be hosted correctly.

3.1.1 Where it must live

Host the file at exactly this path on your primary domain (and on every domain associated with the in-scope product, e.g. a cloud companion app):

[<https://yourdomain.example/.well-known/security.txt>]

Note: Do not put it at /security.txt only - RFC 9116 requires the /.well-known/ path. A copy may also be made available at the site root, but the file should at least be made available at /.well-known/security.txt, as defined in RFC 9116.

Products with an embedded web server, such as an HMI or an edge device, should direct users and security researchers to the manufacturer's vulnerability disclosure information. Where appropriate, the device's web interface or product documentation can provide a link to the manufacturer's security.txt file or vulnerability disclosure policy. If a separate security.txt file is published for the device's own web interface, its scope and contact details should be clear and kept up to date.

² https://www.bsi.bund.de/DE/Service-Navi/Presse/Pressemitteilungen/Presse2026/260806_security_txt.html

³ <https://www.data.gouv.fr/datasets/fichiers-security-txt-rfc-9116-sur-3-581-domaines-dorganismes-publics-francais-aout-2026>

⁴ <https://www.rfc-editor.org/info/rfc9116/#section-2.6>

3.1.2 Hosting requirements

Requirement	What it means
Must be at /.well-known/security.txt	The security.txt file must be hosted at /.well-known/security.txt in accordance with Request for Comments (RFC) 9116 and Request for Comments (RFC) 8615. If compatibility with older tools is required, a copy may also be made available at the website root (/security.txt); however, this location should redirect to /.well-known/security.txt rather than hosting an independent version of the file.
If both locations exist, /.well-known/ wins	When both the root location and the /.well-known/ location are available, the version hosted under /.well-known/ is considered authoritative. Maintaining separate copies is therefore discouraged, as inconsistencies may occur if one file is updated while the other is not. Implementing a redirect from the root location to /.well-known/security.txt ensures that only a single authoritative version is maintained.
Must be served over Hypertext Transfer Protocol Secure (HTTPS)	The security.txt file must be served over Hypertext Transfer Protocol Secure (HTTPS). Delivery over unencrypted Hypertext Transfer Protocol (HTTP) is not in line with RFC 9116.
Must be served with Content-Type: text/plain; charset=utf-8	The security.txt file must be delivered with the Hypertext Transfer Protocol (HTTP) response header Content-Type: text/plain; charset=utf-8. This requirement is frequently overlooked because some hosting providers automatically assign an incorrect content type to plain text files. Verification of the hosting configuration is therefore recommended rather than assuming the correct content type has been applied during upload. Once deployed, the configuration can be validated by running <code>curl -I https://yourdomain.example/.well-known/security.txt</code> and confirming that the response includes Content-Type: text/plain; charset=utf-8.
Redirects are allowed but scrutinised	Redirects are permitted when accessing the security.txt file or any resources referenced within it, such as the security policy page or, where one has been published, a PGP public key. However, because redirects can introduce additional trust and security considerations, it is considered best practice to host the security.txt file and any referenced resources on infrastructure under the organisation's control. Contact and encryption links are also recommended to point directly to trusted resources rather than using third-party Uniform Resource Locator (URL) shortening services or unrelated domains, which may reduce trust and introduce unnecessary security concerns.

3.1.3 Field-by-field template

Field	Required? ⁵	Purpose
Contact	Mandatory	How to reach you - email, phone, or a contact-page URL. You can list several; the first one listed is your preferred method, so put your best option first.
Expires	Mandatory	A "use-by" date for the file. Prevents a forgotten, stale file from quietly sending researchers to a dead inbox. Keep it under 12 months out and put a renewal reminder in your calendar.
Encryption	Optional, but recommended if Contact is an email	A link to your PGP key, if you have one. Do not paste the key itself there.
Policy	Optional, valuable	A link to your full CVD policy, so researchers can understand your process before reporting anything.
Canonical	Optional	The canonical URL for this exact file. Without it, someone who finds a copy hosted somewhere unusual cannot tell if it is legitimate or tampered with.
Acknowledgments	Optional	Link to a credits page thanking researchers by name: a real incentive to report to you rather than post publicly.
Preferred-Languages	Optional	Languages in which you can handle reports, for example en, de.

RFC 9116 recommends digitally signing the security.txt file using an OpenPGP cleartext signature. However, digital signing is not mandatory and requires additional key management and signature verification considerations. SMEs should assess whether they have the necessary capabilities to implement and maintain signing correctly. Where these capabilities are not available, priority should be given to publishing an accurate, accessible and regularly maintained security.txt file in accordance with RFC 9116.

3.1.4 Ready-to-deploy file

Copy the block below into a plain-text file named security.txt (no .txt.txt, no BOM (byte order mark), Unix line endings), replace the placeholders, and upload it to /.well-known/ on your web server. Remove any optional fields that are not used by your organisation, including the Encryption line if no PGP key has been set up.

```
Contact: mailto:security@yourdomain.example
Contact: https://yourdomain.example/security/report
Encryption: https://yourdomain.example/.well-known/pgp-key.asc
Expires: 2027-07-27T00:00:00.000Z
Acknowledgments: https://yourdomain.example/security/hall-of-fame
Policy: https://yourdomain.example/security/disclosure-policy
Preferred-Languages: en, [add others]
Canonical: https://yourdomain.example/.well-known/security.txt
```

⁵ The terms **Mandatory** and **Optional** refer to the requirements defined in **RFC 9116** and do not indicate any legal obligation.

Note: Set Expires to no more than 12 months out⁶ and put a calendar reminder to renew it. An expired file signals to scanners and researchers that the contact details may be stale.

3.2 Coordinated Vulnerability Disclosure (CVD) Policy

This section provides a ready to use CVD policy template that organisations can adapt to establish and communicate their vulnerability disclosure practices. The template should be tailored to the organisation's products, reporting channels and vulnerability handling processes before publication.

3.2.1 Template

Organisation: *[Company legal name]*
Effective date: *[DD/MM/YYYY]*
Version: *[1.0]*

1. Introduction and our commitment

At *[Company Name]*, we take the security of our products seriously. We encourage security researchers, customers, and anyone who discovers a potential security issue to report it to us. We are committed to reviewing all reports, working with the reporter where needed, and resolving confirmed vulnerabilities as quickly as possible. We also aim to communicate openly throughout the process while protecting our customers and supporting responsible disclosure. This policy outlines how security researchers and other third parties can report vulnerabilities to us responsibly, what they can expect from us in return, and the rules we asked to be followed while conducting the research.

2. Scope

In scope: *[product names, models and firmware or software versions within their declared support period / domains covered]*

Reports concerning products outside their support period are also welcome.

Not authorised under this policy: testing of third-party systems, services or infrastructure not owned or controlled by *[Company name]*, as well as physical attacks, social engineering of our staff.

If you identify a potential vulnerability affecting our product through a third-party component, we encourage you to report it to us. We will forward vulnerabilities in third-party components to the respective manufacturer or maintainer and may involve them in the coordination.

3. How to report

Please report a potential vulnerability using one of the contact mechanisms below. Our preferred reporting channel is *[email / web form / other]*.

Please not disclose the issue publicly until we have had a chance to review and respond. If your report includes sensitive information, such as working exploit code, you may encrypt it using the encryption method referenced in our security.txt file. Encryption is not required to submit a vulnerability report.

Email: *[security@yourdomain.example]*

Web form: *[link to form, if available]*

Tel: *[contact number, if available]*

⁶ Recommendation of the RFC

4. Rules for responsible testing

When investigating potential vulnerabilities, please observe the following rules:

- Only perform tests that are necessary to demonstrate a vulnerability,
- do not access data that does not belong to you,
- do not modify, delete, or exfiltrate data,
- avoid impairing our systems and services,
- do not conduct denial-of-service tests,
- do not exploit identified vulnerabilities beyond what is necessary for verification purposes,
- if you unintentionally gain access to data belonging to others, please inform us immediately,
- do not publicly disclose details of the vulnerability until this has been coordinated with us.

5. Required information

To help us review your report as quickly as possible please include the following information:

Field	Description
Voluntary contact details	Name, affiliation (optional), email or other contact details
Vulnerability type	CWE or OWASP category if applicable (optional)
Affected asset	Product, software or service name; model or type; hardware revision; firmware or software version; affected version range; serial number range where relevant; configuration and network exposure. For web applications and online services, include the URL or service name.
Technical description	Clear, detailed description of the vulnerability
Steps to reproduce	Step-by-step reproduction procedure
Proof of concept	Screenshots, HTTP requests/responses, scripts, or logs (ZIP max [x MB])
Discovery date & IP	Date and time of discovery and, where relevant, IP address(es) used during research
Potential impact	Your assessment of exploitability and impact
Suggested remediation	Optional, appreciated but not required

Unless it is strictly necessary, please do not transmit sensitive third-party data. If sensitive data is involved, please describe the issue in a way that minimises the amount of data shared.

6. What to expect

Communication with the reporter will be done using the submitted contact details unless another channel is agreed. Each report will be assigned a unique tracking identifier, which will be used in subsequent communications about the vulnerability. Additional information may be requested during triage and remediation, and status updates will be provided as per the timelines below. Where coordination with third parties is needed, this will be handled in accordance with the 'coordinated disclosure timeline' and 'data protection and confidentiality' sections below.

Milestone	Commitment
Acknowledgement of receipt	Within [x days] ⁷
Initial triage and severity assessment	Within [x days]
Status update, even if unresolved	At least every [x days/weeks] until case closed
Mitigation released OR deadline reached	Within [x days] ⁸

7. Safe harbour/Legal notice

[Company Name] will not pursue legal action against researchers who act in good-faith and make an effort to comply with this policy: testing only in-scope targets, not accessing, modifying or deleting others' data, not degrading service availability, and reporting through the channel above rather than exploiting or disclosing the issue first. We consider activity conducted in accordance with this policy to be authorised.

We consider activity conducted in accordance with this policy to be authorised.

This statement only applies within the scope of our own decision-making authority. It does not release from any statutory obligations or the rights of third parties.

8. Coordinated disclosure timeline

We follow a coordinated disclosure model with a default embargo window of [x] calendar days from acknowledged receipt. Public disclosure takes place after a fix or mitigation is available and, where justified, after users have had a reasonable opportunity to apply it. In that case, we will inform users of the planned date of public disclosure. We are willing to extend the embargo window by mutual agreement where remediation is genuinely complex. During this period, the parties are expected not to disclose technical details publicly, except as agreed for coordination or remediation purposes.

We may share relevant information on a need-to-know basis with affected suppliers, service providers, maintainers, coordinators, CSIRTs or competent authorities where necessary to investigate, remediate, or manage the risk. Where appropriate, such sharing will be subject to confidentiality requirements.

At the time of public disclosure, security advisories and remediation information will be published through [Company Name]'s designated security advisory channel(s), including [website/advisory page/platform/feed], and made available to affected users.

We ask that details of a vulnerability are not made public without prior coordination with us. Allow us a reasonable period of time to remediate before any public disclosure.

As a general guideline the following applies:

- Critical vulnerabilities: coordinated disclosure after remediation or in accordance with an agreement with the reporting person ,
- other vulnerabilities: disclosure generally no earlier than [x] days after remediation,
- if a vulnerability is being actively exploited or poses a significant risk, an accelerated process may be required,

⁷ The notification period should reflect organisational capacity and any relevant requirements; e.g. draft prEN 40000-1-3 sets a maximum of 7 calendar days for the acknowledgement of receipt

⁸ The remediation timeframe should take into account the product type, the nature and severity of the vulnerability, and the time reasonably required to develop and deploy a mitigation or fix. Any adjustments to the target timeframe should be communicated to the reporter.

- Where additional time is required, the reasons will be explained to the reporting person and an appropriate timeline coordinated.

9. Recognition

With the reporter's consent, we credit researchers by name or pseudonym (at their discretion) or handle in our security advisories once the issue is resolved and disclosed.

Unless expressly agreed otherwise, there is no entitlement to compensation, rewards or inclusion in a Hall of Fame.

10. Data protection and confidentiality

[Company name] will treat all reporter information as strictly confidential. Reporter details will not be shared with third parties except where required by applicable Union or national law. Personal data submitted as part of a vulnerability report will be processed in accordance with applicable data protection legislation. Vulnerability related information may be shared with relevant parties where necessary, as described in the 'coordinated disclosure timeline' section.

Please only submit personal data that is necessary for processing the report.

3.2.2 Implementation notes

- Publish the CVD policy in an accessible format, for example as an accessible web page that can be read and navigated using assistive technologies.
- In the "How to report" section, include one or more contact mechanisms that can be used to report vulnerabilities. These may include a dedicated email address, web form, ticketing portal, telephone number, or another suitable reporting channel. Where possible, provide options that are accessible through more than one sensory channel.
- Check every incoming report for indications of active exploitation. Where the manufacturer becomes aware of an actively exploited vulnerability in its product, it has to notify the CSIRT designated as coordinator and ENISA via the Single Reporting Platform, starting with an early warning within 24 hours, and inform the impacted users (Article 14 CRA). Define in advance who assesses this and who submits the notification.
- Target times in the policy are examples and have to be realistic for the product. For machinery and other OT products, a fix may require revalidation, including of safety functions, and can often only be installed during planned maintenance. Where a fix takes longer than the policy target times, provide a mitigation or supporting measures first (see Commission FAQ on the CRA, question 4.3.1). CVSS describes severity, not the risk in a specific operating environment.
- The safe harbour statement can only authorise testing of the manufacturer's own systems and waive the manufacturer's own claims. It cannot authorise testing of systems owned by third parties and cannot exclude liability for activities beyond its scope. The legal situation differs between Member States. Reporters and manufacturers both carry responsibilities in a disclosure process.

3.3 Security advisory

The following template provides a clear and consistent format for publishing security advisories for resolved vulnerabilities. It is designed to help organisations communicate key information to customers and other stakeholders in an accessible and transparent way, while supporting coordinated disclosure and maintaining a public record of published advisories.

3.3.1 Template

[Company Name] Security Advisory [YYYY-NNN] – [Vulnerability title]

Identifiers: *[CVE-YYYY-NNNN / EUVD-YYYY-NNNNN / other identifiers, where applicable]*

Severity: *[Critical/High/Medium/Low]* **CVSS:** *[version, score and vector]*

Safety impact (optional): *[description]*

Published: *[date]* **Last update:** *[date, if applicable]* **Intended audience:** *[e.g. end users, operators, integrators, service partners]*

1. Affected products/versions

[product name, model/product identifier, affected version(s)]

Fixed version(s): *[version(s) in which the vulnerability is fixed]*

Not affected (optional): *[related products or versions that customers typically ask about]*

Third-party component (if applicable): *[affected component and reference to the supplier's advisory or to the updated component version]*

2. Summary

[Plain-language description of the vulnerability and its potential impact - avoid exploit-enabling detail before customers have had time to patch.]

3. Remediation

Fix: *[Fixed in version X.Y.Z, available from ... / firmware update instructions]*

Supporting measures: *[Temporary measures to reduce risk while a fix is being developed or deployed, such as network segmentation, disabling remote access or applying firewall rules. These measures should not be considered a substitute for providing a fix where required.]*

3.1. Timeline

- Reported: *[date]*
- Acknowledged: *[date]*
- Fix released: *[date]*
- Disclosed: *[date]*
- Updated: *[date and summary of the change, if applicable]*

3.2. Credit

[Reported by NAME/handle, credited with their consent or "Reported anonymously" / "Identified internally".]

Contact: *[contact information]*

3.3.2 Implementation notes

- Publish a security advisory for each resolved vulnerability once the coordinated disclosure date has been reached. Maintain a publicly accessible index of all published advisories, as this provides a clear record of your vulnerability disclosure activities and supports evidence of ongoing compliance.
- Distinguish two cases. Information about fixed vulnerabilities is published once a security update is available, with the option to delay publication in duly justified cases until users have had the possibility to apply the patch (Annex I, Part II, point (4) CRA). Where a vulnerability is actively exploited, impacted users have to be informed in accordance with Article 14(8) CRA, if necessary before a fix is available, for example with supporting measures.
- Publish the security advisories in an accessible format, for example as an accessible web page that can be read and navigated using assistive technologies.
- In addition to a human-readable advisory, organisations should also publish advisories in a machine-readable format such as CSAF⁹ and make them available through automated distribution feeds, where feasible. Article 14(8) CRA asks for user information, where appropriate, in a structured, machine-readable format. CSAF is standardised as ISO/IEC 20153:2025, and its VEX profile allows publishing statements that a product is not affected. Organisations that do not want to operate their own CSAF infrastructure can use publication services offered by coordinators or sector CERTs, where available.

⁹ <https://www.csaf.io/>

Bibliography / References

1. **Bundesamt für Sicherheit in der Informationstechnik (BSI)**, Nur 1,8 Prozent der Webseitenbetreiber nutzen security.txt – BSI und ACS raten zur Umsetzung, 2026: https://www.bsi.bund.de/DE/Service-Navi/Presse/Pressemitteilungen/Presse2026/260806_security_txt.html
2. **Bundesamt für Sicherheit in der Informationstechnik (BSI) and Allianz für Cyber-Sicherheit (ACS)**, security.txt – Eine Kontaktmöglichkeit für Schwachstellenmeldungen, 2026: https://www.allianz-fuer-cybersicherheit.de/SharedDocs/Downloads/Webs/ACS/DE/Flyer_security_txt.pdf?__blob=publicationFile&v=5
3. **csaf.io**, Common Security Advisory Framework, <https://www.csaf.io/>
4. **CERT-FR / Agence nationale de la sécurité des systèmes d'information (ANSSI)**, Signalements du CERT-FR: <https://cert.ssi.gouv.fr/signalements/>
5. **data.gouv.fr**, Fichiers security.txt (RFC 9116) sur 3 581 domaines d'organismes publics français (août 2026), 2026: <https://www.data.gouv.fr/datasets/fichiers-security-txt-rfc-9116-sur-3-581-domaines-dorganismes-publics-francais-aout-2026>
6. **Github**, Github Advisory Database, <https://github.com/advisories>
7. **securitytxt.org**, security.txt – A proposed standard which allows websites to define security policies: <https://securitytxt.org/>
8. <https://www.rfc-editor.org/rfc/rfc9116.html>
9. **ISO/IEC 20153:2025**, Information technology, OASIS Common Security Advisory Framework (CSAF) v2.0 Specification
10. **European Commission**, C(2026) 5252 final, Commission guidance on the application of Regulation (EU) 2024/2847 (Cyber Resilience Act), 2026
11. **European Commission**, FAQs on the Cyber Resilience Act, version 1.4

Annex:

A.1 How this package supports CRA obligations

Regulation (EU) 2024/2847, Annex I, Part II sets out eight vulnerability-handling requirements for products with digital elements. The templates provided in this package support the implementation of these requirements but do not fulfil the corresponding obligations on their own. The associated processes must also be put into practice. The table below goes through all of the requirements, including ones that are not supported by this package.

CRA Annex I, Part II requirement (summarised)	Supported by
(1) Identify and document vulnerabilities and components (e.g. a software bill of materials)	Not supported by this package
(2) Address and remediate vulnerabilities without delay, including by providing security updates, where technically feasible separately from functionality updates	CVD Policy template: establishes response-time and remediation targets and a structured process for handling reported vulnerabilities. These processes must then be implemented and followed to ensure vulnerabilities are assessed and remediated without undue delay.
(3) Apply effective and regular testing and review of the product's security	Not supported by this package. An internal engineering process, not a public facing artefact
(4) Publicly disclose information about fixed vulnerabilities	CVD Policy template: supports coordination of disclosure security advisory template: provides a consistent structure for communicating fixed vulnerabilities and remediation information. Manufacturers must still prepare and publish the relevant advisories when a vulnerability is fixed and a security update is made available.
(5) Establish and enforce a coordinated vulnerability disclosure policy	CVD Policy template: supports putting a documented policy in place. Manufacturers must customise the policy, and establish internal responsibilities, processes, and resources needed to enforce and operate the policy.
(6) Facilitate the sharing of information about potential vulnerabilities in the product and in third-party components contained in it, including providing a contact address	security.txt and CVD Policy: provide clear and discoverable channels for reporting vulnerabilities. Manufacturers must ensure that these channels remain available, up to date, and actively monitored so that reports can be received and acted upon.
(7) Provide mechanisms for secure distribution of updates	Not supported by this package: depends on update delivery infrastructure
(8) Disseminate security updates without delay and free of charge, accompanied by advisory messages	Partly supported by the security advisory template, which provides a structure for the advisory messages accompanying security updates. Dissemination without delay and free of charge not supported by this package.

Relation to the draft prEN 40000-1-3

- The security.txt guidance implements the publication of a security.txt file recommended by the draft.
- The CVD policy template covers the elements the draft requires for a CVD policy, namely contact mechanisms, expectations on communication including acknowledgement, response and update time frames, conditions for sharing information with third parties, coordination of public disclosure including embargo periods, report content expectations, scope, publication practices and recognition of reporters.
- The security advisory template covers the advisory content required by the draft, including identifiers, affected products, impact, severity, remediation, guidance on actions and contact information. The draft also recommends publication in a machine-readable format such as CSAF.

DRAFT

ABOUT ENISA

The European Union Agency for Cybersecurity, ENISA, is the Union's agency dedicated to achieving a high common level of cybersecurity across Europe. Established in 2004 and strengthened by the EU Cybersecurity Act, the European Union Agency for Cybersecurity contributes to EU cyber policy, enhances the trustworthiness of ICT products, services and processes with cybersecurity certification schemes, cooperates with Member States and EU bodies, and helps Europe prepare for the cyber challenges of tomorrow. Through knowledge sharing, capacity building and awareness raising, the Agency works together with its key stakeholders to strengthen trust in the connected economy, to boost resilience of the Union's infrastructure, and, ultimately, to keep Europe's society and citizens digitally secure. More information about ENISA and its work can be found here: www.enisa.europa.eu.

ENISA

European Union Agency for Cybersecurity

Athens Office

Agamemnonos 14
Chalandri 15231, Attiki, Greece

Brussels Office

Rue de la Loi 107
1049 Brussels, Belgium

enisa.europa.eu



Publications Office
of the European Union