ETSI TR 103 XXX V 0.0.5 (2021-08)

CYBER;
Guide to Coordinated Vulnerability Disclosure

Reference
DTR/CYBER-0062

Keywords
cybersecurity, vulnerability disclosure

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

Contents

Intellectual Property Rights

Essential patents

IPRs essential or potentially essential to normative deliverables may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (https://ipr.etsi.org/).

Pursuant to the ETSI IPR Policy, no investigation, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Trademarks

The present document may include trademarks and/or tradenames which are asserted and/or registered by their owners. ETSI claims no ownership of these except for any which are indicated as being the property of ETSI, and conveys no right to use or reproduce any trademark and/or tradename. Mention of those trademarks in the present document does not constitute an endorsement by ETSI of products, services or organizations associated with those trademarks.

Foreword

This Technical Report (TR) has been produced by ETSI Technical Committee Cyber Security (CYBER).

Modal verbs terminology

In the present document "**shall**", "**shall not**", "**should**", "**should not**", "**may**", "**need not**", "**will**", "**will not**", "**can**" and "**cannot**" are to be interpreted as described in clause 3.2 of the ETSI Drafting Rules (Verbal forms for the expression of provisions).

"**must**" and "**must not**" are **NOT** allowed in ETSI deliverables except when used in direct citation.

Introduction

Security vulnerabilities are frequently discovered and, when they are, the finders of these vulnerabilities want to be able to report them directly to the organisation who can fix the issue. These vulnerability reports provide an organisation with valuable information, which it can use to improve the security of its products and services. It is therefore in the best interest of an organisation to encourage vulnerability disclosure.

Having a clearly sign-posted disclosure process demonstrates that an organisation takes security seriously. By providing such a process, organisations receive the information to address the vulnerability and to reduce the risk of compromise. This process also reduces the potential for reputational damage; by providing a way to report, and a defined policy of how the organisation will respond, the vulnerability is responsibly managed and not publicly disclosed until it is fixed.

1 Scope

This technical report is for companies and organisations of all sizes who want to implement a vulnerability disclosure process. It is not intended to be a comprehensive guide to creating and implementing a vulnerability disclosure process, but instead focuses on the essential steps.

The report contains an example vulnerability disclosure policy, a defined triage process and generic advice on how to respond to and manage a vulnerability disclosure.

This work is complementary to EN ISO/IEC 29147 [i.1], ETSI's own CVD process and can be used to support EN 303 645 Cyber Security for Consumer Internet of Things: Baseline Requirements.

2 References

2.1 Normative references

Normative references are not applicable in the present document.

2.2 Informative references

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

NOTE: While any hyperlinks included in this clause were valid at the time of publication, ETSI cannot guarantee their long term validity.

The following referenced documents are not necessary for the application of the present document but they assist the user with regard to a particular subject area.

[i.1] EN ISO/IEC 29147 Information technology - Security techniques - Vulnerability disclosure

[i.2] EN ISO/IEC 30111 Information technology - Security techniques - Vulnerability handling processes

[i.3] draft-foudil-securitytxt: "A File Format to Aid in Security Vulnerability Disclosure", E. Foudil and Y. Shafranovich, IETF, 2021.

[i.4] CVSS 3.0 User Guide, FIRST, https://www.first.org/cvss/v3.0/user-guide.

[i.5] NIST National Vulnerability Database, Common Vulnerability Scoring System Calculator, https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator.

[i.6] OASIS Common Security Advisory Framework, https://oasis-open.github.io/csaf-documentation/

[i.7] Request CVE ID, MITRE, https://cve.mitre.org/cve/request_id.html

3 Definition of terms, symbols and abbreviations

3.1 Terms

For the purposes of the present document, the following terms apply.

exploit: code that takes advantage of one or many vulnerabilities

finder: person who discovers and reports a vulnerability in a system, product or service

payload: malicious deliverable, delivered by the exploit

EXAMPLE: A keylogger is a malicious deliverable.

vulnerability: security defect or bug in a system, product or service

vulnerability disclosure process: course of action in which a finder tells the relevant entity of a vulnerability

NOTE: The vulnerability disclosure process is only part of the vulnerability management process.

vulnerability management process: course of action in which an organisation addresses and remediates a disclosed vulnerability

3.2 Symbols

Void.

3.3 Abbreviations

For the purposes of the present document, the following abbreviations apply:

CVD	Coordinated Vulnerability Disclosure
CVE	Common Vulnerabilities and Exposures
CWE	Common Weakness Enumeration

4 Introduction

4.1 Importance of establishing a vulnerability disclosure process

Security plays a crucial role in the development and lifecycle of systems, products and services. At any time in the lifecycle, a vulnerability can be found that weakens the security if left unaddressed. If a vulnerability is found in development, this can be addressed before the product is released. Often, however, vulnerabilities are found after a system, product or service has been deployed. In this case, it can be difficult for the finder to know how or where to report the vulnerability.

An organisation should have a vulnerability disclosure process. There are many reasons good reasons to do so:

1. A vulnerability disclosure process helps an organisation to respond most effectively to a security vulnerability.
2. By providing a clear process, organisations can receive the information directly so the vulnerability can be addressed, and any associated risk reduced.
3. Vulnerability reports can provide organisations with valuable information that can be used to improve the security of systems, products and services.
4. The presence of a vulnerability disclosure process demonstrates that an organisation takes security seriously.
5. By accepting and receiving vulnerability reports, organisations will reduce the number of vulnerabilities in their systems, products or services.
6. It allows organisations to engage constructively with finders. This engagement means can give valuable information that would otherwise be missed, or require additional time and effort to discover.

By contrast, if an organisation does not provide a vulnerability disclosure route, finders who discover vulnerabilities can resort to public disclosure of the information. This public release can result in reputational damage and can lead to a compromise.

4.2 The vulnerability disclosure process

The vulnerability disclosure process should allow a finder to report a security vulnerability easily. A vulnerability disclosure process should be easy to find.

Internally, the organisation should have clear communication and escalation paths to ensure that the vulnerability information remains protected but gets to those whom can address and resolve it.

A vulnerability disclosure process should:

- enable the disclosure of vulnerabilities, and
- be clear, simple and secure, and
- define how the organisation will respond.

4.3 How to use this document

This document describes the essential components in creating and implementing a vulnerability disclosure process. It is intended as the basis for an organisation's vulnerability disclosure process and to align with the organisation's vulnerability management process.

NOTE: Implementing a vulnerability disclosure process and receiving the vulnerability is only the beginning of the vulnerability management process.

5 Guidance on implementation

5.1 General

An organisation's vulnerability disclosure process should be clear and simple to use. Submissions of vulnerability reports can be undertaken in a range of ways, including a secure web form on an organisation's website or using a dedicated vulnerability disclosure platform.

Regardless of process used, the process should be easy to find. There should be an easy to find page on an organisation's website that clearly states both its vulnerability disclosure policy and where to report the vulnerability to. Using a standard name and location is a key part in ensuring the process is easily found and understood.

EXAMPLE: An organisation includes a 'Vulnerability Disclosure' section on the 'Contact Us' web page on its website. It also publishes a security.txt file [i.3] containing the information.

Organisational staff, especially those who manage external communications, should be made aware of the vulnerability disclosure process.

5.2 Vulnerability disclosure policy

By providing a clear policy, organisations define what they expect from someone disclosing a vulnerability, as well as what they will do in response. This enables the organisation and the finder to confidently work within an agreed framework.

EN ISO/IEC 29147 [i.1] defines the minimum requirements for a vulnerability disclosure policy. In its basic form, a vulnerability disclosure policy should contain all of the following information:

- how an organisation wants to be contacted
- secure communication options

EXAMPLE: a secure web form

- what information the finder can include in the report
- what the finder can expect to happen

- guidance on what is in and out of scope

An example of a basic vulnerability disclosure policy comprising these elements is given in clause 6.1 of the present document.

5.3 How to receive a vulnerability report

5.3.1 General

A secure web form should be used for a finder to report a vulnerability. A web form is the easiest way to report a vulnerability and so it is preferred by finders. A web form is a structured way to ensure all the required information is provided.

The secure web form should allow for anonymous vulnerability reports. An incentive may be given for a finder to provide contact details.

Each report should be automatically assigned a unique reference number to allow both finder and organisation to track the ticket.

5.3.2 Vulnerability disclosure template

This section details the standard information that should be submitted in a vulnerability report. Text in brackets is for information only and may be excluded.

Vulnerability Details (Mandatory)

Asset (web address, IP, product or service name)

Weakness (such as a CWE) (optional)

Severity (this can be calculated via CVSS v3.0 [i.4] [i.5]) (optional)

Title of vulnerability (mandatory)

Description of vulnerability (mandatory), including all of the following:

- a summary of the vulnerability
- steps to reproduce the vulnerability
- supporting files
- possible mitigations or recommendations

Impact (what could an attacker do?) (mandatory)

Contact Details (Optional)

Name

Email Address

5.4 security.txt

One of the most important elements of a vulnerability disclosure process is that it can be found when needed. Security.txt [i.3] is a draft IETF Internet standard that describes a text file that holds details of the vulnerability disclosure process, which webmasters can host in the "/.well-known" directory of the domain root. The purpose of security.txt is to advertise the organisation's vulnerability disclosure process so that someone can quickly find all of the information needed to report a vulnerability.

The security.txt file contains two mandatory fields:

- CONTACT: How finders report vulnerabilities, such as by email or secure web form.
- POLICY: A link to the organisation's vulnerability disclosure policy.

The ENCRYPTION field is optional. If the ENCRYPTION field is used, it should link to the PGP public key that an organisation wants to be used for encrypted communication.

The security.txt file should be published to all of the domains and subdomains of an organisation, in the standard location of /.well-known/security.txt

EXAMPLE 1: A security.txt file that only applies to example.com would be found at the location:
https://example.com/.well-known/security.txt

EXAMPLE 2: A security.txt file that only applies to subdomain.example.com would be found at the location:
https://subdomain.example.com/.well-known/security.txt

5.5 Responding to a vulnerability disclosure

5.5.1 Communication and response

Without a vulnerability disclosure process, an organisation can receive unsolicited messages from a finder detailing a vulnerability. But even if an organisation does have a process in place, good communication is important in ensuring a positive vulnerability disclosure experience. This clause contains some guidance for organisations that can help to ensure good communication and maintain a positive relationship with the finder.

1. An organisation should not ignore the report. An organisation should respond promptly to the finder and should thank them for their report. At this early stage, an organisation should reiterate its vulnerability disclosure process as detailed in its published policy.

EXAMPLE: An organisation responds quickly to a vulnerability report to thank the finder and reminds the finder of the policy's stated triage time. This feedback promotes trust and encourages engagement, making a finder more inclined to help an organisation again in the future.

2. An organisation should not force the finder to sign documents such as non-disclosure agreements. This is because the individual is simply looking to ensure the vulnerability is fixed.
3. The process should escalate the report to the correct party in your organisation who is responsible for the affected product or service. This party should perform triage (see clause 5.5.2) on the report to establish if the vulnerability does exist and if so, what its severity and impact is.
4. If more information is needed to confirm and remediate the issue, an organisation should politely request that additional information from the finder.
5. Once triage is complete, an organisation should promptly inform the finder to let them know that the issue is being managed. An organisation need not provide technical information or commit to timescales.
6. If the issue takes a significant amount of time to remediate, the organisation should send periodic updates back to the finder, such as fortnightly.
7. Once the issue is remediated, the organisation should let the finder know. The finder may retest the issue to confirm the fix.
8. The organisation should consider publicly acknowledging and thanking the finder, as this creates a sense of trust and transparency.

5.5.2 Triage

Triage is an important function for the success of a vulnerability disclosure process. Triage ensures that there is an assessment of the report, its severity and likely impact to the organisation. It avoids rushed or incorrect responses to a vulnerability disclosure. The information found as a result of triage (severity and impact) should be used to assign a priority to remediating the vulnerability.

The triage process may be performed by an in-house team, or may be outsourced. In both cases, it should be undertaken by technical staff who understand security vulnerabilities and how they can impact the specific organisation.

Adequate care should be taken and security protections in place when working with proof-of-concept code in the triage stage.

EXAMPLE: A team uses a sandboxed environment for executing proof-of-concept code and testing against a representative, non-live system.

The triage process should comprise the following four stages:

1. Understanding

   The triage team should understand the technology used, the application and the purpose of the product or service being tested and the organisation's strategic aims. Together, these can be used to assess the business impact.

2. Criticality

   The triage team should assess the criticality of the vulnerability. Assessing the criticality means assessing the impact on Confidentiality, Integrity and Availability. Standard ways include assigning a CVSS score [i.4] [i.5]. This should also take into consideration how easy the vulnerability could be exploited by an attacker.

3. Communications

   Ensuring effective communications with the finder is important for an effective triage process (see clause 5.5.1). The triage function should be undertaken in the stated timeframe and status updates should be provided promptly to the finder.

4. Report Status

   A vulnerability report should be marked in one of the following states, which describes where the ticket is in the process:

   - New: The report has not yet been triaged.
   - Triaged: The report has been triaged and assessed as a valid vulnerability.
   - Open: The report has been passed to the relevant team for remediation.
   - Closed:
     - Duplicate: The report is the same as another report. This status should be annotated with the ticket number of the original.
     - Remediated: The report has been remediated. The finder may re-test to ensure the fix is complete.
     - N/A: The report is spam, not going to be fixed, out of scope, or not a security vulnerability.

5.5.3 Acknowledging the finder

Once the reported vulnerability has been remediated, an organisation should consider acknowledging the finder. Acknowledgement may be included in the public advisory (see clause 5.5.4). However, if there is no public advisory, acknowledgment may be provided in other ways, such as:

- Named in a 'hall of fame' web page on the organisation's website
- A letter of appreciation
- Merchandise, such as a challenge coin or company-branded gift.

Before public acknowledgement, the organisation should consult the finder to ensure that the finder is happy with the content of the acknowledgement, and that they would like to be publicly acknowledged.

If the vulnerability disclosure process is outsourced to a dedicated vulnerability disclosure platform, they may acknowledge the finder through awarding a different number of points depending on how the report has been triaged.

EXAMPLE: A valid report receives more points that a duplicate report and out of scope reports can remove points.

5.5.4 Public Advisory

Once the reported vulnerability has been remediated, an organisation should consider creating a public advisory. A public advisory ensures that customers and stakeholders are aware of the vulnerability and the associated risks, and have the requisite remediation advice.

The advisory should include accurate information to allow the reader to understand the impact of the vulnerability and how it might affect systems they are responsible for. It should not include detailed technical information that would make exploiting the vulnerability easier, such as proof-of-concept code .

The advisory should include the date it was originally published and the date of the latest revision. Changes to the advisory should be highlighted to ensure the reader can easily see what has changed, especially if this changes the impact or mitigations.

The advisory should include all of the following information:

- Description
- Impact
- Exploitability (how easy is the vulnerability to exploit)
- Remediation/mitigation
- Acknowledgement of the finder (if they wish to be credited)

As well as a text-based advisory, an organisation may provide a machine-readable version.

EXAMPLE: A machine-readable advisory can be created using the OASIS Common Security Advisory Framework (CSAF) [i.6].

In parallel to creating a public advisory, an organisation may request the assignment of a CVE ID [i.7], though creating a CVE ID in isolation is not the appropriate mechanism for publicly disclosing vulnerabilities (see clause 5.5.5).

5.5.5 Requesting a CVE ID

The mission of the Common Vulnerabilities and Exposures (CVE) programme is to identify, define, and catalogue publicly disclosed vulnerabilities. A CVE identifier (ID) is the de facto standard for uniquely and naming publicly disclosed vulnerabilities pertaining to specific versions of software or codebases. This allows someone to refer to a CVE ID and know they are talking about a specific, unique vulnerability.

Once a vulnerability has been received by the organisation, they may request the assignment of a CVE ID via a CVE Naming Authority. This process verifies whether the issue has already been reported or if another CVE ID has already been assigned for the issue.

NOTE: CVE is a dictionary of publicly disclosed vulnerabilities that uses publicly disclosed vulnerability information as its source of information. Therefore, a CVE ID is not the appropriate mechanism for publicly disclosing vulnerabilities.

5.6 Vulnerability Management

Typically a vulnerability disclosure process is implemented once the product or service is already live. However, the most effective vulnerability disclosure process forms part of a wider vulnerability management framework. New products and services should be designed with vulnerability disclosure and vulnerability management as an integrated part of their lifecycle.

Vulnerability management is a process that enables an organisation to know what vulnerabilities are present within their organisation, products or services on a regular basis. This process should include all of the following steps:

1. Identification: includes secure development lifecycle, vulnerability scans, penetration testing and vulnerability disclosure

2. Assessment: includes triage, severity and priority
3. Mitigation: steps to remediate the vulnerability
4. Feedback and improvement to remove root causes.

A vulnerability disclosure process forms part of the identification stage and can provide a reporting process for tactical security issues. The triage and assessment process ensures that vulnerability reports are addressed in severity and priority order. However, without vulnerability management, an organisation can expend vast resources simply fixing reported security vulnerabilities and not addressing the underlying causes of the security issues.

Each vulnerability is triaged and assessed in the same way to ensure a consistent severity and priority. This ensures that organisations stop focusing on isolated security fixes. An organisation should have a process to understand the root causes of their vulnerabilities; this allows them to take steps to mitigate against those causes across the organisation, product or service portfolio.

5.6.1 Third Party Suppliers

A vulnerability can be reported in a third party product or service. In this case, it is important to establish as much information as possible from the finder, such as any CVEs assigned to the vulnerability. This will help to ensure the correct mitigation is put in place. If the vulnerability was previously not known, then information detailing the specific vulnerability should be disclosed to the third party.

A vulnerability can be reported on a system managed by a third party. In this case, the service level agreement should include who covers the costs of mitigation and in what timeframe will the mitigation be applied.

6 Examples

6.1 Example Vulnerability Disclosure Policy

Introduction

(Add an introduction to your organisation.)

This vulnerability disclosure policy applies to any vulnerabilities you are considering reporting to us (the "Organisation"). We recommend reading this vulnerability disclosure policy fully before you report a vulnerability and always acting in compliance with it.

We value those who take the time and effort to report security vulnerabilities according to this policy. However, we do not offer monetary rewards for vulnerability disclosures.

Reporting

If you believe you have found a security vulnerability, please submit your report to us using the following link/email:

[insert link/email]

In your report please include:

Vulnerability Details:

* Asset (web address, IP, product or service name) where the vulnerability can be observed

* Weakness (e.g. CWE) (optional)

* Severity (e.g. CVSS v3.0) (optional)

* Title of vulnerability (mandatory)

* Description of vulnerability (this should include a summary, supporting files and possible mitigations or recommendations) (mandatory)

* Impact (what could an attacker do?) (mandatory)

* Steps to reproduce. These should be a benign, non-destructive, proof of concept. This helps to ensure that the report can be triaged quickly and accurately. It also reduces the likelihood of duplicate reports, or malicious exploitation of some vulnerabilities, such as sub-domain takeovers.

Optional Contact Details:

* Name

* Email Address

What to expect

After you have submitted your report, we will respond to your report within 5 working days and aim to triage your report within 10 working days. We'll also aim to keep you informed of our progress.

Priority for remediation is assessed by looking at the impact, severity and exploit complexity. Vulnerability reports might take some time to triage or address. You are welcome to enquire on the status but should avoid doing so more than once every 14 days. This allows our teams to focus on the remediation.

We will notify you when the reported vulnerability is remediated, and you may be invited to confirm that the solution covers the vulnerability adequately.

Once your vulnerability has been resolved, we welcome requests to disclose your report. We'd like to unify guidance to affected users, so please do continue to coordinate public release with us.

Guidance

You must NOT:

* Break any applicable law or regulations.

* Access unnecessary, excessive or significant amounts of data.

* Modify data in the Organisation's systems or services.

* Use high-intensity invasive or destructive scanning tools to find vulnerabilities.

* Attempt or report any form of denial of service, e.g. overwhelming a service with a high volume of requests.

* Disrupt the Organisation's services or systems.

Annex A (informative): Authors & contributors

The following people have contributed to the present document:

Rapporteur:

Other contributors

History

Document history		
Version	Date	Description
0.0.1	Jan 2021	Initial draft
0.0.2	Mar 2021	Early draft – adding text to headings
0.0.3	May 2021	Early draft expanded to include feedback
0.0.4	July 2021	Stable draft
0.0.5	August 2021	Stable draft with editorial changes