

ETSI TR 103 838 V1.1.1 (2022-01)



TECHNICAL REPORT

**Cyber Security;
Guide to Coordinated Vulnerability Disclosure**

Reference

DTR/CYBER-0062

Keywords

cyber security, vulnerabilities

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 - APE 7112B
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° w061004871

Important notice

The present document can be downloaded from:

<http://www.etsi.org/standards-search>

The present document may be made available in electronic versions and/or in print. The content of any electronic and/or print versions of the present document shall not be modified without the prior written authorization of ETSI. In case of any existing or perceived difference in contents between such versions and/or in print, the prevailing version of an ETSI deliverable is the one made publicly available in PDF format at www.etsi.org/deliver.

Users of the present document should be aware that the document may be subject to revision or change of status.

Information on the current status of this and other ETSI documents is available at

<https://portal.etsi.org/TB/ETSIDeliverableStatus.aspx>

If you find errors in the present document, please send your comment to one of the following services:

<https://portal.etsi.org/People/CommitteeSupportStaff.aspx>

Notice of disclaimer & limitation of liability

The information provided in the present deliverable is directed solely to professionals who have the appropriate degree of experience to understand and interpret its content in accordance with generally accepted engineering or other professional standard and applicable regulations.

No recommendation as to products and services or vendors is made or should be implied.

No representation or warranty is made that this deliverable is technically accurate or sufficient or conforms to any law and/or governmental rule and/or regulation and further, no representation or warranty is made of merchantability or fitness for any particular purpose or against infringement of intellectual property rights.

In no event shall ETSI be held liable for loss of profits or any other incidental or consequential damages.

Any software contained in this deliverable is provided "AS IS" with no warranties, express or implied, including but not limited to, the warranties of merchantability, fitness for a particular purpose and non-infringement of intellectual property rights and ETSI shall not be held liable in any event for any damages whatsoever (including, without limitation, damages for loss of profits, business interruption, loss of information, or any other pecuniary loss) arising out of or related to the use of or inability to use the software.

Copyright Notification

No part may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm except as authorized by written permission of ETSI.

The content of the PDF version shall not be modified without the written authorization of ETSI.

The copyright and the foregoing restriction extend to reproduction in all media.

© ETSI 2022.
All rights reserved.

Contents

Intellectual Property Rights	4
Foreword.....	4
Modal verbs terminology.....	4
Introduction	4
1 Scope	5
2 References	5
2.1 Normative references	5
2.2 Informative references.....	5
3 Definition of terms, symbols and abbreviations.....	6
3.1 Terms.....	6
3.2 Symbols.....	6
3.3 Abbreviations	6
4 Introduction	7
4.1 Importance of establishing a vulnerability disclosure process	7
4.2 The vulnerability disclosure process	7
4.3 How to use the present document.....	7
5 Guidance on implementation.....	8
5.1 General	8
5.2 Vulnerability disclosure policy.....	8
5.3 How to receive a vulnerability report.....	8
5.3.1 General.....	8
5.3.2 Vulnerability disclosure template	9
5.4 security.txt	9
5.5 Responding to a vulnerability disclosure.....	10
5.5.1 Communication and response	10
5.5.2 Triage.....	10
5.5.3 Acknowledging the finder	11
5.5.4 Public Advisory	12
5.5.5 Requesting a CVE ID	12
5.6 Vulnerability Management.....	13
5.6.1 Process	13
5.6.2 Third Party Suppliers.....	13
6 Examples	13
6.1 Example Vulnerability Disclosure Policy	13
History	15

Intellectual Property Rights

Essential patents

IPRs essential or potentially essential to normative deliverables may have been declared to ETSI. The declarations pertaining to these essential IPRs, if any, are 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 Directives including the ETSI IPR Policy, no investigation regarding the essentiality of IPRs, 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.

DECT™, **PLUGTESTS™**, **UMTS™** and the ETSI logo are trademarks of ETSI registered for the benefit of its Members. **3GPP™** and **LTE™** are trademarks of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners. **oneM2M™** logo is a trademark of ETSI registered for the benefit of its Members and of the oneM2M Partners. **GSM®** and the GSM logo are trademarks registered and owned by the GSM Association.

Foreword

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

Modal verbs terminology

In the present document "**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 organization who can fix the issue. These vulnerability reports provide an organization 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 organization to encourage vulnerability disclosure.

Having a clearly sign-posted disclosure process demonstrates that an organization takes security seriously. By providing such a process, organizations 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 organization will respond, the vulnerability is responsibly managed and not publicly disclosed until it is fixed.

1 Scope

The present document is for companies and organizations 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 present document contains generic advice on how to respond to and manage a vulnerability disclosure, a defined triage process, advice on managing vulnerabilities in third party products or suppliers, and an example vulnerability disclosure policy.

NOTE: Organizational programs specifically intended to encourage identification and hunting for vulnerabilities, such as bug bounty, are not specifically addressed by the present document.

This work is complementary to EN ISO/IEC 29147 [i.1], ETSI's own CVD process [i.11] and can be used to support specifications including ETSI EN 303 645 [i.2].

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] ETSI EN 303 645: "CYBER; Cyber Security for Consumer Internet of Things: Baseline Requirements".
- [i.3] IETF Draft Foudil Securitytxt: "A File Format to Aid in Security Vulnerability Disclosure", E. Foudil and Y. Shafranovich, IETF, 2021.

NOTE: Available at <https://datatracker.ietf.org/doc/html/draft-foudil-securitytxt-12>.

- [i.4] MITRE Common Weakness Enumeration.

NOTE: Available at <https://cwe.mitre.org>.

- [i.5] FIRST CVSS v3.0: User Guide.

NOTE: Available at <https://www.first.org/cvss/v3.0/user-guide>.

- [i.6] NIST National Vulnerability Database, Common Vulnerability Scoring System Calculator.

NOTE: Available at <https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator>.

- [i.7] ISO 8601: "Date and time format".

NOTE: Available at <https://www.iso.org/iso-8601-date-and-time-format.html>.

[i.8] IETF RFC 3339: "Date and Time on the Internet: Timestamps".

NOTE: Available at <https://datatracker.ietf.org/doc/html/rfc3339>.

[i.9] OASIS Common Security Advisory Framework.

NOTE: Available at <https://oasis-open.github.io/csaf-documentation>.

[i.10] Request CVE ID, MITRE.

NOTE: Available at <https://www.cve.org/ResourcesSupport/ReportRequest#RequestCVEID>.

[i.11] ETSI's Coordinated Vulnerability Disclosure (CVD) process.

NOTE: Available at <https://www.etsi.org/standards/coordinated-vulnerability-disclosure?jjj=1642530129259>.

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 organization addresses and remediates a disclosed vulnerability

3.2 Symbols

Void.

3.3 Abbreviations

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

CSAF	Common Security Advisory Framework
CVD	Coordinated Vulnerability Disclosure
CVE	Common Vulnerabilities and Exposures
CVSS	Common Vulnerability Scoring System
CWE	Common Weakness Enumeration
ID	IDentifier
IETF	Internet Engineering Task Force
IP	Internet Protocol
ISO	International Organization for Standardization
N/A	Not Applicable
OASIS	Organization for the Advancement of Structured Information Standards
PGP	Pretty Good Privacy
RFC	Request For Comments

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.

To remedy this, an organization should have a vulnerability disclosure process. There are many reasons to do so:

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

By contrast, if an organization does not provide a vulnerability disclosure route, finders who discover vulnerabilities may 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 easily report a security vulnerability. A vulnerability disclosure process should also be easy to find. The process should also include vulnerabilities with third party products or suppliers (see clause 5.6.2).

Internally, the organization should have clear communication and escalation paths to ensure that the vulnerability information remains protected but gets to those who 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 organization will respond.

4.3 How to use the present document

The present document describes the essential components in creating and implementing a vulnerability disclosure process. It is intended as the basis for an organization's vulnerability disclosure process and to align with the organization'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 organization'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 organization's website or using a dedicated vulnerability disclosure platform.

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

EXAMPLE: An organization 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.

Organizational 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, organizations define what they expect from someone disclosing a vulnerability, as well as what they will do in response. This enables the organization 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 organization 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

The vulnerability disclosure policy can include guidance on the actions a finder should and should not do. This can include vulnerability classes that are deemed out of scope, for example testing for denial of service.

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. The web form can be provided as part of a commercial vulnerability disclosure platform.

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

To reduce junk or spam reports, consideration should be given to rate limiting the number of submissions allowed in a period of time, or implementing a challenge-response test.

5.3.2 Vulnerability disclosure template

This clause 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 Address, product or service name)
- Weakness (such as a CWE [i.4]) (optional)
- Severity (this can be calculated via CVSS v3.0 [i.5] [i.6]) (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 organization's vulnerability disclosure process so that someone can quickly find all of the information needed to report a vulnerability.

The security.txt file contains three important fields:

- **CONTACT:** How finders should report vulnerabilities. Ideally a link to a secure web form. If contact is via email, the Encryption field should link to the PGP public key to be used for encrypted communication.
- **EXPIRES:** Indicates the date and time after which the data contained in the "security.txt" file is considered stale and should not be used. The value of this field is formatted according to the Internet profile of ISO 8601 [i.7] as defined in IETF RFC 3339 [i.8]. It is recommended that the value of this field be less than a year into the future to avoid staleness.
- **POLICY:** A link to the organization'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 organization wants to be used for encrypted communication.

The security.txt file should be published to all of the domains and subdomains of an organization, 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 organization can receive unsolicited messages from a finder detailing a vulnerability. But even if an organization does have a process in place, good communication is important in ensuring a positive vulnerability disclosure experience. This clause contains guidance for organizations that can help to ensure good communication and maintain a positive relationship with the finder. Adequate care should be taken with any attachments and web links that may form part of the vulnerability disclosure:

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

EXAMPLE: An organization 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 organization again in the future.

- 2) An organization 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 the organization 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 organization should politely request that additional information from the finder.
- 5) Once triage is complete, an organization should promptly inform the finder to let them know that the issue is being managed. An organization need not provide technical information or commit to timescales.
- 6) If the issue takes a significant amount of time to remediate, the organization should send periodic updates back to the finder, such as fortnightly.
- 7) Once the issue is remediated, the organization should let the finder know. The finder may retest the issue to confirm the fix.
- 8) The organization 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 organization. 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 organization.

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 organization'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.5] and [i.6]. 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:

- Open:
 - New: The report has not yet been triaged.
 - Triaged: The report has been triaged and assessed as a valid vulnerability.
 - Assigned: 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.
 - Informative: The report contained useful security information but does not warrant remediation.
 - 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 organization 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 organization's website
- A letter of appreciation
- Merchandise, such as a challenge coin or company-branded gift

Before public acknowledgement, the organization 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 than a duplicate report and out of scope reports can remove points.

5.5.4 Public Advisory

Once the reported vulnerability has been remediated, an organization 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.

If the remediation removes, limits or changes functionality, this should be highlighted. Where possible, a best practice alternative solution should be provided.

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 organization may provide a machine-readable version.

EXAMPLE: A machine-readable advisory can be created using the OASIS Common Security Advisory Framework (CSAF) [i.9].

In parallel to creating a public advisory, an organization may request the assignment of a CVE ID [i.10], 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 a standard for uniquely 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 organization, 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

5.6.1 Process

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 organization to know what vulnerabilities are present within their organization, 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 organization 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 organizations stop focusing on isolated security fixes. An organization 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 organization, product or service portfolio.

5.6.2 Third Party Suppliers

A vulnerability can be reported in a third party product or service where that product or service is included as a part of the product or service covered by the vulnerability disclosure process. 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 securely 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 the mitigation will be applied.

6 Examples

6.1 Example Vulnerability Disclosure Policy

Introduction

(Add an introduction to your organization.)

This vulnerability disclosure policy applies to any vulnerabilities you are considering reporting to us (the "Organization"). 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 Address, 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 will 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 would like to unify guidance to affected users, so please do continue to coordinate public release with us.

Guidance

Do NOT:

- Break any applicable law or regulations
- Access unnecessary, excessive or significant amounts of data
- Modify data in the Organization'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 Organization's services or systems

History

Document history		
V1.1.1	January 2022	Publication