SEC Consult
an Eviden business

Responsible Disclosure Policy

SEC Consult Vulnerability Lab
An integrated part of SEC Consult, an Eviden business

Version: 3.3.1 | Date: 2023-05-23
Author: J. Greil | Responsible: J. Greil
Confidentiality Class: Public

Contents

SEC Consult Unternehmensberatung GmbH
Wagramer Straße 19 / Floor 16 | 1220 Vienna | **T** +43 (1) 890 30 43 - 0 | **F** +43 (1) 890 30 43 - 15 | **M** office@sec-consult.com | https://www.sec-consult.com
UID-Nr. ATU56165223 | FN-Nr. 227896t LG Wiener Neustadt

1 SEC Consult Vulnerability Lab

The SEC Consult Vulnerability Lab is the integrated research organization of SEC Consult, an Eviden business, one of the leading international security consultancies, with a special focus and recognized experience in application security.

Details on SEC Consult and the activities of the SEC Consult Vulnerability Lab can be found at

https://sec-consult.com/vulnerability-lab/.

For any inquiry, feedback or comments please send your email to security-research@sec-consult.com.

We recommend using email encryption for contacting us. You can use PGP for encryption of emails or documents, see Appendix for our public PGP key.

2 Introduction

2.1 Purpose of this document

During vulnerability research and security testing, e.g., penetration tests, SEC Consult regularly discovers security vulnerabilities in commercial and open-source software products. While important vulnerability information should be provided to the vendor, to the product's customers and the security community for a variety of reasons, it is equally important to minimize the risk which vulnerability disclosure poses to the affected vendors and customers.

This document aims to provide vendors with the necessary information and timeframe needed to validate and fix a security flaw to mutually coordinate the public release of a security advisory as part of the responsible disclosure process, based on [1]. This document also clarifies the extent and limitation of effort the SEC Consult Vulnerability Lab will invest.

If SEC Consult – before or during a disclosure process of a specific vulnerability – starts a direct contractual relationship with the respective vendor, the process and steps of the responsible disclosure might be changed to the specific terms and conditions of the contract with the respective vendor.

2.2 Objective of responsible disclosure

The objectives of responsible disclosure comprise:

- Improve the quality of the vendor's product in the domain of application security and trigger further improvements of the software vendor.
- Ensure that vulnerabilities can be identified and eliminated effectively and efficiently for all parties.
- Minimize the risk to customers from known vulnerabilities which could impact their systems.
- Provide customers with sufficient information for them to evaluate the level of security in a vendor's product and their assessment of the vendor's maturity in application security.
- Provide the security community with the necessary information to develop tools and methods for identifying, managing, and reducing the risks of vulnerabilities in information technology.
- Minimize the amount of time and resources required to manage vulnerability information.
- Facilitate long-term research and development of techniques, products, and processes for avoiding or mitigating vulnerabilities.

Besides other topics, the following is **not** objective of the responsible disclosure:

- Provide free of charge quality assurance for insecure products.

SEC Consult Unternehmensberatung GmbH
Wagramer Straße 19 / Floor 16 | 1220 Vienna | **T** +43 (1) 890 30 43 - 0 | **F** +43 (1) 890 30 43 - 15 | **M** office@sec-consult.com | https://www.sec-consult.com
UID-Nr. ATU56165223 | FN-Nr. 227896t LG Wiener Neustadt

3 Scope

The scope of this policy includes any technical security vulnerabilities in software or hardware products found by SEC Consult. The policy details the process of vendor notification as well as time limits and conditions for the publication of vulnerability information.

The technical and organizational processes of vulnerability resolution needed on the vendor side are beyond the scope of this document. Those are described in ISO/IEC 29147:2018 [2] and ISO/IEC 30111:2019 [3].

Software vulnerabilities are often found in dedicated projects, such as penetration tests and source code reviews for customers of SEC Consult. SEC Consult will contact the vendor with an anonymous security advisory without mentioning any customer system details.

Hence, other customers of SEC Consult and the vendor, which may have the same software deployed, will also benefit by a security patch from the vendor.

SEC Consult may suspend the responsible disclosure process under certain exceptional circumstances.

4 Responsible Disclosure Policy

The following section describes each phase of the vulnerability notification and disclosure process.

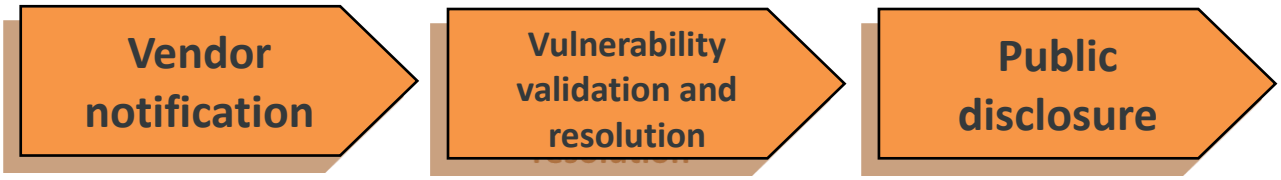

Figure 1 – Overview Responsible Disclosure Phases

4.1 Phase 1 - Vendor notification

SEC Consult notifies the vendor of the vulnerability during this phase. In turn, the vendor is expected to provide SEC Consult with an acknowledgement that the notification was received.

The steps in this phase are:

1. SEC Consult creates a security advisory after a security vulnerability has been identified. This security advisory is usually a text document containing an overview and all available details, and proof of concept material of the vulnerability. SEC Consult diligently evaluates the proof of concept and validates that the results are as accurate as possible. Furthermore, several quality assurance steps ensure an accurate and high-quality documentation of the entire disclosure process before contacting the vendor.
2. Contacting the vendor
    a. Case 1: Vendor has public security contact with encryption information online

        SEC Consult will send the encrypted security advisory information, provide this *responsible disclosure document* and *public encryption keys* to the vendor.

    b. Case 2: Vendor has no public security contact online

        SEC Consult will send an initial email to the vendor's technical support contact, or another suitable contact address found online. In this initial e-mail, the vendor is informed that a security vulnerability has been found in one of their products. *Public encryption keys* and this *responsible disclosure policy document* are provided to the vendor, but no security advisory information just yet.

        The vendor is kindly asked to provide an appropriate security contact including encryption certificates for the encrypted receipt of the security advisory.

SEC Consult Unternehmensberatung GmbH
Wagramer Straße 19 / Floor 16 | 1220 Vienna | **T** +43 (1) 890 30 43 - 0 | **F** +43 (1) 890 30 43 - 15 | **M** office@sec-consult.com | https://www.sec-consult.com
UID-Nr. ATU56165223 | FN-Nr. 227896t LG Wiener Neustadt

If no encryption certificates are provided to SEC Consult, the vendor agrees with unencrypted communication and the associated risks of plain text transmission of the advisory.

Once a security contact has been established, the security advisory is sent to the vendor.

3. The vendor is being asked to react timely upon the security advisory information and provide which further steps will be taken to fix the vulnerability.
4. If the vendor does not respond to any contact attempts or if there is no adequate response from the vendor, the security advisory will be published within the deadline mentioned in chapter 4.3.

All contact attempts are documented and included in the vendor communication section "timeline" in the final security advisory. If the vendor does not respond to any contact attempts, the vulnerability validation and resolution phase of the next chapter will be skipped.

4.2 Phase 2 - Vulnerability validation and resolution

In this phase, the vendor verifies and validates the reporter's claims. The vendor tries to identify where the flaw resides, and which components or other systems might be affected. The vendor develops a patch or workaround that eliminates or reduces the risk of the vulnerability.

1. The vendor will assess the delivered security advisory which is provided as-is with no further free-of-cost support from SEC Consult.
2. The vendor is expected to validate and reproduce the vulnerability and notify the reporter of the result. Upon validation of the vulnerability, the vendor must provide the reporter with an estimate on when the vulnerability will be fixed.
3. The vendor must provide a patch, configuration change, or workaround that appropriately reduces or eliminates the risk of the vulnerability or provide SEC Consult with specific reasons for their inaction.
4. The vendor should provide SEC Consult with update information to be included in the final security advisory. This includes the software versions or hardware revisions affected by the security issue, the number of the fixed version, and a means to obtain the update (e.g., the URL of a website where the security fix or updated version can be downloaded). We recommend the vendor to request CVE numbers for the corresponding vulnerability. If this does not happen, SEC Consult will request a CVE number.
5. The vendor should credit the researcher, who identified the security issue and the SEC Consult Vulnerability Lab within release notes / announcements, etc. made by the vendor, e.g.:
    a. "*$Vendor thanks $researcher (discovery, analysis, coordination) from the SEC Consult Vulnerability Lab (https://www.sec-consult.com) for responsibly reporting the identified issues and working with us as we addressed them.*"

SEC Consult will strictly enforce the communicated deadline of usually 50 days, but public disclosure of a security advisory may be delayed up to at most four months (beginning of the initial contact) if the vendor provides valid reasons why the issue cannot be resolved earlier, and the new patch date has been accepted by SEC Consult.

If no further agreement is reached, the mentioned deadline of usually 50 days will be used for publication.

If the vendor requires in-depth support from SEC Consult in this phase (e.g., explanations, meetings, telephone calls, email conversations, workshops, solution concepts, etc.) the vendor needs to order additional support that will be charged by SEC Consult.

SEC Consult Unternehmensberatung GmbH
Wagramer Straße 19 / Floor 16 | 1220 Vienna | **T** +43 (1) 890 30 43 - 0 | **F** +43 (1) 890 30 43 - 15 | **M** office@sec-consult.com | https://www.sec-consult.com
UID-Nr. ATU56165223 | FN-Nr. 227896t LG Wiener Neustadt

4.3 Phase 3 - Public disclosure

A security advisory is published under the following circumstances:

- In a mutually coordinated release with the vendor including proof of concept information as soon as a security update is available to the vendor's customers.
- If the vulnerability has not been resolved within **50 days** after the initial contact of SEC Consult, and no other coordinated release date has been planned or the vendor did not supply valid reasons for a delay or is unresponsive, the deadline of usually 50 days will be used for publication. The proof of concept will usually not be released, if there is no patch available, depending on the impact of the vulnerability.
- Latest four months after the initial contact made by SEC Consult, if the vendor provides valid reasons why the issue cannot be resolved within 50 days and the new patch date has been accepted by SEC Consult. If no further agreement is reached, the advisory will be prepared for public release.

SEC Consult may withhold or delay disclosure of proof-of-concept information from the public if the publication would pose a severe risk to customers, users, other companies, or public infrastructure.

SEC Consult may contact world-wide or local computer emergency response teams (CERT) during the responsible disclosure process to coordinate public disclosure in case critical vulnerabilities have been identified that affect a large user base.

4.4 Content of the Security Advisory

The final security advisory may be published via public security mailing lists, SEC Consult's website or other means of publication. The security advisory contains:

- Advisory title
- Product / Software name
- Affected / vulnerable and fixed version(s)
- Impact / criticality rating
- CVE numbers (if available)
- Vendor URL
- Date found
- Name or pseudonym of reporter
- Vendor description of the product
- Business recommendation
- Vulnerability overview/description
- Proof of concept
- Vulnerable versions and information regarding tested versions
- Vendor contact timeline
- Solution / Patch information (if available) or workaround
- Advisory URL and SEC Consult contact information

SEC Consult Unternehmensberatung GmbH
Wagramer Straße 19 / Floor 16 | 1220 Vienna | **T** +43 (1) 890 30 43 - 0 | **F** +43 (1) 890 30 43 - 15 | **M** office@sec-consult.com | https://www.sec-consult.com
UID-Nr. ATU56165223 | FN-Nr. 227896t LG Wiener Neustadt

5 Effort and cost

This document also clarifies the extent and limitation of effort the SEC Consult Vulnerability Lab will invest:

- The effort and cost for security identification and documentation before the Phase 1 "Vendor Notification" is an investment by a customer of SEC Consult and/or by the SEC Consult Vulnerability Lab. From the perspective of a vendor this is part of the quality assurance of the vendor's product which is received for free.
- The effort and cost to document the preliminary security advisory and to track the vendor responses and timeline is an investment by the SEC Consult Vulnerability Lab. This comprises the Phase 1 – "Vendor notification" and Phase 3 – "Public disclosure". From the perspective of a vendor this is part of the quality assurance of the vendor's product which is received for free.
- Any additional support exceeding the as-is provided preliminary security advisory especially in Phase 2 – "Vulnerability validation and resolution" (e.g., explanations, meetings, telephone calls, email conversations, workshops, solution concepts, etc.) may be charged by SEC Consult, if there is any in-depth support needed by the vendor.

SEC Consult Unternehmensberatung GmbH
Wagramer Straße 19 / Floor 16 | 1220 Vienna | **T** +43 (1) 890 30 43 - 0 | **F** +43 (1) 890 30 43 - 15 | **M** office@sec-consult.com | https://www.sec-consult.com
UID-Nr. ATU56165223 | FN-Nr. 227896t LG Wiener Neustadt

6 References

Parts of this policy are based on / incorporate ideas from the following documents:

[1] Internet-Draft, Responsible Vulnerability Disclosure Process, by Steve Christey (MITRE) and Chris Wysopal (@stake, Inc.), Feb. 2002, http://tools.ietf.org/html/draft-christey-wysopal-vuln-disclosure-00

[2] ISO/IEC 29147:2018, Information technology - Security techniques - Vulnerability disclosure, https://www.iso.org/standard/72311.html

[3] ISO/IEC 30111:2019, Information technology - Security techniques - Vulnerability handling processes, https://www.iso.org/standard/69725.html

SEC Consult Unternehmensberatung GmbH
Wagramer Straße 19 / Floor 16 | 1220 Vienna | **T** +43 (1) 890 30 43 - 0 | **F** +43 (1) 890 30 43 - 15 | **M** office@sec-consult.com | https://www.sec-consult.com
UID-Nr. ATU56165223 | FN-Nr. 227896t LG Wiener Neustadt

7 Appendix – Public encryption keys

Public PGP key for security-research@sec-consult.com

Fingerprint: F9A9 D4AF 3DC2 D298 8350 9025 2D2D D7B5 C6EE 883F

Expiry: 6th May 2024

```
-----BEGIN PGP PUBLIC KEY BLOCK-----

mQINBFRQ3twBEACyAcBt7jX9fHlrjUd3fH/ZYsT4XOZ+KDa7cP8gZp07O4WpgBBh
hXC6zNggZTVM0dPiAhWp6N6FYZddkeR/iHFxxhOxcFx0Vg2WFuwi1YfGZN1RTXYS
0i2AfLVH8JlBQcRc7JxhX6FRx+RyxjHmWeibG5axwMCqem5oSZbYMi3jkdLkUg3i
HQX8eMB8dYWg2cUwRlmGfuLJsN2nlLGrn7QDQN0HUJtlriQDRUwfE4wnlbgu6zU0
R4fTnRL1ltJHW1mVqX5Ov8REvVwXxwnUBOAPgOGmxIV4diIsnBzSAq5WXQW08dCY
GETcQAEWlTtzKnWbYWpTQfF59F2/dHCrdQNOliC7lBjQLrPLwi4y6MWROaXHOcVk
x5ovr0lJ61P2q1Jfh5Ie5Q1FlhwkUkLYkhKGIn4sXB59R65/jg0li4Ikmf9Dat2F
vA1TziH5O3Tr9sDWtUcinubv89O3IwDV3swR14NNzuHm1IAMM0PSWNJJxyw7b+3W
feZY26/tbJDjaD03rwjhYj7dLlZbA5wk5/C6JeWnkoh/6ss9ebk27bJKCm8vjz+p
O+YvYbe5x7X4Ol90/USecPEWHy7w4ym80Yn5Skxo7Ufwu8y6KyZD8O7KVG8hPsIT
SyIDnMqWAHJ4vtuegaAllLWm9U4cs8ra8WECXP0p7Qr0MxJlLcEjheO9NQARAQAB
tHRTRUMgQ29uc3VsdCBWdWxuZXJhYmlsaXR5IExhYiAoU0VDIENvbnN1bHQgVW50
ZXJuZWhtZW5zYmVyYXR1bmcgR21iSCB3d3cuc2VjLWNvbnN1bHQuY29tKSA8cmVz
ZWFyY2hAc2VjLWNvbnN1bHQuY29tPokCVgQTAQoAQAIbLwcLCQgHAwIBBhUIAgkK
CwQWAgMBAh4BAheAFiEE+anUrz3C0piDUJAlLS3XtcbuiD8FAmHlUxQFCRIPWEQA
CgkQLS3XtcbuiD/Q0hAAmh/vwz+UKyirs7JjdzyPNzDEwUANka4iUj23EyheNlKm
Uxn35NohVmFLsN2IlZTz5THlDl96QI+/nvVGcutOseXmHX+Lsqtm+IJkURmkMNZ9
bCsXdAW70sdZqV7lr3vkEEJI95UJghe6RyghEIPUZxupDBLZTyaNI+RKfahukDpq
cBYrkUsN9dsD5juM0Jc1PCnnz4sqMVmroXt5EvH1nkwpcZxX6EMxvZGrYaDKXRwd
4etEqqR8zpinVebfDYhD6UCa/ocZX8/4kskiKtXwUSdKuFJIEiwksUcgHpavIAhS
dEvIrynODpDLfD4cH56/yd8nvtPJHcPAIUewCpHbrl5B0x9WFIWQ9/8PaeSXnj71
+1suiyxpcmiaQmGqJpi+YYu9ZjxO/O9h9FfQpSLJCkt4uFEWmUPo8evmmkJaLRm3
bVl4HqM1VM+cF5xPf7Do47rHoaMtuzDsSfqMQPjXqbE/Qof+aA/Oa/I/JjYS7Plx
PbdaBTj8xJy9k8yZMFPhtd2Q1MOSWfuOIhn+5OCPxE+Y6+tdL2zL4SLkmBZGV9k+
1qOSKT+4moPZ8/7Pz0eZhQ0bGF0hJsrV+dppsd8kotYPT2FBbht4nuNS9S3Sfteb
grn7K9bu+fI/8tgzUzjMDbc/31DbaGRH7HFL4UM3eL252w1mlNYSEfu1CoZlLzKI
RgQQEQIABgUCVLUsHAAKCRBVAk8FmTmAqcMpAJ4gujZmcbrFKsJL5cyJTJKAicn0
SgCeJUNg2bzVPcgeN75tIBoOyVLyag60aVNFQyBDb25zdWx0IFZ1bG5lcmFiaWxp
dHkgTGFiIChhbiBBdG9zIGNvbXBhbnkgLSB3d3cuc2VjLWNvbnN1bHQuY29tKSA8
c2VjdXJpdHktcmVzZWFyY2hAc2VjLWNvbnN1bHQuY29tPokCVAQTAQoAPgIbLwUL
CQgHAgYVCgkICwIEFgIDAQIeAQIXgBYhBPmp1K89wtKYg1CQJS0t17XG7og/BQJh
5VMUBQkSD1hEAAoJEC0t17XG7og/logP/j34uxYoGS0ZYV+IAePkr1yGlOkMXH1U
5e5INQRpwOm1mLoEjDABl84VNpdNISGxilk56uasmPagwztMrnKxjDkZ/+ARjo0H
FOGHJnsFgUaOCXYf7uZwKhXXxLTPhU553knjk7LEwk/4U2ZK313mZdckQaFKeFsP
+UG4sIcnv8HGCca236J6SiEN5h3rNXrRHlEkBnpqFEWHgIcqPtQfa6OAtTpOW5Vf
ToxXw+Khk+lg603OKA3h6iiB2VJTdsl3fPBSEDuOMPl6MHIek/xrInnjOrBXqLiw
qWxAqQc/fMex7FDt8e7YecPvvDJJQE46XEKYBRZlBCCI3nn0hPPMGdLsn2hjeKaI
xswcWW60vVHyoaKeEMckkA1Hg6p9gfqdbIyr6taybD/h88/2GGQVx2RRRT0w1gIo
gvu+V/fnTbbzpSBvOufGa2QZUYI9SQt+FZS3fHBoCSMTuVW6wdIkmT3MlEuvG8GP
5SHVDod4Kq7VQi/L1CbaRMrd9TtT/k3QDzkPNN8wEhST1BS5ZfktCqGQTC7Q5H7s
OQG2WbKoWkSjqiArBPVwtqI2VsMPt8y4tT2ABGhEH2vXXKIzD/mftHQ7PflNl/Mb
Eq5HF9gJfUHx/V3YCizjEulG3l89C2nU5FFba69ccw6b7a0OwM8Imz680p5+EbaX
PHkYW+Tj24zL
=r6yh
-----END PGP PUBLIC KEY BLOCK-----
```


SEC Consult Unternehmensberatung GmbH
Wagramer Straße 19 / Floor 16 | 1220 Vienna | **T** +43 (1) 890 30 43 - 0 | **F** +43 (1) 890 30 43 - 15 | **M** office@sec-consult.com | https://www.sec-consult.com
UID-Nr. ATU56165223 | FN-Nr. 227896t LG Wiener Neustadt

8 Version History

Version	Date	Status/Changes	Created by	Responsible
1.0	29.08.2008	Final version	B. Müller	B. Müller
1.2	31.3.2011	Updated version with amendments on effort sharing and refined process.	J. Greil	M. Eiszner
1.3	05.02.2013	Minor changes (logo, PGP key, formatting, …)	J. Greil	J. Greil
2.0	07.03.2014	Major updates regarding disclosure procedure	J. Greil	J. Greil
2.0.1	29.10.2014	New PGP key	J. Greil	J. Greil
3.0	2016-11-23	New layout, minor adjustments, additional references, added S/MIME fingerprint	J. Greil	J. Greil
3.0.1	2017-11-23	Updated S/MIME fingerprint	J. Greil	J. Greil
3.0.2	2019-09-02	Updated PGP key expiry date, SEC Consult address	J. Greil	J. Greil
3.0.3	2020-02-19	Updated S/MIME fingerprint	J. Greil	J. Greil
3.1	2021-02-15	Update PGP key expiry date, Atos logo	J. Greil	J. Greil
3.2	2023-03-07	Adjusted wording regarding deadlines, PGP key expiry update, contact information	J. Greil	J. Greil
3.3	2023-05-15	Further adjusted wording, address, new SEC Consult / Eviden logo	J. Greil	J. Greil
3.3.1	2023-05-23	Minor updates	J. Greil	J. Greil

SEC Consult Unternehmensberatung GmbH
Wagramer Straße 19 / Floor 16 | 1220 Vienna | **T** +43 (1) 890 30 43 - 0 | **F** +43 (1) 890 30 43 - 15 | **M** office@sec-consult.com | https://www.sec-consult.com
UID-Nr. ATU56165223 | FN-Nr. 227896t LG Wiener Neustadt