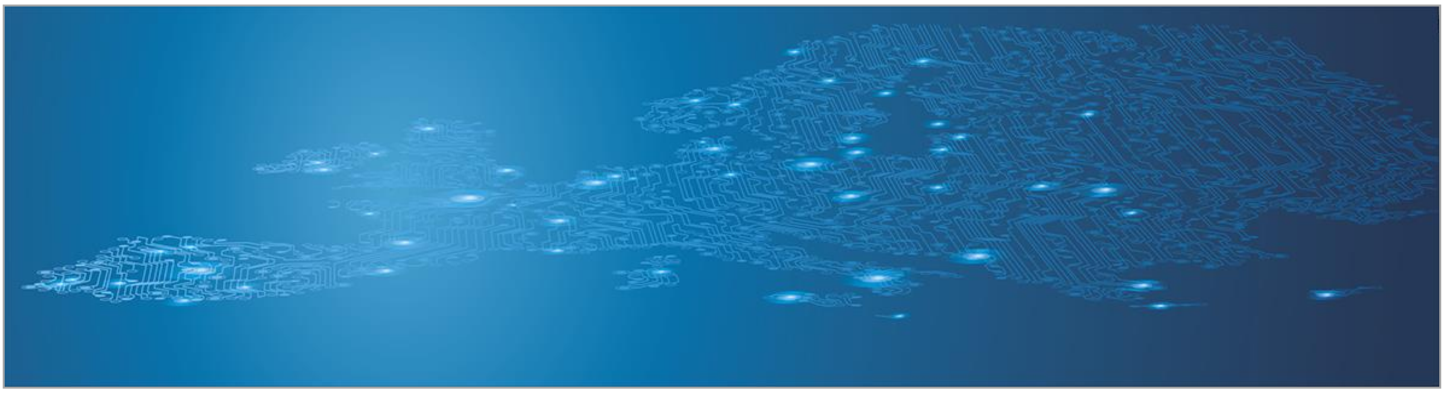

Vulnerability Handling

Toolset, Document for students

September 2014

European Union Agency for Network and Information Security

www.enisa.europa.eu

About ENISA

The European Union Agency for Network and Information Security (ENISA) is a centre of network and information security expertise for the EU, its member states, the private sector and Europe's citizens. ENISA works with these groups to develop advice and recommendations on good practice in information security. It assists EU member states in implementing relevant EU legislation and works to improve the resilience of Europe's critical information infrastructure and networks. ENISA seeks to enhance existing expertise in EU member states by supporting the development of cross-border communities committed to improving network and information security throughout the EU. More information about ENISA and its work can be found at www.enisa.europa.eu.

Acknowledgements

Contributors to this report

We would like to thank all our ENISA colleagues who contributed with their input to this report and supervised its completion, especially Lauri Palkmets, Cosmin Ciobanu, Andreas Sfakianakis, Romain Bourgue, and Yonas Leguesse. We would also like to thank the team of Don Stikvoort and Michael Potter from S-CURE, The Netherlands, Mirosław Maj and Tomasz Chlebowski from ComCERT, Poland, and Mirko Wollenberg from PRESECURE Consulting, Germany, who produced the second version of this documents as consultants.

Agreements or Acknowledgements

ENISA wants to thank all institutions and persons who contributed to this document. A special 'Thank You' goes to the following contributors: Anna Felkner, Tomasz Grudzicki, Przemysław Jaroszewski, Piotr Kijewski, Mirosław Maj, Marcin Mielniczek, Elżbieta Nowicka, Cezary Rzewuski, Krzysztof Silicki, Rafał Tarłowski from NASK/CERT Polska, who produced the first version of this document as consultants and the countless people who reviewed this document.

Contact

For contacting the authors please use CERT-Relations@enisa.europa.eu

For media enquires about this paper, please use press@enisa.europa.eu**.**

Legal notice

Notice must be taken that this publication represents the views and interpretations of the authors and editors, unless stated otherwise. This publication should not be construed to be a legal action of ENISA or the ENISA bodies unless adopted pursuant to the Regulation (EU) No 526/2013. This publication does not necessarily represent state-of the-art and ENISA may update it from time to time.

Third-party sources are quoted as appropriate. ENISA is not responsible for the content of the external sources including external websites referenced in this publication.

This publication is intended for information purposes only. It must be accessible free of charge. 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.

Copyright Notice

Table of Contents

1 What Will You Learn 1

2 Exercise Task 1

2.1 Task 1 Incident Handling – Incident Analysis 1

2.2 Further 3-5 services 1

1 What Will You Learn

The objective of this exercise is to give you a practical overview of the vulnerability handling process and how vulnerabilities reported to a CERT team should be handled. You will learn:

- What the main responsibilities of a CERT team involved in a vulnerability case are;
- How to design a vulnerability disclosure policy suitable for your CERT; and
- How to deal with difficult situations that may arise through your role as a coordinator.

2 Exercise Task

2.1 Task 1 Responsibilities of a CERT team in a vulnerability case

You will hear a description of a typical vulnerability case. Your task is to identify the CERT's main responsibilities and activities in handling the reported vulnerability.

- Think about the responsibilities which the CERT has as coordinator towards the vendor and the reporter of the vulnerability.
- Name the actions that CERT has to take to resolve the case.

Keep in mind that the CERT team always acts as an independent coordination centre.

2.2 Task 2 Vulnerability disclosure

The vulnerability handling process always involves the problem of disclosing information about the vulnerability. What is your opinion on vulnerability disclosure? Do you think this information should be kept secret or publicly disclosed? Think about the advantages and disadvantages of disclosing a vulnerability.

2.3 Task 3 Designing a vulnerability disclosure policy

Now you have some ideas as to what responsible vulnerability disclosure should be. What main aspects should be addressed in a vulnerability disclosure policy? Develop a general policy for your CERT.

2.4 Task 4 Role-playing game: Introducing CERT coordination in a vulnerability case

The trainer will tell you two stories. One will be a true story from the past, based on the Michael Lynn case: http://en.wikipedia.org/wiki/Michael_Lynn. The second one is a scenario which will be used in the game.

The rules of the role-playing game:

- The trainer is the game leader.
- A game leader has an absolute power to shape, modify and adjust a game scenario; i.e.:
  - he can stop an action and introduce new factors and new conditions;
  - he can rewind an action to change factors or conditions or actions already performed; and
  - he can accelerate an action to avoid valueless activities.

- All students must fit their actions to what the trainer decides.
- Students can communicate during a role-playing game only as players, not as students (e.g., they are not allowed to comment on an action, unless the trainer changes it).
- A main purpose of the trainer is to achieve the goals of the exercise.

2.5 Task 5 Identification of vulnerability handling phases

During this post role-playing activity, students are given the task of identifying as many activities and processes as possible. This is achieved by a kind of brain-storming session with the trainer as the group leader.

2.6 Task 6 Coordination of a single and multiple vendor case

During the game in the previous task, you dealt with a single vendor case. It may happen, however, that a reported vulnerability affects more than one vendor. Think about the possible complications in a multiple vendor case. The trainer will give you some tips on the aspects you should consider especially carefully.

ENISA
European Union Agency for Network and Information Security
Science and Technology Park of Crete (ITE)
Vassilika Vouton, 700 13, Heraklion, Greece

Athens Office
1 Vass. Sofias & Meg. Alexandrou
Marousi 151 24, Athens, Greece

PO Box 1309, 710 01 Heraklion, Greece
Tel: +30 28 14 40 9710
info@enisa.europa.eu
www.enisa.europa.eu