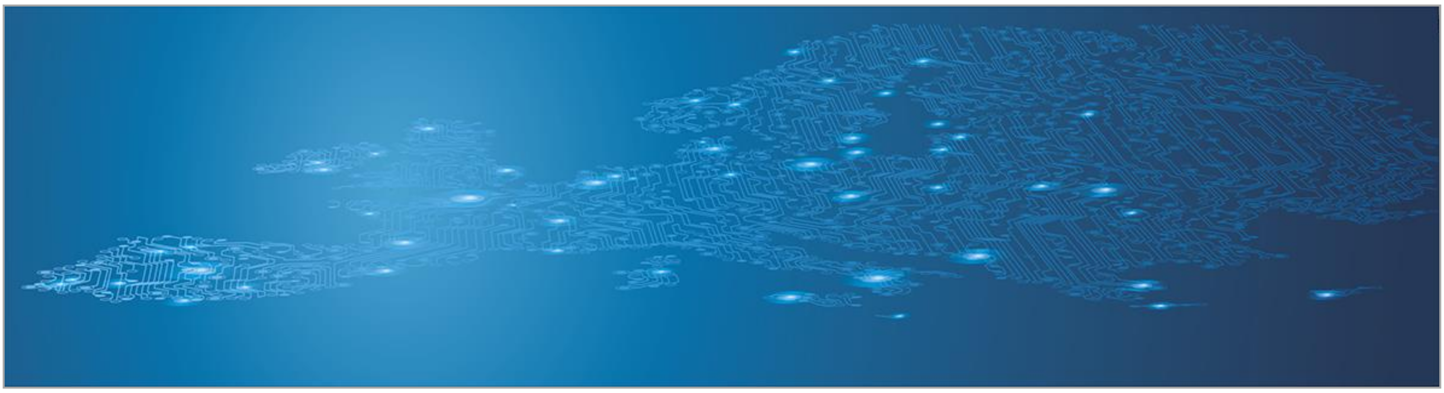

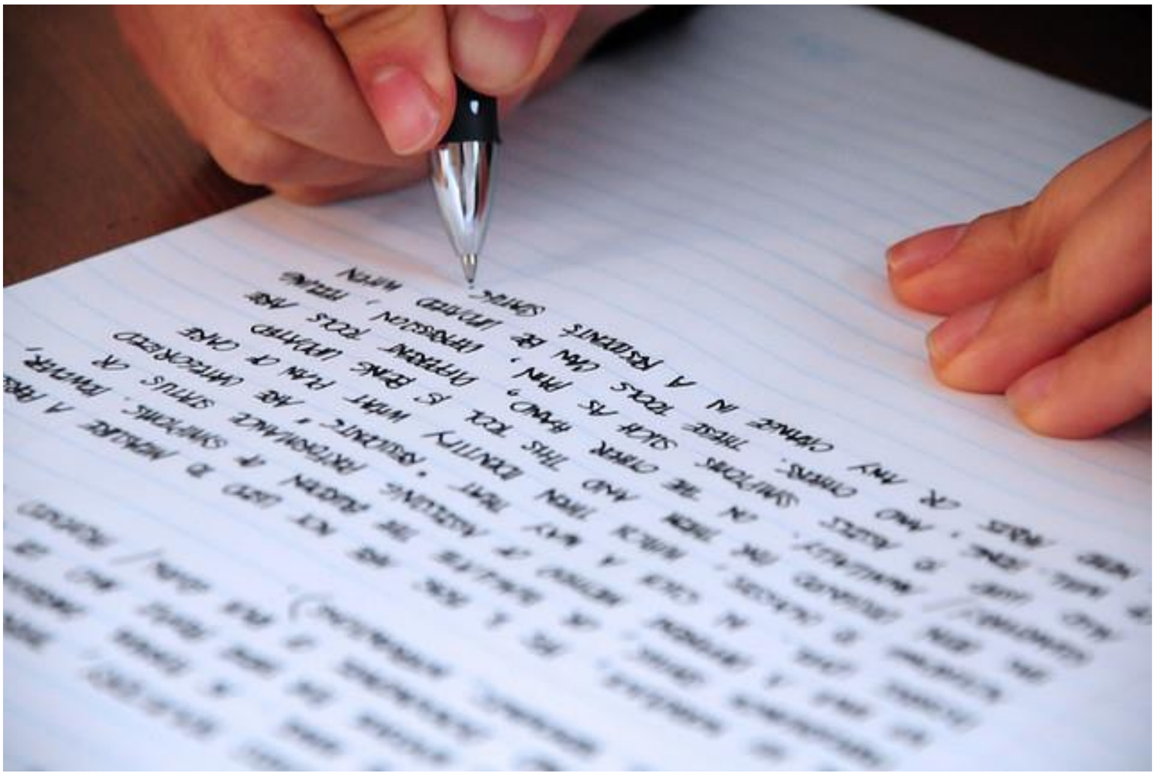

Writing Security Advisories

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

During this exercise you will learn how to write a good security advisory publication for your constituency. In particular, you will:

- learn how to create your own template for security advisories;
- learn how to judge whether an advisory is well written and can be referenced as a source;
- gain an understanding of the specifics of your constituency and its influence on the content of security advisories; and
- learn the basics of CVSS..

2 Exercise Task

2.1 PART 1 KEY POINTS IN AN ADVISORY

The trainer will give you a brief introduction about security advisories. Listen carefully, as you will have to participate actively.

2.1.1 Task 1 Identifying key points in an advisory

You will be asked what you think are the key points required in an advisory. List as many points as you can. The trainer will present a real advisory. What points do you think were missing?

2.1.2 Task 2 Example step-by-step advisory comparison

Listen to the trainer as he leads you through a comparison of two different advisories. Which structure of the advisories did you like better? What were the strengths and weaknesses of both advisories?

2.1.3 Task 3 Advisory comparison

Perform an analysis on your own, comparing a much larger set of advisories covering the same topic. This is a DNS vulnerability advisory - CVE-2008-1447. Attached below, you will find a checklist which will aid you. Fill it in with comments. These comments could include ratings, such as POOR or GOOD, PRESENT or ABSENT, or more elaborate statements if necessary The trainer can give it to you in the form of a printout you can use. All the advisories being discussed and compared are on the CERT Exercises Virtual Image or can be found on the Internet.

The advisories are listed below

- US-CERT (Technical Cyber Security Alert): http://www.us-cert.gov/cas/techalerts/TA08-190B.html
- US-CERT (Vulnerability Note): http://www.kb.cert.org/vuls/id/800113
- NVD NIST: http://nvd.nist.gov/nvd.cfm?cvename=CVE-2008-1447
- SecurityFocus: http://www.securityfocus.com/bid/30131
- Secunia: http://secunia.com/advisories/cve_reference/CVE-2008-1447/
- Microsoft: http://www.microsoft.com/technet/security/Bulletin/MS08-037.mspx
- ISC (BIND): http://www.isc.org/sw/bind/bind-security.php

Document	US-CERT (TCSA)	US-CERT (TCSA)	US-CERT (TCSA)	US-CERT (TCSA)	US-CERT (TCSA)	US-CERT (TCSA)	US-CERT (TCSA)
Problem Name and ID							
Threat severity and Impact							
Affected systems							
Description							
Possible remedies (solutions, workarounds, patch locations)							
References							
Revision notes							
Other fields: digital signatures, contact information?							
How informative?							
Structure of the documents?							
Additional comments							

DNS CVE-2008-1447 Checklist:

2.2 PART 2: CVSS TRAINING

This part of the exercise is devoted to learning the basics of CVSS.

2.2.1 Task 1 CVSS basics and tools

Listen carefully to the introduction to CVSS by the trainer. Click through the available CVSS calculators – you will need to use them for the next tasks.

2.2.2 Task 2 CVSS vectors and metrics of the DNS CVE-2008-1447 vulnerability

Together with the trainer, you will calculate CVSS scores for the DNS CVE-2008-1447 vulnerability.

2.2.3 Task 3 Calculating CVSS scores by yourself

In this task, students will be split into smaller groups. Your group should create a short description of an organization and its network. Next, pick a security vulnerability found in an advisory and calculate its CVSS scores. The trainer may introduce different variants of this exercise.

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