6. Exercise: Writing Security Advisories

Main Objective	The objective of the exercise is to provide a practical overview of what constitutes a good and a bad advisory publication for a CERT constituency.	
Targeted Audience	Technical and management CERT staff	
Total Duration	About 4 hours	
Time Schedule	Introduction to the exercise	10 min.
	PART 1	
	Task 1: Identifying key points in an advisory	30 min.
	Task 2: Step-by-step comparison of real advisories	30 min.
	Task 3: Comparison of real security advisories by students	60 min.
	PART 2	
	Task 1: CVSS basics and tools	30 min.
	Task 2: CVSS vectors and metrics of the DNS CVE-2008-1447 vulnerability	30 min.
	Task 3: Calculation of CVSS scores by students themselves	30 min.
	Summary of the exercise	15 min.
Frequency	This exercise should be carried out when the CERT is first set up or new members who are responsible for writing security advisories join the team.	

6.1 GENERAL DESCRIPTION

The objective of the exercise is to provide a practical overview of what constitutes a good and a bad advisory publication for a CERT constituency. After completion of the exercise, the students will:

- Understand how to write good security advisories;
- Understand the specifics of their constituency and its influence on the content of security advisories;
- Be able to create their own template for security advisories;
- Have learned how to judge the severity level of an advisory; and

- Have learned the basics of CVSS.

Before carrying out this exercise, read this handbook carefully. The handbook lists specific advisories that have been published by real organizations in the past – CERTs, vendors, etc. You are encouraged to become familiar with them. You can also add new advisories to the exercise.

To fully carry out the exercise, you will need to give students access to the CERT Exercise Book Virtual Image. Students should be asked to boot their laptops from this DVD and select this exercise, which will contain instructions on how to proceed. The DVD will contain all the examples of the advisories mentioned in this exercise. A short presentation as an introduction would be beneficial. For the comparison of real advisories carried out by the students themselves, it is advisable that you provide each student with a printout of the checklist. Students should have paper and pencils. A whiteboard would be useful. CVSS training sessions require access to the Virtual Image or the Internet.

6.2 EXERCISE COURSE

The course of this exercise is as follows:

6.2.1 Introduction to the exercise

As the trainer, you are expected to give a general introduction on the topic of writing security advisories. You should be familiar with the list of sources shown in the references. Your introduction should describe the topics that may be covered by security advisories and how the development process could work. You should cover the following aspects of writing advisories:

- CERTs are usually not the initial sources of information regarding a security vulnerability. These sources are primarily software vendors, security vendors and various researchers. To provide accurate information about what is going on, it is recommended that the information from various sources be aggregated. This will allow for a better picture of the actual situation. Furthermore, effort should be made to get information from the original reporter, as this tends to be both the most detailed and the most accurate.
- When a vulnerability or other threat is first disclosed, there is usually some confusion as to the details of the problem. The understanding of the problem changes over time and this is something that should be reflected in the procedure for creating the security advisory.
- If a CERT has the capability to perform their own analysis of the problem (for example, disassembly of an actual malware or testing of a vulnerability), this would further improve the quality of the advisory.
- CERTs have constituencies which can vary in character. It is important that the persons responsible for writing advisories understand the specific character of their constituency. For example, a Windows only group will probably not be very interested

in new UNIX or Mac flaws - sounding the alarm for such problems would not be very useful and could be counter-productive as future advisories may be ignored.

- Various standardization schemes for writing (and exchanging) security advisories have been proposed. However, none of these have gained common acceptance. The reasons probably include complexity, lack of a drive to implement software solutions that enable automation, and different classification schemes.

6.3 PART 1 KEY POINTS IN AN ADVISORY

6.3.1 Task 1 Identifying key points in an advisory

Ask each student to make a list of key points they would expect to find in a good security advisory that concerns a vulnerability or a major threat. The students should cross-check these lists among themselves and arrive at an agreed list. Once consensus has been reached on a list, you should ask one of the students to present it. These key points are expected to cover most of the fields that should be present in some form in a real advisory, along with a short description: PROBLEM NAME AND ID, SEVERITY, AFFECTED PLATFORMS, IMPACT, DESCRIPTION, WORKAROUND, SOLUTION, SOFTWARE UPDATES, URLS WHERE THE ADVISORY CAN BE FOUND, REVISION NOTES, CREDITS, CONTACT/DIGITAL SIGNATURE, ALSO KNOWN AS, etc.

After this discussion, take a real advisory as an example and analyse it according to the introduction above. A suitable example might be the CERT CA-2001-19 (http://www.cert.org/advisories/CA-2001-19.html) advisory which describes the Code Red worm which was very active in 2001 and exploited vulnerability in the MS IIS Server buffer overflow. Below is an example of an analysis which may be carried out:

All CERT advisories have a similar structure that stays constant. First of all, every advisory has its unique ID. The ID consists of the letters CA (from CERT Advisory), the year of publication and the number of the advisory published in the year. The advisory we analysed was the 19th document in 2001. Clear document identification makes it possible for the advisory to be referred to.

The next section contains the dates of first release and last update. The last update date is very important, as this helps check if the document is up to date compared to another one covering the same issue.

Then comes one of the key parts of the advisory: the list of systems affected. It is extremely important for this list to be accurate and updated if necessary. Advisories with lists prepared in a reckless manner will definitely not be highly regarded and considered as valuable in the IT community.

The next parts of the advisory – overview, description and impact – contain a brief description of consequences that the issue may cause, a description of the problem and its impact on affected systems (eg, severe performance degradation).

The solution section is expected to tell the users how to secure their network. If there is official solution published by the vendor, a link to it is enough.

The analysed advisory contains one more section which is very important – Appendix A – vendor information. There, the reader can find links to advisories published by vendors (Cisco and Microsoft in this case). As CERT advisories are usually brief, it is very important to give the user links to more detailed information should he need it. The section with links is usually called references.

Discuss with the students the differences between their agreed list and the example of a CERT advisory. Did the students miss any key fields? Was the CERT advisory complete?

6.3.2 Task 2 Example of a step-by-step advisory comparison

Once a general introduction has been made, the students should be given a step-by-step comparison guide to advisories. You can use the following CISCO IOS example or prepare your own. An example analysis is given below. Encourage the students to participate by asking them what they like or dislike about each particular advisory. Moderate the discussion.

In 2003 a vulnerability that enabled the blocking of a router interface by sending only one crafted IPv4 packet was revealed. The vulnerability was quite serious as it opened the possibility for a denial-of-service attack on Cisco routers. The advisories that were published describing the vulnerability can be found on the Virtual Image.

Let us start with the document published by IBM ISS.[8] The document begins with a short description of the problem. Then a long list of affected versions of the IOS system is included. The list may seem a bit overwhelming, but it gives the administrator precise information as to whether the software he is using is under threat. Two elements are circled on the picture depicting part of the advisory: the ID of the advisory and the level of the threat.

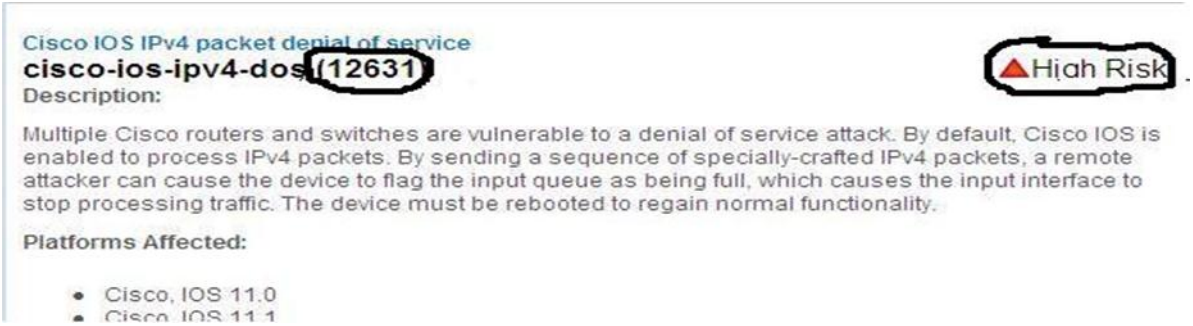
Cisco IOS IPv4 packet denial of service
cisco-ios-ipv4-dos (12631)
High Risk
Description:
Multiple Cisco routers and switches are vulnerable to a denial of service attack. By default, Cisco IOS is enabled to process IPv4 packets. By sending a sequence of specially-crafted IPv4 packets, a remote attacker can cause the device to flag the input queue as being full, which causes the input interface to stop processing traffic. The device must be rebooted to regain normal functionality.
Platforms Affected:
- Cisco, IOS 11.0
- Cisco, IOS 11.1

Figure 1: Advisory ID and threat severity

It is very important that advisories published by institutions are clearly identifiable. However the ISS ID number approach may be confusing. Would it be better if it included the date of publication? It would then be immediately obvious whether the issue is current or not. The severity of the issue is also stated plainly at the very beginning, which is very helpful in

[8] *http://xforce.iss.net/xforce/xfdb/12631*

drawing the reader's attention when the issue is serious. How complex should this severity level system be? As you will see, many advisories lack information concerning the severity. We should notice that this advisory does not actually include any remedy for the issue. There is only the ID of Cisco's advisory which includes the remedy and to which the link is given in the references part.

The next advisory on the very same issue was published by the CERT Coordination Center.[9] The first noticeable difference is the document ID: CA-2003-15 is more informative than 12631 in the ISS case. On the other hand, the CERT advisory does not provide precise information concerning the systems affected by the issue. There is only one sentence, claiming that all devices running Cisco IOS software and processing IPv4 protocol are affected.

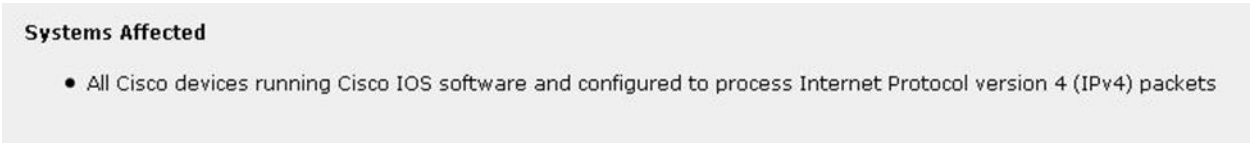

Figure 2: Vague information about affected systems

Even if it were true at the time of publication, it is always doubtful whether this kind of statement is still valid. Furthermore, someone reading this advisory today could think that it is still true and start looking for a remedy. Of course, there should be a way to check the date of publication of the advisory and compare it with the date of the IOS release. But would it not just be easier and more reliable to list all the releases of IOS software that are affected? Would it be useful if a list of unaffected systems was also maintained? Confusion is definitely not the feeling we want administrators to have after reading an advisory. Therefore vague statements should be avoided in this kind of document. Compared to the ISS advisory, the CERT document also lacks specification of the severity. Aside from these issues, the CERT document is a well-prepared brief explanation of the problem. Solutions for the problem are presented, as well as references to other sources including the Cisco advisory – which is very important.

The next document we are going to examine is the advisory published by Cisco[10] – the provider of the software that was revealed to be vulnerable. In the last paragraph you had a chance to see advisories published by so-called *other parties* - not involved in the software development process. You will see that the document published by Cisco is quite different – the issue description and analysis is much more thorough. This is because Cisco, as the developer and maintainer, is expected to give the last and the final solution. Note that the Cisco's document includes an even more detailed list of the affected systems than the ISS advisory. Moreover, the procedure for checking the version of the software the router is running is also specified. For each version of the software an individual solution is suggested. Where an upgrade is suggested, an alternative workaround is also given. One more thing that

[9] http://www.cert.org/advisories/CA-2003-15.html

[10] http://www.cisco.com/warp/public/707/cisco-sa-20030717-blocked.shtml

is characteristic for a document published by the provider is a more thorough description of the problem – the causes and consequences. You should also notice that aside from the ID, Cisco's document also has a revision number and the period of time during which it was actively updated is broader compared to, for example, the CERT document. (The CERT advisory was published on July 16, 2003, and last updated on July 17, 2003 – while Cisco's was published the same day but last updated on July 22, 2004.)

6.3.3 Task 3 Comparison of real advisories by the students themselves

Once an example comparison has been carried out, the students should be tasked with carrying out a comparison between advisories by themselves. The trainer can use the example prepared below, use a different vulnerability, or ask the students to suggest a set of advisories to be compared.

In this exercise students are expected to work alone or in small groups. Ask the students to review seven security advisories describing vulnerabilities in DNS servers (CVE-2008-1447). As the trainer, you are expected to lead and moderate the discussion. A checklist table should be supplied as shown below, which the students can fill out with their comments. These comments could include ratings, such as POOR or GOOD, PRESENT or ABSENT, or more elaborate statements if necessary. The documents you are going to analyse are available on the DVD in the advisories exercise subfolder. Also available online are:

- 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

The students should:

- Study all the advisories carefully.
- Fill in the checklist with their comments.
- Select the document they like best and the one they like least. Students should be prepared to justify their choices.

A general discussion with all the students should be carried out. Is a consensus on the 'best advisory' possible? What is the value of standards such as CVE?

DNS (CVE-2008-1447) checklist

Document	US-CERT (TCSA)	US-CERT (VN)	NVD NIST	Security Focus	Secunia	Microsoft	ISC
Problem Name and ID	1.1.32	1.1.33	1.1.34	1.1.35	1.1.36	1.1.37	1.1.38
Threat severity and Impact	1.1.39	1.1.40	1.1.41	1.1.42	1.1.43	1.1.44	1.1.45
Affected systems	1.1.46	1.1.47	1.1.48	1.1.49	1.1.50	1.1.51	1.1.52
Description	1.1.53	1.1.54	1.1.55	1.1.56	1.1.57	1.1.58	1.1.59
Possible remedies (solutions, workarounds, patch locations)	1.1.60	1.1.61	1.1.62	1.1.63	1.1.64	1.1.65	1.1.66
References	1.1.67	1.1.68	1.1.69	1.1.70	1.1.71	1.1.72	1.1.73
Revision notes	1.1.74	1.1.75	1.1.76	1.1.77	1.1.78	1.1.79	1.1.80
Other fields: digital signatures, contact information?	1.1.81	1.1.82	1.1.83	1.1.84	1.1.85	1.1.86	1.1.87
How informative?	1.1.88	1.1.89	1.1.90	1.1.91	1.1.92	1.1.93	1.1.94
Structure of the documents?	1.1.95	1.1.96	1.1.97	1.1.98	1.1.99	1.1.100	1.1.101
Additional comments	1.1.102	1.1.103	1.1.104	1.1.105	1.1.106	1.1.107	1.1.108

6.4 PART 2 CVSS TRAINING

This part of the exercise is optional.

It deals with the *Common Vulnerability Scoring System*. It has been added as an optional tool as it could assist a CERT team in properly categorizing the severity level of a vulnerability being described in a security advisory. The main lessons to be learned from these exercises are:

- Different vulnerabilities may have differing impacts on different organizations (CERT constituency);
- The severity of a vulnerability may change with time; and
- Whether the complexity of such a scoring system is a benefit compared to simpler methods of rating the severity levels of a problem.

You should discuss the above issues with the students at the end of the exercise.

6.4.1 Task 1 CVSS basics and tools

The Common Vulnerability Scoring System (CVSS) is a standard for assessing the characteristics and impact of vulnerabilities in computer security. Its main goal is to establish the importance and priority of a particular vulnerability and describe its characteristics. The score consists of a series of assessments called ***metrics***. The currently used version is CVSS v2. CVSS is under the custodial care of the Forum of Incident Response and Security Teams (FIRST: www.first.org). However, it is a completely free and open standard.

In this part, as the trainer you are expected to:

- Introduce the CVSS (describe the differences between particular metrics, how they are established, and what Vector is and how to read and write it);
- Establish CVSS metrics, together with the students, based on one example: DNS vulnerability (CVE-2008-1447); and
- Perform an exercise that relies on the environment metrics.

The exercises will use the free *JVNRSS: CVSS V2.0 Calculator for PC* which was developed, provided and copyrighted by the JVN (http://jvnrss.ise.chuo-u.ac.jp/jtg/cvss/en/index.02.html#ssCVSSv2PC). This calculator is available on the *Cert Exercises Virtual Image.* If there is an Internet connection, the online *NVD CVSS v2 Calculator*: (http://nvd.nist.gov/cvss.cfm?calculator&version=2) may be used instead.

Introduce these tools to the students.

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

In this exercise you should help the students to establish the CVSS vectors and metrics of the DNS CVE-2008-1447 vulnerability.

First, together with students, establish the base metrics (vector and score) of the CVE-2008-1447 vulnerability (based on http://nvd.nist.gov/nvd.cfm?cvename=CVE-2008-1447):

Access Vector (AV): Network (N)

Access Complexity (AC): Low (L)

Authentication (Au): None (N)

Confidentiality Impact (C): None (N)

Integrity Impact (I): Partial (P)

Availability Impact (A): Partial (P)

So, the vector is: **(AV:N/AC:L/Au:N/C:N/I:P/A:P)** and the **base score is 6.4** (medium).

Explain the above.

Next, together with the students, establish temporal metrics (vectors and scores) for this vulnerability, but depending on the timeline. (Note that these temporal metrics are not official, but are simply an example.)

Timeline:

8.07.2008: public information about vulnerability in multiply DNS implementations[11]. There were no technical details available. Note that most vendors release an official fix together with a security advisory.

Suggested temporal score: 4.3 (E:U/RL:OF/RC:UC)?

21.07.2008: a leak with more specific information. This blog entry was removed.

Suggested temporal score: 4.5 (E:U/RL:OF/**RC:UR**)?

23/24/25.07.2008: public exploit on BIND released.

Suggested temporal score: 5.0 (**E:POC**/RL:OF/**RC:C**)?

29.07.2008: first confirmed successful attack (on AT&T's DNS servers[12]):

Suggested temporal score: 5.3 (**E:F**/RL:OF/RC:C)?

2.08.2008: update of official Bind patch:

Suggested temporal score: 5.3 (E:F/**RL:OF**/RC:C)?

Next you should outline an example organization's environment and, together with the students, establish environmental metrics (vector and score) for this organization. You should moderate any discussion with the students.

Example:

The organization is a medium ISP which has its own DNS servers for its clients. DNS is based on Bind 9.4.1 (this is a vulnerable version) …

6.4.2 Task 3 Calculation of CVSS scores by students themselves

For this task divide students into groups (2-3 persons each). First, every group should imagine its own organization's environment and write a short description of it. Next, all groups together should choose one of the security advisories that describe some vulnerability. Students could choose one from earlier stages of this exercise ('writing security advisories'). Next, all groups must separately establish all CVSS metrics (in about 10-15 minutes). After that, all groups should discuss their results together.

[11] http://isc.sans.org/diary.html?storyid=4687

[12] http://isc.sans.org/diary.html?storyid=4801

Two other different variants of this exercise are also possible: all groups are operating in that same organization's environment or each group has a different security advisory but the same organization's environment.

6.5 Summary of the exercise

Summarize the exercise and the conclusions of the discussions. Encourage students to exchange their opinions, ask questions, and give their feedback about the exercise.

6.6 EVALUATION METRICS

The students should be judged on their performance in answering the questions posed during the exercise.

Additional evaluation metrics may include:

- Did the students fail to point out anything that was missing in any real advisory?
- Did the students adequately explain why they preferred one data format to the other?
- Where the students were able to identify something specific to their constituency in the context of security advisories, was the rationale behind their arguments sound?
- Did the students understand why CVSS scores may differ?

6.7 REFERENCES

1. WARP How to write a Warning Advisory
   http://www.warp.gov.uk/WARPServices/HowToWriteAdvisoryV2.0.pdf
2. Janet Guidance Notes - Writing Advisories
   http://www.ja.net/documents/publications/technical-guides/gn-advisories.pdf
3. A Complete Guide to the Common Vulnerability Scoring System, version 2.0

   http://www.first.org/cvss/cvss-guide.pdf