EUROPEAN COMMISSION
DIRECTORATE-GENERAL
HUMAN RESOURCES AND SECURITY
Directorate DS - Security
Coordination and Informatics Security

Brussels, 30/09/2011
HR.DS5/GV/ac ARES (2011) 1039224
SEC20.10.05/04 - Standards

European Commission

Information System Security Policy

C(2006) 3602

GUIDELINES ON TECHNICAL VULNERABILITY MANAGEMENT

Version 0.2_28/07/2011

TABLE OF CONTENTS

1. INTRODUCTION

Technical vulnerabilities are weaknesses in information systems that can cause the occurrence of a threat. These threats are usually deliberate ones, such as malware or hackers, but they can also be technical problems, for instance a memory leak that could cause systems to become unstable.

Since new vulnerabilities are constantly identified in information systems, the effective level of security of these systems will decrease over time if they are not properly maintained, as these vulnerabilities become known and attacks are devised that exploit them. Consequently, any such vulnerabilities must be identified and appropriate measures taken to control them.

This Guidelines document is a supplement to the *Standard on Technical Vulnerability Management*, and provides suggested methods for applying some of the rules in the Standard.

2. OBJECTIVES

See the *Standard on Technical Vulnerability Management*.

3. SCOPE

This document is a supplement to the *Standard on Technical Vulnerability Management*, and has the same scope. Its application is optional.

4. TERMINOLOGY

See the *Standard on Technical Vulnerability Management* for terminology.

5. BACKGROUND INFORMATION

The Standard on Technical Vulnerability Management states the following:

> *Every information system must be evaluated to establish a Vulnerability Baseline Score for its sensitivity to technical vulnerabilities. This score is based on two main elements:*
>
> - *Number of systems affected*
> - *CIA classifications*
>
> *The system's Vulnerability Baseline Score is then used together with the severity rating for each vulnerability identified in order to determine the deadline for remediation. Additional risk factors that affect the impact or likelihood of a particular vulnerability should also be taken into account.*

This document describes a suggested method for performing this evaluation, as described below. This method has been designed to be simple, flexible and practical. Other methods may also be used, provided that they fulfil the requirements of the *Standard on Technical Vulnerability Management*.

6. EVALUATION METHODS

6.1. Determining the Vulnerability Baseline Score

The Vulnerability Baseline Score may be calculated from data that are readily available, specifically the number of systems affected and their CIA classifications.

Number of Systems Affected

The potential impact depends partly on the number of systems (workstations, servers etc.) that must be patched. This affects the cost and time required to complete the process.

The number of systems affected is scored as follows:

Number of systems	**Score**
1 to 9	3
10 to 99	6
100 or more	9

CIA Classifications

The classifications for the confidentiality, integrity and availability must be established for each information system (see Commission Decision C(2006) 3602 and the *Standard on Risk Management*).

The CIA classifications for non-EUCI systems are scored as follows.

Confidentiality	**Integrity / Availability**	**CIA Score**
PUBLIC	Moderate	1
LIMITED BASIC	Critical	2
LIMITED HIGH	Strategic	3

Calculating the Vulnerability Baseline Score

The final Vulnerability Baseline Score (VBS) is the sum of the scores for the aspects described above. The following table may be used to summarise the scores.

Aspect	**Possible values**	**Score**
Number of Systems	3 (<10), 6 (10 to 100) or 9 (>100)	
Confidentiality	1 (PUBLIC), 2 (LIMITED BASIC) or 3 (LIMITED HIGH)	
Integrity	1 (Moderate), 2 (Critical) or 3 (Strategic)	
Availability	1 (Moderate), 2 (Critical) or 3 (Strategic)	
	TOTAL	/ 18

The total score will be a figure in the range of 6 to 18 points.

Specific factors relating to the information system which can materially increase or decrease the risk from vulnerabilities should be documented together with the VBS, and may be used to increase or decrease the total score. The following is a list of suggested factors that would significantly modify the level of risk of the system, together with suggested score modifiers (other factors may be taken into consideration too). A positive score (+) indicates higher risk, and a negative score (-) indicates a lower risk:

- The system is a security device (firewall, IDS, proxy etc) (+2)
- The system performs financial transactions (+1)
- The system is available for use on the Internet (+1)
- The system is only used within a secure network zone (-1)
- The system is not yet in production (-1)

6.2. Determining Patch Deadlines

Response times for the remedial actions must be determined on the basis of the VBS (see § **Error! Reference source not found.** above) and the severity (see the *Standard on Technical Vulnerability Management*). These two elements are combined in the following table, which gives suggested

deadlines for remediation[1]. The table may be revised if the deadlines are not considered to be appropriate.

Severity **VBS**	*Low*	*Moderate*	*Important*	*Critical*
<= 7	3 months	2 months	1 month	2 weeks
8 – 10	2 months	1 month	2 weeks	2 weeks
11 – 13	1 month	2 weeks	2 weeks	1 week
14 – 16	2 weeks	2 weeks	1 week	5 days
>= 17	2 weeks	1 week	5 days	3 days

For systems that are installed on multiple computers, a target percentage of systems successfully patched must also be determined. As a general rule, the figure of 95% is suggested.

7. REFERENCES

Note that documents marked (*) are in draft at the time of writing of this document.

- Commission Decision C(2006) 3602 of 16/8/2006

- Implementing rules for Commission Decision C(2006) 3602 of 16.8.2006.

- Standard on Technical Vulnerability Management (*)

[1] Note: these deadlines should be counted from the time of first publication of a vulnerability by one of the sources used by the Commission.