737/1024

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

STANDARD ON TECHNICAL VULNERABILITY MANAGEMENT

ADOPTED BY MRS. IRENE SOUKA,

DIRECTOR-GENERAL OF DG HUMAN RESOURCES AND SECURITY, ON 30/09/2011

Version 0.6_05/08/2011

TABLE OF CONTENTS

1. ADOPTION PROCEDURE

This Security Standard is adopted in accordance with Article 10(3) of Commission Decision C(2006) 3602 concerning the security of information systems used by the European Commission, adopted on 16 August 2006.

It is drawn up under the responsibility of the Security Directorate pursuant to Article 9(1)(b) and takes into account the items listed in Article 10(2) of Commission Decision C(2006)3602, in particular internationally recognised norms and standards applicable in the field of information systems security.

Under Article 10(3) of Commission Decision C(2006) 3602, the implementing rules may be supplemented by measures of a technical, physical, procedural or organisational nature proposed by the Director of the Security Directorate and adopted by the Director-General of the Directorate-General for Human Resources and Security in consultation with departments that have a legitimate interest. These supplementary measures are called 'security standards' where their application is mandatory, or 'security guidelines' where their application is optional or where they provide guidance on security standards implementation.

2. 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.

3. OBJECTIVES

This standard provides instructions for the maintenance of information systems used by the Commission, specifically relating to the remediation of technical vulnerabilities (usually through software updates). The instructions are intended to ensure that the equipment and the information stored and handled thereon are protected against threats seeking to exploit such vulnerabilities, whilst taking into consideration the risk of unavailability of the information systems that may be caused by faulty updates.

4. SCOPE

This standard applies to all IT systems that are operated by or on behalf of the European Commission, including servers, workstations, network equipment and mobile computing devices. The measures mandated by this standard must be followed by all relevant personnel, including all Commission officials, contractors and third parties who are responsible for operating Commission IT systems.

5. THREATS COVERED

Security controls defined in this information security standard will help to reduce the impact of the following threats (their description is in the *Standard on Information Security Risk Management*).

T13 – Failure of Telecommunication Equipment

T26 – Tampering with Software

T31 – Software Malfunction

T32 – Breach of Information System Maintainability

T33 – Unauthorised Use of Equipment

T36 – Corruption of Data

6. TERMINOLOGY

Back-up: the process of copying data to a separate store in order to protect it from unavailability or corruption of the principal store; also the data so stored.

Exploit: a technique whereby an attacker makes use of a vulnerability to perform unauthorised actions in an information system.

Incident: any event which is not part of the standard operation of a service and which causes, or may cause, an interruption to, or a reduction in, the quality of that service. Specifically, an information security incident is an incident that entails a breach of the confidentiality, integrity or availability of EU information, or non-compliance with the Commission's security rules.

Mobile device: any computing or telephony device that is capable of being carried and used independently. See the *Standard on Mobile Computing and Teleworking* for more information on mobile devices.

Operating procedures: formal documentation of the approach to executing tasks related to the production and maintenance of hardware and software.

SECOPS: Security Operating Procedures

Vulnerability: a lack or failure of an information system that could be exploited by a threat. Also sometimes referred to as a weakness (see the *Standard on Risk Assessment*, particularly section 3.2 of the annex, for more explanation of vulnerabilities).

Weakness: see Vulnerability

7. BACKGROUND INFORMATION

Technical vulnerabilities are weaknesses or faults in hardware or software that can cause a failure or enable an attacker to compromise the system somehow (e.g. using an exploit). They are usually issues relating to software, although occasionally hardware items can be affected (for example, faulty hard disks or processors)[1]. They can increase the risk of deliberate attacks, such as malware or hackers attempting to penetrate systems, or the risk of accidental incidents, e.g. through hardware failures.

To reduce the risk of security incidents, technical vulnerabilities need to be identified, analysed and, where necessary, corrected soon after they become known. Many of the viruses that have caused widespread problems in the past used known vulnerabilities, and did not affect systems that had been updated with the most recent security patches.

Information on technical vulnerabilities may come from a number of different sources, including:

- Notification of vulnerabilities by software suppliers
- Notification of vulnerabilities by third parties (e.g. CERTs)
- Results of technical vulnerability assessments or audits
- Weaknesses reported by users
- Analysis of incident records (problem management)

8. CONTROL OF TECHNICAL VULNERABILITIES

Policy objective 6.7.1 – Control of Technical Vulnerabilities – Timely information about technical vulnerabilities of information systems being used must be obtained, the Commission's exposure to such vulnerabilities evaluated and appropriate measures taken to address the associated risk.

8.1. General Principles

A process must be in place to identify and address technical vulnerabilities in the Commission's information systems (including both software and hardware) in order to reduce the risks from malicious software or attackers. This process must be in place for all information systems, although the methods and frequency of checking for vulnerabilities and updates may be more rigorous for higher risk systems.

---

[1] This standard generally describes software vulnerabilities since they are far more common, but the same process should be followed in the event of hardware vulnerabilities (for instance, a manufacturer notifying customers that a specific component is faulty or subject to particularly high rates of failure).

To support this process, a comprehensive inventory of information systems (hardware and software) must be in place that includes details of versions in use. See the *Standard on Asset Management* for further information.

The remainder of this standard describes a process for performing this security control. It is also acceptable for a different process to be in place (e.g. using another method for calculating the levels of risk), as long as it covers the principles described below.

8.2. Evaluating Information Systems

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.

A suggested method for calculating the Vulnerability Baseline Score and the deadline for remediation is given in the accompanying *Guidelines on Technical Vulnerability Management*.

8.3. Identifying Technical Vulnerabilities

Technical vulnerabilities must be identified for all systems as quickly as possible in order to minimise the time lost before a solution can be implemented. The following methods must be used for all systems:

- Checking for vulnerabilities and patches with the system's manufacturer(s) – ideally through subscription to a notification service; if this is not available, then a periodic check should be performed (e.g. on the manufacturer's web site), with the period varying from 1 day to 1 month depending on the exposure to risks of the system.
- Users must be able to report weaknesses (see the *Standard on Information Systems Security Incident Management*).
- Results of technical vulnerability assessments or audits.

For sensitive systems, such as dedicated security software or devices (firewalls, proxy servers, IDS/IPS, authentication services etc.), information on vulnerabilities must also be obtained from third party sources such as CERTs or security monitoring services.

Patch or vulnerability notifications are often signed to authenticate the sender. These signatures must be validated before further action is taken to ensure that the notification is genuine. If a notification is received without a signature from a source that normally signs its notifications, the information must be verified.

It should be noted that this standard only applies to vulnerabilities and patches or fixes that are related to security. Functional updates are out of scope (although functional updates to security devices are also considered to be security updates).

8.4. Evaluating Risks

Once a technical vulnerability has been recognised, a risk analysis must be performed to identify the potential impact of the vulnerability on the Commission's information systems (risk of inaction). The risk analysis is based on the severity of the vulnerability combined with the system's vulnerability baseline score, and any other relevant factors.

The severity of a vulnerability is measured on a scale as described in the table below. This is the same as the scale used by many major software manufacturers[2], and so in many cases the rating assigned by the software manufacturer can be used without further analysis.

Level	**Description**[3]	**Score**
Low	A vulnerability whose exploitation is extremely difficult, or whose impact is minimal.	1
Moderate	Exploitability is mitigated to a significant degree by factors such as default configuration, auditing, or difficulty of exploitation.	2
Important	A vulnerability whose exploitation could result in compromise of the confidentiality, integrity, or availability of users' data, or of the integrity or availability of processing resources.	3
Critical	A vulnerability whose exploitation could allow the propagation of malware without user action.	4

Mitigating factors may be taken into account to reduce the severity rating. For example, if a vulnerability exists in a module that is not used by the EC, or requires certain use conditions (e.g. a specific port open to the Internet

---

[2] Including Microsoft, Adobe, VMWare and Red Hat

[3] The descriptions are based on the "Microsoft Security Response Center Security Bulletin Severity Rating System (Revised, November 2002)" (http://www.microsoft.com/technet/security/bulletin/rating.mspx)

which is closed on the EC's firewalls), then the severity level may be reduced by one.

The Vulnerability Baseline Score (VBS) and any specific factors that are documented for the system (see the Guidelines on Technical Vulnerability Management) should also be taken in consideration when evaluating the potential impact of a vulnerability.

Response times for the remedial actions must be determined on the basis of the VBS and the severity[4].

For systems that are installed on multiple computers, a target percentage of systems successfully patched must also be determined, in the range of 90-100%.

8.5. Determining appropriate actions

In risk management, the options for treating risks are to *Mitigate*, *Transfer*, *Avoid* or *Accept* them. If the risk relating to a vulnerability is not acceptable, a course of action must be determined[5]. Possible actions include one or more of the following:

- Implement the relevant patch as an emergency change (mitigate)
- Implement the relevant patch as (part of) a scheduled change (mitigate)
- Implement alternative countermeasures instead of a patch (e.g. if a patch is not yet available or as a temporary measure until the patch is implemented), such as:
    - Turning off services or capabilities related to the vulnerability (avoid)
    - Adapting or adding access controls, e.g. firewalls, at network borders (mitigate)
    - Increased monitoring to detect or prevent actual attacks (mitigate)
    - Using alternative software (avoid)
    - Changing configuration settings (mitigate)
    - Raising awareness by informing users of behaviour or use to be avoided (mitigate)

---

[4] A suggested method for determining response times is given in the *Guidelines on Technical Vulnerability Management*.

[5] See the accompanying Guidelines for help on determining risk levels.

Other factors such as the cost and risks of the possible solutions and any potential business impact may be taken into account when determining the most appropriate course of action.

8.6. Implementing Solutions

Solutions must be implemented within the agreed response time as defined above.

All security patches must be tested before being implemented on operational systems.

The system manager must ensure that:

- All patch and update procedures are conducted in accordance with established change control procedures (see the *Standard on Operational Management* and, where relevant, the *Standard on Secure Systems Development*).
- All patches and updates are obtained from authorised patch delivery sources.
- Patches are only installed by appropriate IT staff.
- Patch and update procedures include rollback procedures to return to the last working configuration whenever possible.
- When appropriate, security monitoring and scanning tools are used to verify that remediation activities have been performed; then a new system vulnerability baseline must be created.
- Configuration procedures, hardening scripts, inventories, etc. are updated as required to reflect the new baseline (after the vulnerability has been corrected).

If an update cannot be applied within the deadline (e.g. an update is not available to correct a vulnerability or a decision is taken to delay implementation), then the vulnerability must be mitigated by an acceptable alternative countermeasure such as those listed in section 8.5 above.

All patching or other vulnerability mitigation actions must be recorded in an audit log. The outcome of the patching procedure must be checked and reported, particularly where systems are updated using automated tools.

New systems must be assessed for vulnerabilities and patched (or other measures applied) as appropriate before they are deployed.

Reference configurations must also be updated to include patches.

9. ROLES AND RESPONSIBILITIES

System Managers: responsible for ensuring that an appropriate technical vulnerability management process is in place for their systems, and that updates are applied in accordance with the relevant change control procedures.

LISO: responsible for advising on the need for technical vulnerability management, the severity of vulnerabilities and possible alternative countermeasures & checking patch audit logs.

DIGIT: responsible for establishing technical vulnerability management processes for all systems and software that it provides.

System Owner: responsible for approving any decisions to delay patches and accepting residual risks.

10. REFERENCES

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

- Commission Decision C(2006) 3602 of 16/8/2006
- Implementing rules for Commission Decision C(2006) 3602 of 16.8.2006.
- Guidelines on Technical Vulnerability Management (*)
- Standard on Asset Management
- Standard on Information Systems Security Incident Management (*)
- Standard on Information Security Risk Management (*)
- Standard on Mobile Computing and Teleworking (*)
- Standard on Controls against Malicious Code (*)
- Standard on Operational Management (*)
- Standard on Secure Systems Development (*)

11. RELATED DOCUMENTS

- International standard ISO/IEC 27001 – Second edition 2005-06-15