

**Comments on the Report "Security Economics and the  
Internal Market"**

**(subsequently referred as the Report)**

**commissioned by European Network and Information  
Security Agency**

**Comments made by FIRST Vendor SIG**

**2008-April-30**

INTRODUCTION .....	3
SUMMARY .....	4
VENDORS' PARTICIPATION IN THE REPORT'S CREATION .....	5
DEFINITION OF A SECURITY VULNERABILITY.....	5
ON LIABILITY.....	7
<i>Need for additional liability legislation</i> .....	7
<i>Origin of the vulnerability</i> .....	7
ON RECOMMENDATION 5: "STANDARD FOR NETWORK-CONNECTED EQUIPMENT" .....	8
ON RECOMMENDATION 6: "VULNERABILITY DISCLOSURE" .....	8
ON RECOMMENDATION 7: "FREE PATCHES AND SEPARATION FROM FEATURES" .....	9
ON AUTOMATED PATCHING .....	10
CONCLUSION .....	11

## Introduction

This document is put forward by FIRST Vendor Special Interest Group (Vendor SIG, <http://first.org/vendor-sig/>). This forum comprises teams that deal with product security vulnerabilities within their respective companies. The following companies are members of the Vendor SIG:

Alcatel-Lucent	Mindjet
Apple	Motorola
Aruba Networks	NEC
Axliance	Netasq
Beeware	Nokia
Cisco Systems	Nortel
Ericsson	NTT
Force10 Networks	Oracle
Hitachi	RedHat
HP	Ricoh USA
IBM	SAP
Intel	SGI
Juniper	Skype
Microsoft	Sun Microsystems

The comments in this document are not intended to and do not represent the individual views or policies of each member company of Vendor SIG. Individual companies reserve the right to submit additional comments in their own right. To contact individual members of Vendor SIG, you may use the information at <http://first.org/vendor-sig/participants/>.

Vendor SIG would be glad to answer any questions arising from these comments. We can be contacted (collectively) at [vendor-sig@first.org](mailto:vendor-sig@first.org).

## Summary

The Report raises some interesting points and may be used as a starting point for a discussion. Some of the recommendations made in the Report are formulated without consideration of a full picture of the critical network infrastructure and the current state of affairs among networks, users, and vendors. Additionally, some crucial definitions are missing, most notably the definition of a security vulnerability.

The Vendor SIG strongly recommends further research before final conclusions are made. Members of the Vendor SIG would like to help with subsequent research and participate in discussions. Reaching the correct conclusions is in the interest of all parties involved.

Our comments are focused around the following recommendations and statements made in the Report:

- Definition of a security vulnerability
- On liability
- Recommendation 5: "We recommend that the EU develop and enforce standards for network-connected equipment to be secure by default."
- Recommendation 6: "We recommend that the EU adopt a combination of early responsible vulnerability disclosure and vendor liability for unpatched software to speed the patch-development cycle."
- Recommendation 7: "We recommend security patches be offered for free, and that patches be kept separate from feature updates."
- On automated patching

Summary of comments of Vendor SIG:

- 1) Vendors are concerned that they were not consulted during the work on the Report. The Report presents only one perspective on the issues and does not fully take into account certain realities of fixing security vulnerabilities.
- 2) We call for establishing an objective and quantitative definition of what constitutes a security vulnerability.
- 3) We believe that imposing further liability on vendors will have a stifling effect on the industry. This effect would be especially devastating to open source vendors and small vendors in general.
- 4) The Report's recommendation for responsible disclosure does not take into account different deployment models (home versus business users) and must be revisited to fit business users. Furthermore, the proposal is not fully articulated; some of the premises on which these recommendations are based may not reflect the reality in which vendors or users operate.
- 5) The recommendation for vendors to offer free patches fails to accommodate vendors' different business models. The lack of a quantitative definition of security vulnerability makes it difficult to distinguish security fixes from new features.
- 6) The recommendation for automated patching fails to account for different deployment models. Two examples are:

- Enterprise computing environments where patches must be thoroughly tested before deployment.
- Supervisory Control and Data Acquisition (SCADA) systems where applying updates can void the maintenance contract with the vendor.

Having the capability for automatic patching will not help if it is not possible or if it is risky to actually use it.

Members of the Vendor SIG are more than willing to address any comments that may arise from this document and look forward to a further dialogue between ENISA, EU and Vendor SIG.

## **Vendors' Participation in the Report's Creation**

In its current form, the Report presents a single perspective on a complex issue. Recommendations in the Report, while made in good faith and with good intentions, fail to include vendors' and users' perspectives, incentives, and realities.

We are cognizant that recommendations made in the Report do not reflect European Network and Information Security Agency (ENISA) opinion; however, it is troublesome that only a singular perspective is given. We do not believe that balanced conclusions can be reached unless the issue is considered from multiple perspectives.

**Vendor SIG strongly recommends that another report be commissioned before any final conclusions are made. The new report should include vendors' perspectives. Vendors have a compelling, vested interest to fix security vulnerabilities and are making progress in that area.**

## **Definition of a Security Vulnerability**

Throughout the Report, "security vulnerability" is used as a term but is never defined. To enable a truly productive discussion on this topic, the term must be defined.

Currently, there are several definitions on what constitutes a security vulnerability. For example, the definitions from the National Infrastructure Advisory Council (NIAC) and the National Institute of Standards and Technology (NIST) can be used. According to NIAC's "Vulnerability Disclosure Framework"<sup>1</sup> document:

“For purposes of this report, a vulnerability is defined as a set of conditions that leads or may lead to an implicit or explicit failure of the confidentiality, integrity, or availability of an information system. Examples of the unauthorized or unexpected effects of a vulnerability may include any of the following:

---

<sup>1</sup> NIAC Vulnerability Disclosure Framework, Final Report, <http://www.dhs.gov/xlibrary/assets/vdwgreport.pdf>, 2004-Jan-13, pg. 13.

- Executing commands as another user
- Accessing data in excess of specified or expected permission
- Posing as another user or service within a system
- Causing an abnormal denial of service
- Inadvertently or intentionally destroying data without permission
- Exploiting an encryption implementation weakness that significantly reduces the time or computation required to recover the plaintext from an encrypted message

Common causes of vulnerabilities are design flaws in software and hardware, botched administrative processes, lack of awareness and education in information security, and advancements in the state of the art or improvements to current practices, any of which may result in real threats to mission-critical information systems.”

National Institute of Standards and Technology (NIST), in its "Risk Management Guide for Information Technology Systems"<sup>2</sup>, defines security vulnerability as:

“Vulnerability: A flaw or weakness in system security procedures, design, implementation, or internal controls that could be exercised (accidentally triggered or intentionally exploited) and result in a security breach or a violation of the system’s security policy. “

Neither of the above definitions (and many others that exist) are quantitative. These definitions cannot, in a general case, be used directly to gauge if something is or is not a security vulnerability.

The importance of this comes to light when considering Recommendation 7 in the Report. If vendors do not have a quantitative and non-subjective way to determine what a security vulnerability is, it is impossible to ask vendors to separate fixes from new features.

**The Vendor SIG recommends that further research be conducted to devise an objective and quantitative definition of what constitutes a security vulnerability. The research should be conducted jointly by academia and industry.**

---

<sup>2</sup> NIST Special Publications, SP800-30 “Risk Management Guide for Information Technology Systems“, <http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf>, July-2002, pg. 15.

## On Liability

Our comments on liability can be divided into several aspects:

- Need for additional legislation related to software liability
- Origin of the vulnerability

### **Need for additional liability legislation**

Vendors have a vested interest to make products with as few defects as possible. There is a wealth of research that shows that addressing security issues in the design and implementation phases is much less costly than after the product is delivered to the market.

Authors of the Report point out that EU already has legislation in place via the Product Liability Directive, so the need for additional regulation is questionable.

Introducing further liability legislation will have dramatic effects on all vendors, but it may be especially devastating to open source and small vendors. Faced with the threat of liability, many of these vendors may shut down. The loss of open source and small vendors will trigger a chain reaction among the rest of the industry. OpenSSL encryption library, Apache web server, and MySQL database server are used in many products (commercial and otherwise) and these products could vanish if liability is introduced.

The demise of open source and small vendors would increase the price of the products because vendors would have to develop missing elements themselves. Having to start from the beginning would certainly mean more problems (interoperability, usability and security) for several years.

Finally, the proposed liability will force further industry consolidation (in order to be able to handle liability suites), which would constrict users' choices even more.

**The Vendor SIG is very concerned about the potential demise of small and open source vendors and the subsequent effects on all vendors, which would stifle innovation, increase product prices, and decrease competitiveness.**

### **Origin of the vulnerability**

Additionally, when talking about liability, it is important to determine the source of the issue. In some cases, vendors correctly implement a standard only to discover that the standard itself is flawed. In all such instances, vendors must not bear any responsibility for having correctly implemented the standard.

When talking about the correctness of an implementation, so far there are no mechanisms that would prove the correctness of a complex program. It is not even possible to prove that a specification (whether a standard, a problem, or task) is complete and sufficient. Therefore, the best that the industry can do is to give its best effort. This is the area when industry is looking at the academia for help.

**Any discussion on liability must take into account the origin of the vulnerability.**

## **On Recommendation 5: "Standard for network-connected equipment"**

This recommendation calls for developing standards for security by default for network-connected products. While this is a laudable goal, it is important to emphasize that there is no single standard that is applicable for all usage cases. Expectations of home users differ from those of business users. The security profile for business users tends to be 'everything off,' so by default, the product is barely usable. In contrast, home users generally lack the necessary skills to configure products to meet their requirements, so they prefer a security profile where more features are enabled. Obviously, there are few more profiles between these two extremes.

The point is that users will be forced to choose one of the security profiles. It is not difficult for vendors to come up with a preset set of security profiles. Choice is where the real issue lies—by choosing an incorrect (for their purposes) profile, users will expose themselves to unnecessary risk.

**The Vendor SIG recommends that further research and education of users is needed. The research is needed to establish what constitutes safe usage models. Users must be educated so that they can make informed choices about exposure to on-line risks.**

## **On Recommendation 6: "Vulnerability disclosure"**

Producing a patch is not only about addressing a vulnerability, but also about addressing it correctly. Putting pressure on vendors to patch faster can have detrimental consequences on the quality of the fixes.

Depending on the scope of the issue, the time to properly address the vulnerability can vary. In extreme cases, vendors must conduct interoperability testing before the fix is considered valid. These actions cannot always be planned in advance, so factors such as timelines and how fast a vendor can produce the fix can not be set in advance, nor prescribed by a framework.

The other issue is so-called responsible disclosure—responsible, but towards whom? The Vendor SIG stance is that all actions must strive to protect customers and customer interests. The best way to do that is to provide sufficient information for customers to determine their exposure and the fix for the issue at the same time. Providing either of these two components separately is useless for customers and may only expose them to a greater risk.

Speed in applying patches is also important. The figures of 10 and 30 days (cited in the Report on page 64) are misleading. They represent how quickly vendors can react if a problem is discovered in the initial fix. These figures are not representative of how fast users actually apply the fixes. In many business environments, testing any software update (security relate or not) can take several months; in some cases, even a year. Overall, the speed of applying fixes (whether security fixes or new features) is

not governed by vendors but by the users. Vendors can and do produce fixes at a much faster rate than business users apply them.

Another issue that is missing from the Report is that many home users have not patched their computers even though patches have been readily available for several years. Because of this behavior by home users, it is important to ask what would constitute a "reasonable chance to update," as stated in the Report. More importantly, who would determine that time? Businesses operate on a different time scale from the average home user. Additionally, reasonable time to update seems to contradict the Report's recommendation for automated patching. If automated patching exists, it should install patches as soon as the patches are available, so reasonable time would be less than 24 hours.

**The Vendor SIG recommends that the proposal for vulnerability disclosure be reinvestigated because it neglects to consider the user's operational model.**

### **On Recommendation 7: "Free patches and separation from features"**

The sentiment of this recommendation is noble. However, there are several issues that have not been fully considered. The issues are:

- Distinguishing a vulnerability fix from a new feature
- Model of releasing security fixes
- Vendor's business model

Because no quantitative definition of what constitutes a security vulnerability is offered in the Report, it is impossible (in a general case) to differentiate a security fix from a feature. Replacing a DES encryption algorithm with EAS can be viewed as a security fix and also as a feature.

Let us consider the very basic issue of Denial of Service (DoS). If a single, properly formed packet can render a device completely inoperable, then probably everyone would agree that this is a security issue. If we start increasing the packet rate required to make the device inoperable, the situation can change. If sending 1000 packets per second (pps) results in a device's CPU utilization of 95%, is that a security vulnerability? What if we need packet rate of  $10^6$  pps or  $10^8$  pps to force the same CPU utilization? The general question is at what packet rate and CPU utilization will the event become a security vulnerability??"

The current definitions are qualitative rather than quantitative (e.g., NIST's definition contains "Causing an abnormal denial of service."). What is abnormal packet rate in this sense?

Separating features from a patch is not always feasible. The recommendation is made assuming a model where vendors release security fixes and features in the form of patches. This model fails on two accounts. The first is that some vendors do not release patches but re-release the new (fixed) software release as that works better for their product set.

The second issue with providing free patches is that the model that the authors of the Report had assumed that vendors are charging for their software. Not all vendors fit into this model. A notable exception from that model is Oracle. Oracle provides practically all of its software for free. The cost is recuperated through support and updates, and fixes are part of that support contract.

**The Vendor SIG does not support a forced separation of security fixes from features and free distribution of patches. The former is not feasible in a general case and the latter intrudes into vendors' business models.**

## **On Automated Patching**

The Report calls for all vendors to support automated patching in their products. The idea is good and again, vendors are not opposed. However, while not further elaborated, it seems that the automated patching is formulated having one specific model in mind. The model is software running on a general purpose computer or, with a stretch, a mobile phone or similar hand-held appliance. Further assumptions are that all updates should be performed automatically and that products would automatically check for them (this is often referred to as 'call home'). While the model and the assumptions may hold some validity for home users, it is not valid for business users.

No business user would allow automatic update of its critical components (operating system, database, network) without testing and verifying these updates first. In some environments, especially those that deal with classified material, it is absolutely prohibited for a product to call home. These systems do not, as a rule, have a direct connection to the Internet at all. For these reasons, automatic installation of updates is not a viable option in these cases.

The model in the Report also assumes that devices have some kind of input/output mechanism that can communicate directly with the user. This is not always the case. There are many appliances that lack these features or that are not convenient from the user's standpoint. Wireless access points and printers are some examples where the interface to the user is not readily present. While these devices have a way to be reached and managed, it is not expected of an average user to perform these actions on a regular basis. Therefore, just blindly pushing patches, without the capability for the user to verify, select, and approve patches, is not viable for home users or business users.

Having the capability for automated patching is a good feature, but without supporting elements, it will not provide the desired results. The problem of patching needs to be fully understood and a clear way to the solution found before undertaking any steps.

**The Vendor SIG recommends that further research be done in this area. Requiring industry to add more features before knowing the complete way towards the solution is not productive.**

## **Conclusion**

The recommendations in the Report are based on insufficient information. The Vendor SIG strongly advocates that any decisions made on the basis of the Report only will have adverse effects on the end users.

We strongly recommend that another report that includes participation of the industry be commissioned.

More consultation and research are required to be in a position to make any informed decision on this subject. The Vendor SIG is looking forward to fully participating in further consultation.