May 27, 2015

Response of

Red Hat, Inc.

to the Request for Comments regarding

Stakeholder Engagement on Cybersecurity in the Digital Ecosystem

Published by the National Telecommunications and Information Administration ("NTIA")
Docket No. 150312253-5253-01

Red Hat appreciates the opportunity to provide comments to NTIA on the above referenced matter, which touch on a wide range of potential cybersecurity topics that would benefit from a multistakeholder process.   To assist you in setting priorities, our comments focus specifically on item (d) under the section on 'Network Security', namely:

> Open Source Assurance. Many organizations depend on open source projects for a wide range of purposes across the digital economy. How can stakeholders better support improving the security of open source projects, and the distribution of patches?

Red Hat is the world's leading provider of open source software solutions, using a community-powered approach to deliver reliable and high-performing cloud, Linux, middleware, storage and virtualization technologies. An S&P 500 index member, Red Hat provides high-quality, secure and affordable technology solutions that are found throughout mission-critical systems in the financial, transportation, telecommunications and government (civilian and defense) sectors and in enterprises around the United States and the world. Red Hat is recognized as one of the world's most innovative companies.[1]

[1] See http://www.forbes.com/innovative-companies/list/.   See, also, Forbes, "The World's Most Innovative Companies", Sept. 2012, found at: http://www.forbes.com/innovative-companies/list/.

The 'Collaborative Innovation' Model

Collaborating through upstream software development projects is at the heart of the economic and business model that is driving the growing recognition that open source is the most effective way to develop software. Open source software vendors leverage the work done by innovative, vibrant open source communities (e.g., Linux, Jboss.org, OpenStack, Gluster, and KVM), allowing customers to take advantage of the work of many companies and individual developers. This collaborative model differs from the traditional proprietary software vendors' model where research and development are largely accomplished entirely by the vendors' employees.

In our case, Red Hat works with thousands of developers, only some of whom are our employees, who together contribute code and other work to upstream communities. Red Hat employees are among the key maintainers of, and contributors to, many of those communities. We find strength in the many people who contribute to - and the varied corporate and academic entities that sponsor - the open source projects that are our partners. The benefits of this collaborative innovation model do not flow to just one company; rather, the fruits of the work are available throughout the economy and empower many technology products and sectors.

Stakeholder Engagement in the Security of Open Source Projects

At the outset, it is should be noted that the level of "security" in software refers not only to the number and types of vulnerabilities within any given code, but also how quickly such vulnerabilities are discovered and fixed before exploitation can occur. As reported in the media, a few highly visible vulnerabilities in 2014 affected open source projects, even as open source software generally meets or exceed industry expectations for software quality as measured by low "defect density" rates.[2]

In the collaborative innovation model, more individuals (developer as well as end users) can inspect the source code to find, publicize and contribute to the fix of a possible vulnerability. This can lead to both faster discovery of unintentional security vulnerabilities and prevention of intentional vulnerabilities (backdoors) in the code.[3]

Stakeholder engagement in (and efforts to improve) the security of open source projects is deep and growing. In general, the community engaged in a particular project, along with end users (including vendors who produce products based on the upstream project), work on an on-going basis to maintain the security and address

[2] http://www.coverity.com/press-releases/coverity-scan-report-finds-open-source-software-quality-outpaces-proprietary-code-for-the-first-time/

[3] By contrast, the more traditional (proprietary) model of software development puts the end user in the position of accepting the level of security that the software vendor is willing to deliver, including the rate that patches and updates are released.

vulnerabilities that may arise. Large communities of open source software developers and maintainers such as software foundations and commercial enterprises generally have processes in place for dealing with vulnerability reports.

A notable recent high profile example of stakeholders coming together to fill a ‘gap’ with smaller projects is the Core Infrastructure Initiative (“CII”), which is housed at the Linux Foundation. Announced in April of 2014, CII will fund and support open-source software projects that are widely used, yet underfunded.[4]

Significantly, while the CII was created in the wake of Heartbleed, a critical security bug in OpenSSL, it will be used to identify a variety of important open source projects that need help in addition to OpenSSL[5] and fund specific tasks such as providing compensation to developers to work full-time on an open-source software project, conducting reviews and security audits, deploying test infrastructure, and facilitating travel and face-to-face meetings among developers.

Collaborative Engagement with Government

As appropriate, and with engagement with communities of developers and end users, the US Government has worked to support the improvement of open source software projects and communicate vulnerabilities and fixes.

One of the most significant of such efforts is the National Vulnerability Database (“NVD”), which is maintained by the National Institute of Standards and Technology (“NIST”), one of our nation’s premier national laboratories.[6] NVD is the U.S. government repository of standards-based vulnerability management data. This data enables automation of vulnerability management, security measurement, and compliance (e.g. FISMA). Of the top 50 ‘vendors’ included in the NVD, 16 are open source projects.

NIST also maintains a collaborative, community-based project to support development of tools to enable secure implementation and vulnerability assessment. Most notable is the Security Content Automation Protocol (SCAP),[7] a set of interoperable specifications derived from community ideas. According to NIST, “community participation is a great strength for SCAP, because the security automation community ensures the broadest possible range of use cases is reflected in SCAP functionality. ... We envision further expansion in compliance, remediation, and network monitoring.”

[4] Amazon Web Services, Cisco, Dell, Facebook, Fujitsu, Google, IBM, Intel, Microsoft, NetApp, Rackspace, VMware and The Linux Foundation Form New Initiative to Support Critical Open Source Projects, April 24, 2014.

[5] Tech giants, chastened by Heartbleed, finally agree to fund OpenSSL IBM, Intel, Microsoft, Facebook, Google, and others pledge millions to open source,, ArsTechnica, April 24, 2014.

[6] https://nvd.nist.gov/.

[7] http://scap.nist.gov/

In addition, the Department of Homeland Security is partnering with the private sector and communities through the Software Quality Assurance project to:

> “Develop tools, techniques and environments for analyzing software to detect security vulnerabilities associated with our Nation’s critical infrastructure and networks. Specifically, this project addresses the presence of internal flaws and vulnerabilities in software and deals with the root of the problem by improving software security. Test environments for these tools will also be built; one such facility is the SoftWare Assurance Market Place (SWAMP), which will develop research infrastructure that can be used by open source and commercial software product developers to test the security functionality of their software using source code analysis techniques to discover and eliminate vulnerabilities from large code bases.”[8]

Another key component of collaborative engagement in this area is the role of vendors, both in participation of upstream projects and with regard to the products that are widely used. For example, Red Hat’s Product Security team provides tools and security data to help security measurement[9]. Part of this commitment is our participation and leadership in various projects such as MITRE CVE and OVAL. We also provide reports and metrics, but more importantly, we also provide the raw data below so customers and researchers can produce their own metrics, for their own unique situations[10]. Red Hat shares all of its fixes with the relevant upstream projects, even when many of the underlying vulnerabilities were not discovered internally[11], This shows that emphasis on collaboration is essential.

[8] http://www.dhs.gov/science-and-technology/csd-sqa

[9] https://securityblog.redhat.com/2015/03/18/cwe-vulnerability-assessment-report-2014/

[10] https://www.redhat.com/security/data/metrics/

[11] https://securityblog.redhat.com/2014/10/08/the-source-of-vulnerabilities-how-red-hat-finds-out-about-vulnerabilities/

Conclusion

As NTIA is certainly aware, the questions posed in this matter are not unique to open source software, and the Administration has made clear that a policy of ‘technology neutrality’ is essential to the Government pursuit of the best strategy to meet its particular needs.[12]

There is already underway a discussion on this topic (and related topics) by a wide range of stakeholders, primarily through private sector community efforts, with appropriate collaborations with government in specific areas. New initiatives risk duplication or distracting from these on-going efforts. Efforts to educate and encourage stakeholders who may not already be involved could be beneficial.

Once, again, we appreciate this opportunity to provide our comments on the specific question posed in this Request for Comments. Please do not hesitate to contact us if we can provide further information or answer questions.

Contact:

Mark Bohannon
Vice President, Global Public Policy and Government Affairs
Red Hat
markb@redhat.com

Gunnar Hellekson
Chief Strategist
Red Hat US Public Sector
ghelleks@redhat.com

[12] MEMORANDUM FOR CHIEF INFORMATION OFFICERS AND SENIOR PROCUREMENT EXECUTIVES , “Technology Neutrality”, January 7, 2011.