8 FEB 2023 NEWS

#SOOCon23: UK Government Urges Industry Input on Software Security Policy

James Coker Deputy Editor, Infosecurity Magazine
Follow @ReporterCoker

The UK government is seeking industry views on how to regulate software security without stifling innovation.

Software provides huge economic benefits to the UK economy, through opportunities for innovation and better efficiency, said Naomi Gilbert, head of cyber resilience policy team at the Department for Digital, Culture, Media and Sport (DCMS), speaking during the State of Open Con 23 conference.

"The innovation and creativity stemming from software development is central to the strength of our tech sector," she noted.

Despite this, she noted that there are a number of challenges the UK is facing in securing its digital supply chain. A major component is the software used, including open source.

The UK government recognizes "that open source specifically is a fundamental driver of innovation in the UK and globally," Gilbert added. She also said that "the open source community is a crucial contributor to tech in the UK."

It is vital that any policy developed in this area is created in collaboration with this community and with this in mind, the DCMS recently issued a call for views on software resilience and security, which will run for 12 weeks. Gilbert explained that this details the government's views on the risks around software and possible policy solutions.

Regarding risks, Gilbert highlighted a number of high-profile supply chain cyber-attacks that were launched by targeting software. These included the Kaseya incident in 2021, where attackers injected malicious code into software that was spread through updates to customers.

Related to This Story

Applications Five Years or Older Likely to have Security Flaws

The Security Challenge of Open Source Software

Less Than Half of Organizations Have Open Source Security Policy

RSA Advisory Board Discuss Pressing Issues in Cybersecurity

Unraveling the Challenges of Log4j

"Many of the customers were managed service providers, which meant the attack spread quickly through the software supply chain to their customers as well," noted Gilbert.

Meanwhile, the Log4j vulnerability, uncovered at the end of 2021, highlighted "key transparency issues." Gilbert said that once the vulnerability was identified and made public, it became "low-hanging fruit" for threat actors, and over 800,000 attacks took place in just 72 hours afterwards.

Risk Framework Approach

Gilbert then demonstrated a government software risk framework. This revolves around six risk areas related to development, distribution and service provision, and the role of the customer. These issues are applicable to both open source and proprietary software.

Essentially, they encompass accidental vulnerabilities, malicious or intentional compromises and insecure development environments.

Gilbert highlighted that "the number of attacks targeting open source components is high and growing." Additionally, malicious actors are increasingly targeting open source repositories by creating malicious open source software packages that developers inadvertently include in their software.

Lack of maintainers, time and capacity pressures on the open source community and poor communication around vulnerabilities are particular problems in open source software, she added.

Gilbert acknowledged that "the open source community and industry are already taking some steps to introduce more tools and resources to support developers and maintainers." The government is now keen to look at how it can support these efforts and promote best practice in secure development, "without placing an unnecessary burden on developers and maintainers."

She set out a range of potential policy ideas that the government is keen to get industry feedback on.

To promote software development security:

- Accreditation of organizations and software packages
- Guidance e.g. a code of practice
- Development of an international standard
- Financial support for SMEs that follow best practices
- Support development of vulnerability scanning tools

To support the open-source community:

- Guidance on secure development in open-source
- Funding for industry-led initiatives
- Work with industry to develop tools
- Government-backed teams to maintain critical components

To promote transparency and communication:

- Regulation requiring a minimum standard of transparency
- Certification for vendors following best practice
- Secure information sharing mechanisms

What's Hot on Infosecurity Magazine?

Read Shared Watched Editor's Choice

1 9 FEB 2023 NEWS
Trio Arrested in COVID PPE Fraud Probe

2 9 FEB 2023 NEWS
New Info-Stealer Discovered as Russia Prepares Fresh Offensive

3 8 FEB 2023 NEWS
UK Politician's Email Hacked by Suspected Russian Threat Actors

4 8 FEB 2023 NEWS
#SOOCon23: UK Government Urges Industry Input on Software Security Policy

5 8 FEB 2023 OPINION
SMBs Should Increase Cybersecurity Investment Despite the Economy

6 8 FEB 2023 NEWS
BEC Attacks Surge 81% in 2022

- Guidance for vendors on promoting transparency
- Guidance on SBOMs and comparable tools
- Secure central database of SBOMs

Gilbert emphasized that these options are "neither exhaustive nor will all be feasible or practical to pursue."

Join the debate – sign up for Infosecurity Magazine's Online Summit to hear two pros go head-to-head on the validity of SMOBs.

She added that the government is especially keen to hear from the open source community on three key questions:

- What are the biggest issues impacting software security?
- What further action would help address these issues (government or industry)?
- How should government work with the open-source community to address these risks?

0 Comments

Login

Start the discussion...

LOG IN WITH OR SIGN UP WITH DISQUS

Name

Share Best Newest Oldest

Be the first to comment.

Subscribe Privacy Do Not Sell My Data

ALSO ON INFOSECURITY MAGAZINE

2 months ago • 1 comment
How to Overcome Challenges to ...

a month ago • 1 comment
The LastPass Breaches: Password ...

2 months ago
US Sue Over Cl Safety a

The Magazine
About Infosecurity
Subscription
Meet the Team
Contact Us
Cookies Settings

Advertisers
Media Pack

Contributors
Forward Features
Op-ed
Next-Gen Submission