v.linkedin.com/company/techinformed> < https://flipboard.com/@techinformed?utm_campaign=tools&utm_medium=follow&action=follow&utm_source=techinformed.com>

Tech Informed < https://techinformed.com>

The frontier of tech news

ADVERTISE < HTTPS://TECHINFORMED.COM/ADVERTISE/>

Search

Home < https://techinformed.com> Event News < https://techinformed.com/category/news-analysis/event-news/> Industry News < https://techinformed.com/category/news-analysis/industry-news/> News & Analysis < https://techinformed.com/category/news-analysis/> 'Switch to memory safe coding' White House CyberSec chief urges OSS developers

Event News

'Switch to memory safe coding' White House CyberSec chief urges OSS developers

February 8, 2023

The White House's assistant national cyber security director Anjana Rajan has urged the open source community to switch to safer programming languages such as Rust, Python and Swift – which, she claims, can dramatically reduce the odds of creating vulnerabilities in software.

While Open Source Software (OSS) is now ubiquitous and recognised as a huge driver in the software-based digital economy, numerous security breaches – culminating in the "apocalyptical" Log4Shell < https://techinformed.com/log4shell-threat-cloud-services-must-urgently-update-their-logging-software/> vulnerability – has spurred the Biden administration into liaising with the OSS community to come up with a series of mitigations.

This led to the formation of an inter-agency working group, the Open Source Software Security Initiative (OS3i) which Rajan – an engineer and cryptographer by trade – now co-leads.

The OS3i has a goal to convene with public and private entities across the open-source ecosystem to deliver policy solutions that will make OSS more secure.

The group spent most of last year identifying key risks, the results of which Rajan outlined at the *State of Open Source conference* at the Queen Elizabeth II Centre in Westminster today.

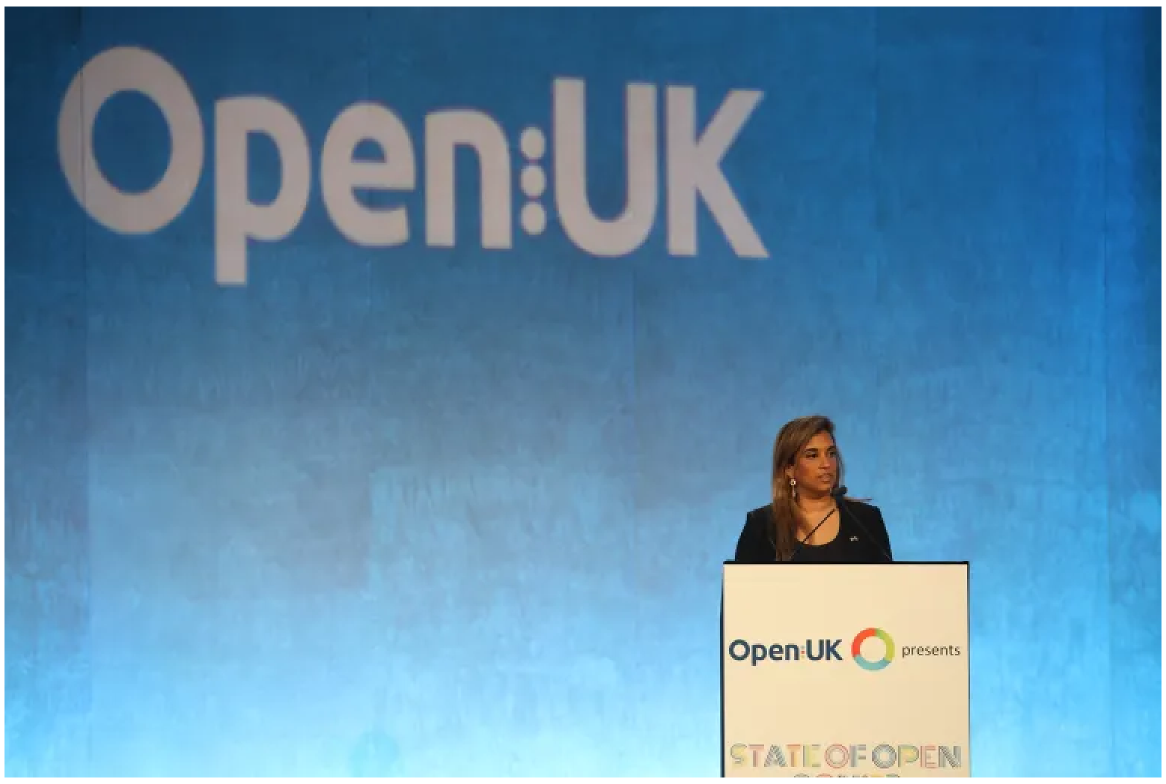
One key recommendation the US government is now advocating is that software developers ditch memory unsafe programming languages, such as C and C++, because they are the "leading cause of the world's software vulnerabilities".

Rajan gave a simple example of memory unsafe error: "Let's say I've enlisted 10 items. And I wrote a programme that called upon the eleventh item. We would reasonably assume that the program would return an error because the 11th item doesn't exist.

"But in a memory unsafe language the error-track doesn't happen by default. What happens instead is that it will return whatever value is current stored in its memory which means that you can read data that you shouldn't see; you can write data you shouldn't be able to change and you can access data that should be available."

"When you think about this at scale that's a pretty catastrophic situation from a cyber security perspective. You can write a programme to mitigate against these risks but all an adversary needs is to attack your system is just one memory unsafe bug."

Rajan added that the scale of this problem was "daunting" because across the US Government "so much of our programming language is written in C and C++ – including proprietary software too."



The White House's assistant national cyber security director Anjana Rajan speaking at State of Open Con 23

She claims that many of the big security hacks the world has seen over the last two decades – from the Slammer Worm DoS attack of 2003 to the WannaCry ransomware attack of 2017 – have been caused by what are now viewed as older, memory unsafe languages.

Mitigation

To mitigate risk, Rajan urged software developers to switch to 'memory safe' programming codes "as soon as possible". These include Rust (for operating system kernel); Go (for network servers); Python for data scientists and swift for iPhone apps.

Rajan maintains that switching to these memory safe languages has an "outsized impact" as research shows for software written in with this code can eliminate 70% of a software's critical vulnerabilities.

She added: "Every single cyber issue starts with a line of code. That means the most atomic unit of the software supply chain is the programming language itself. If the language is not safe, then nothing we build in that language is safe either.

"Advocating for adoption of memory safe languages is the single most impactful thing that government leaders around the world can do for our collective cyber security."

According to Rajan, the OS3i is currently leading an implementation strategy that involves looking at the technical debt across the global IT ecosystem and upgrade to memory safety.

Investment is another key area: according to Rajan the US government needed to "coordinate the diverse portfolio of funding opportunities available to support moves to memory safe coding", as well as funding and encouraging "research that eases the transition to memory safe programming languages.

She added that the government also needed to think about future threats – for instance, ensuring that the technologies underpinning digital currencies, smart contracts decentralised assets and web 3.0 were all memory safe.

CYBER SECURITY < HTTPS://TECHINFORMED.COM/TAG/CYBER-SECURITY/>

out?
https://techinformed.com/switch-
20safe%20coding%E2%80%99%20White%20House%20CyberSec%20chief%20urges%20OSS%20developers%20-
Share memory-safe-coding-white-
rmed.com%2Fswitch-to-memory-safe-coding-white-house-cybersec-chief-urges-oss-
house-cybersec-chief-urges-oss-
ign=tools&utm_medium=article-share&utm_source=techinformed.com>
developers/>

ABOUT THE AUTHOR

Ann-Marie Corvin