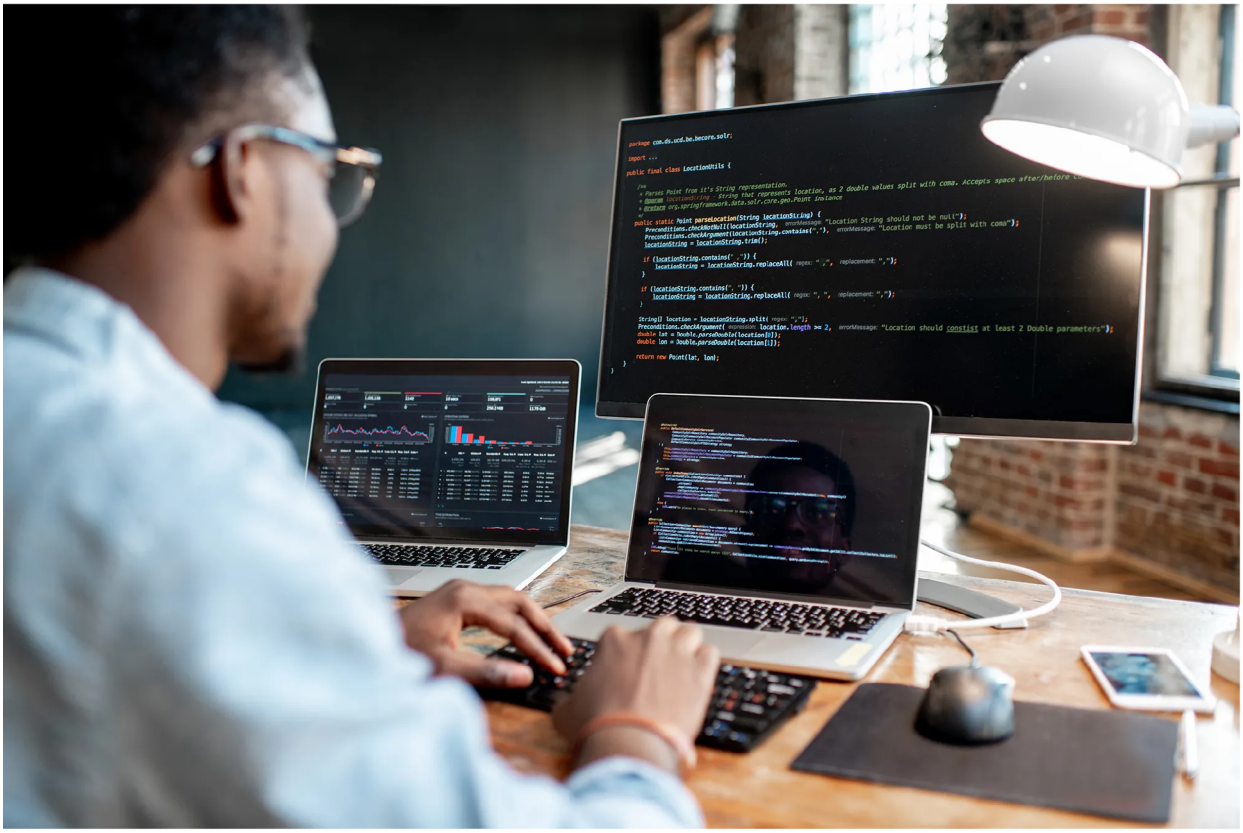
Newsletter | Cyber Bulletin

US Pushes Software Developers to Embrace Memory Safe Languages



Photographer: RossHelen/iStockphoto

By Cameron Fozi

July 9, 2025 at 1:27 PM EDT

Late last month, the federal government made another attempt to push software developers away from the programming languages C and C++.

While the two languages back much of today's technology, subtle programming errors can put cybersecurity and IT systems at risk.

In a 19-page report, the National Security Agency and the Cybersecurity and Infrastructure Security Agency made a pitch for software developers to embrace “memory safe languages” – such as Java and Python – to reduce computer mishaps.

It’s fairly technical stuff, but cybersecurity experts say memory management flaws have caused security breaches, system crashes and operational disruptions. That’s because the C and C++ programming languages give developers greater control over how and where computers store information. But that can lead to mistakes.

For instance, the Chromium projects, the Google-led effort behind the Chrome browser, has traced 70% of its “serious” security bugs to memory safety problems in code written in the two languages.

A Google spokesperson referred to previous statements on the issue. “Memory corruption vulnerabilities have been the standard for attacking software for the last few decades,” Google said in a statement in 2022. “It’s still how attackers are having success.”

In a statement last year, Google said it managed large code bases in other languages, but also hundreds of millions of lines of C++. Rewriting all its all C++, however, would likely remain "impractical,” the company said.

The report from CISA and the NSA noted that memory safety vulnerabilities have “long plagued” software systems. For instance, one such flaw, known as Heartbleed and discovered in 2014, resulted in the theft of sensitive personal data including millions of hospital patient records, according to the report.

Spyware used against a civil society organization exploited memory safety flaws, according to Citizen Lab.

US federal agencies have urged software developers to write in “memory safe languages” that give them less control over computers' memory storage but offer reduced risks. Such languages “manage the computer’s memory so the programmer cannot introduce memory safety vulnerabilities,” according to CISA.

“The importance of memory safety cannot be overstated,” according to the report from CISA and the NSA.

Even if everyone was game to switch, the transition would face obstacles.

Software developers who have built careers writing programs in C and C++ may be reluctant to switch. In addition, those languages are often faster than memory safe alternatives.

Stuart Madnick, a professor of information technology at the Massachusetts Institute of Technology, said such concerns have waned for many applications as computers have generally become faster and cheaper.

But there remain computer programs, he said, where the speed of C and C++ might still be especially advantageous. Some defense technologies, for one, depend on rapidity, he said. And even modest efficiency advantages could result in large savings for programs that demand lots of computing power, such as some artificial intelligence models, he said.

The government’s report said incremental change might be more feasible for organizations than scrapping all C and C++ code.

“When you're maintaining your existing code base, if you can, rewrite parts of it gradually in memory safe languages,” said Daniel Aranki, a cybersecurity expert and an assistant professor at the University of California, Berkeley. “It might take a bit longer than if you just stopped all development and did it all at once, but it's more of a practical and pragmatic approach.”

What We Learned This Week

Two Democratic lawmakers said election security staff at CISA are "afraid to work with state and local election officials and vendors for fear of retribution."

In a letter sent on Monday, Representative Joseph D. Morelle, a Democrat from New York, and Senator Alex Padilla, a California Democrat, said they were concerned about funding and personnel cuts. They sought "urgent updates" from CISA leadership on the status of numerous election security programs previously supported by the agency. Monday's letter was the fourth sent by the lawmakers.

"CISA's repeated failure to respond to our requests for information while undertaking a significant reshaping of the agency's personnel and mission is unacceptable," wrote the lawmakers. "We remain deeply troubled by the lack of information CISA has provided to congressional oversight committees and the lack of substantive responses to our questions."

"We're getting CISA back on mission as America's cyber defense agency," said Marci McCarthy, CISA's director of public affairs, in response to the lawmakers' questions. *–Patrick Howell O'Neill*

What We're Reading

- Musk's xAI working to remove Grok's 'inappropriate' posts.
- Gabbard's team has sought spy agency data to enforce Trump's agenda.
- The AI scraping fight that could change the future of the web.
- Iranian ransomware group offers bigger payouts for attacks on Israel, US.
- Chinese state-sponsored contract hacker arrested in Italy at US request, DOJ says.

Got a News Tip?

You can reach Cameron Fozi at cfozi2@bloomberg.net. You can also send us files safely and anonymously using our SecureDrop.

More from Bloomberg

Get Tech In Depth and more Bloomberg Tech newsletters in your inbox:

- Game On for diving deep inside the video game business
- Power On for Apple scoops, consumer tech news and more
- Screentime for a front-row seat to the collision of Hollywood and Silicon Valley
- Soundbite for reporting on podcasting, the music industry and audio trends
- Q&AI for answers to all your questions about AI

Contact us:
Provide news feedback or report an error

Site feedback:
Take our Survey

Confidential tip?
Send a tip to our reporters