

With the Rise of AI, Cisco Sounds an Urgent Alarm About the Risks of Aging Tech

 www.wired.com/story/cisco-aging-technical-infrastructure/

Lily Hay Newman

November 20, 2025

Aging digital infrastructure equipment like [routers](#), [network switches](#), and network-attached storage—has long posed a silent risk to organizations. In the short term, it's cheaper and easier to just leave those boxes running in a forgotten closet. But this infrastructure may have old, insecure configurations, and legacy tech is often no longer supported by vendors for software patches and other protections. As [generative AI platforms](#) make it easier for attackers to [find](#) and [exploit](#) vulnerabilities in targets' systems, the network tech company Cisco is launching an effort to raise awareness about the issue and promote improvements—both for ancient Cisco devices and products from other companies that are still in use.

Dubbed “Resilient Infrastructure,” the [initiative](#) includes research and industry outreach as well as technical shifts in how Cisco manages its own legacy products. The company says that it is launching new warnings for its products that are approaching end of life, so if customers are running known insecure configurations or attempt to add them, they will receive a clear and explicit prompt when they update a device. Eventually, Cisco will go a step further to completely remove historic settings and interoperability options that are no longer considered safe.

“Infrastructure globally is aging, and that creates a ton of risk,” says Anthony Grieco, Cisco’s chief security and trust officer. “The thing we’ve got to get across is this aging infrastructure wasn’t designed for today’s threat environments. And by not updating it, it’s fostering opportunities for adversaries.”

Research conducted for Cisco by the British advisory firm WPI Strategy looked at the prevalence and impact of end-of-life technology in the “critical national infrastructure” of five countries: the United States, United Kingdom, Germany, France, and Japan. The [study](#) found that the UK (followed closely by the US) faces the biggest relative risk of the group from widespread use of outmoded, legacy technology in key sectors. Japan had the lowest relative risk—thanks, the report says, to more emphasis on consistent upgrades, decentralization in critical infrastructure, and “a stronger, more consistent national focus on digital resilience.”

In general, the research also emphasizes that breaches and other cybersecurity incidents around the world regularly involve attackers exploiting known vulnerabilities that could be avoided through patching or upgrading end-of-life technology.

“The status quo is not free—there is actually a cost, it’s just not being accounted for,” says Eric Wenger, Cisco's senior director for technology policy. “If we can help elevate this risk to something that is treated as a board-level concern, then hopefully that will help to

underscore the importance of making an investment here.” As an industry, he adds, “we’re not making it hard enough for the attackers.”

Founded in 1984, Cisco has been a titan of network computing for decades, and its devices are deeply embedded in digital infrastructure around the world. To the extent that it may feel self-serving, then, for such a company to champion renewed spending on network equipment, Wenger points out that whether customers will choose to buy Cisco equipment again is a different question from whether they should upgrade at all.

“Look, we don’t make money on the stuff that we sold two decades ago. When we convince somebody that they need to move off of the old technology—what we’re selling now is innovative, it’s cost effective, but we’re not going to win everyone over,” he says. “But we need to start the conversation either way.”

Cisco's Grieco points out, too, that he and his colleagues have been attempting to highlight the risks posed by end-of-life technology for years. In an August 2016 Cisco blog post, for example, he [wrote](#), “Systems that were designed, built and deployed in decades past didn’t anticipate the hostile security environment of today. Until now, very few have thought about securing infrastructure because they didn’t think adversaries would target these systems and devices, or they had ‘higher priorities’ to fix. This must change.”

While generative AI platforms still can't devise and execute layered digital attacks on their own, evidence is mounting that AI tools are already making it quicker and easier for attackers to launch social engineering attacks, identify and exploit vulnerabilities, and refine malware. For attackers with little technical expertise, this can give them a crucial leg up, and for teams of highly skilled, well-resourced hackers, AI tools are helping to streamline some of the most labor-intensive aspects of attacks.

“It’s time to give people a jolt about the silent risk of aging infrastructure,” Grieco says. “We’re going to make it loud.”