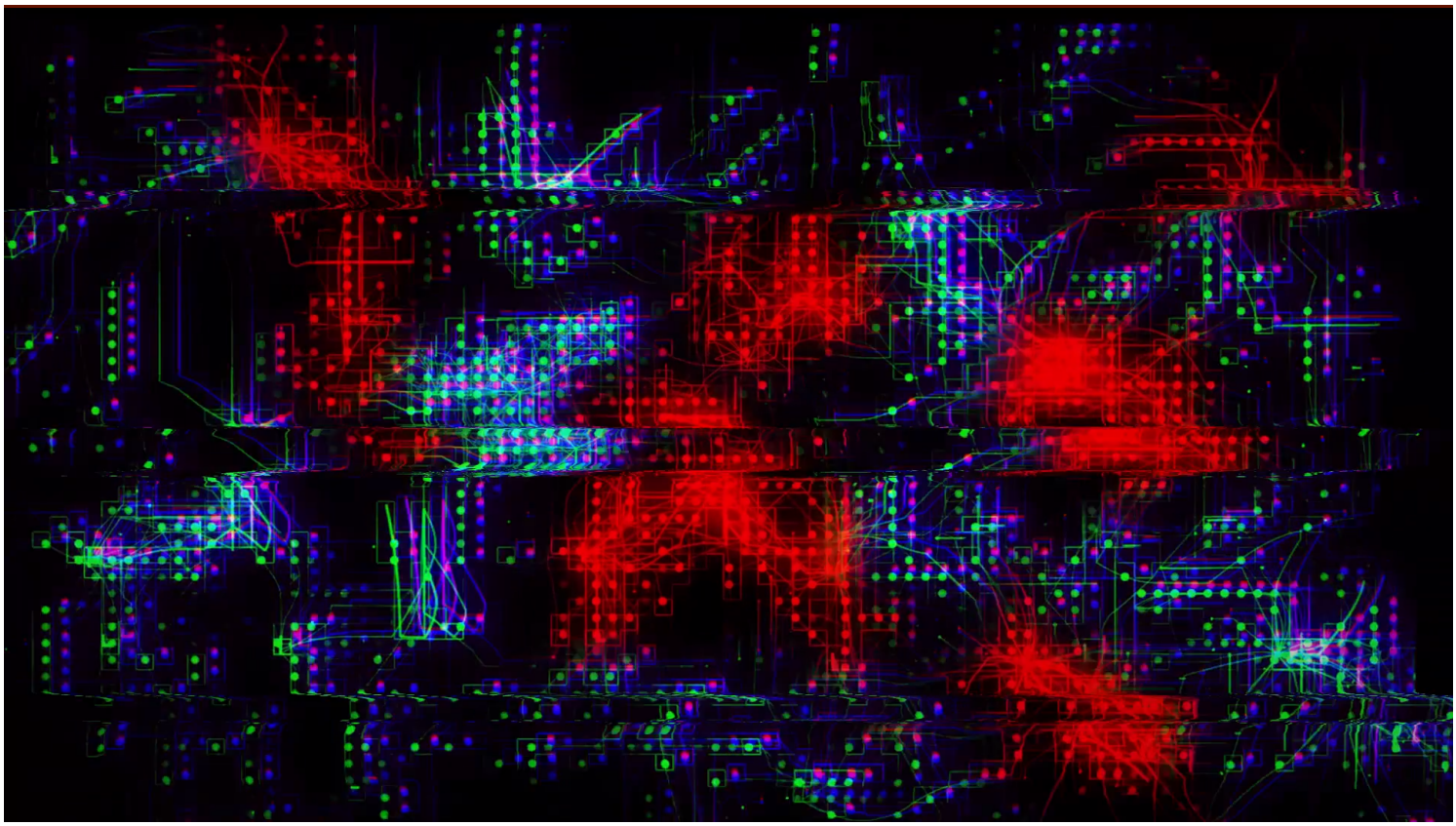


Researchers have found a way to break Cisco's secure boot process, which could affect millions of devices around the world. CASEY CHIN; GETTY IMAGES

LILY HAY NEWMAN SECURITY 05.13.19 02:24 PM

A CISCO ROUTER BUG HAS MASSIVE GLOBAL IMPLICATIONS

THE CISCO 1001-X series router doesn't look much like the one you have in your home. It's bigger and much more expensive, responsible for reliable connectivity at stock exchanges, corporate offices, your local mall, and so on. The devices play a pivotal role at institutions, in other words, including some that deal with hypersensitive information. Now, researchers are disclosing a remote attack that would potentially allow a hacker to take over any 1001-X router and compromise all the data and commands that flow through it.

And it only gets worse from there.

obtain root access to the devices. This is a bad vulnerability, but not unusual, especially for routers. It can also be fixed relatively easily through a software patch.

The second vulnerability, though, is much more sinister. Once the researchers gain root access, they can bypass the router's most fundamental security protection. Known as the Trust Anchor, this Cisco security feature has been implemented in almost all of the company's enterprise devices since 2013. The fact that the researchers have demonstrated a way to bypass it in one device indicates that it may be possible, with device-specific modifications, to defeat the Trust Anchor on hundreds of millions of Cisco units around the world. That includes everything from enterprise routers to network switches to firewalls.

In practice, this means an attacker could use these techniques to fully compromise the networks these devices are on. Given Cisco's ubiquity, the potential fallout would be enormous.

"We've shown that we can quietly and persistently disable the Trust Anchor," says Ang Cui, the founder and CEO of Red Balloon, who has a history of revealing major Cisco vulnerabilities. "That means we can make arbitrary changes to a Cisco router, and the Trust Anchor will still report that the device is trustworthy. Which is scary and bad, because this is in every important Cisco product. Everything."

Dropping Anchor

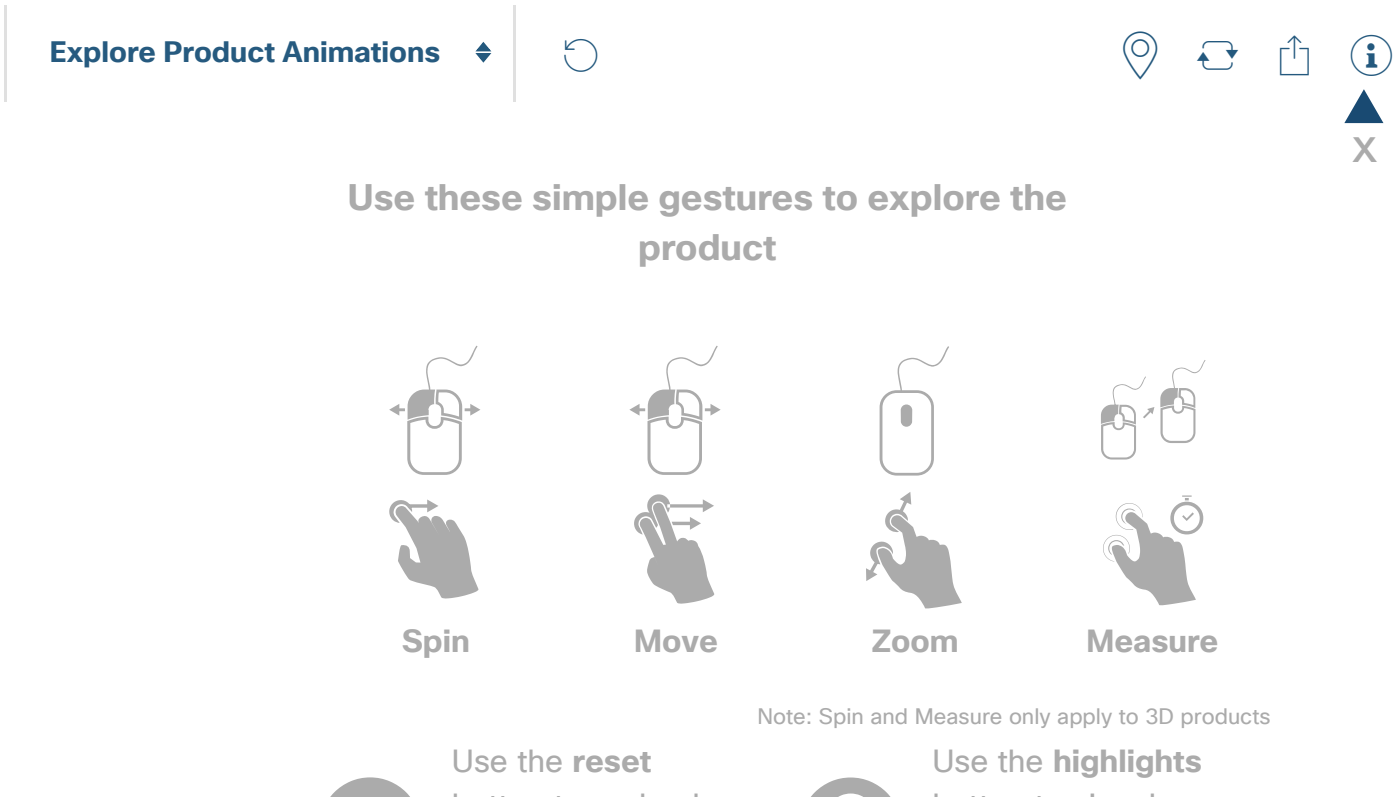
In recent years, security-minded companies have increasingly added "secure enclaves" to motherboards. Different solutions go by different names: Intel has SGX, Arm has the TrustZone, Apple has the secure enclave. And Cisco has the Trust Anchor.

They variously comprise either a secure part of a computer's regular memory, or a discrete chip—a safe, secluded oasis away from the bedlam of the computer's main processor. No user or administrator can modify the secure

everything else.

Secure-computing engineers generally view these schemes as sound in theory and productive to deploy. But in practice, it can be dangerous to rely on a sole element to act as the check on the whole system. Undermining that safeguard—which has proven possible in many companies' implementations—strips a device of critical protections. Worse still, manipulating the enclave can make it appear that everything is fine, even when it's very much not.

That's the case with the Cisco 1001-X. The Red Balloon team showed specifically that they could compromise the device's secure boot process, a function implemented by the Trust Anchor that protects the fundamental code coordinating hardware and software as a device turns on, and checks that it's genuine and unmodified. It's a crucial way to ensure that an attacker hasn't gained total control of a device.



On Monday, Cisco is announcing a patch for the IOS remote-control vulnerability the Red Balloon researchers discovered. And the company says it

disclosure. It also disputed that the secure boot vulnerability directly impacts the Trust Anchor. According to its security bulletin, all fixes are still months away from release, and there are currently no workarounds. When the patches do arrive, Cisco says, they will "require an on-premise reprogramming," meaning the fixes can't be pushed remotely, because they are so fundamental.

"As a point of clarification, Cisco advertises several related and complementary platform security capabilities," a spokesperson told WIRED in a written statement. "One of which that is relevant to this discussion is Cisco Secure Boot which provides a root of trust for system software integrity and authenticity. Another capability offered within certain Cisco platforms is the Trust Anchor module, which helps provide hardware authenticity, platform identity, and other security services to the system. The Trust Anchor module is not directly involved in the work demonstrated by Red Balloon."

Cisco seems to make a distinction between its "Trust Anchor Technologies," "Trustworthy Systems," and "Trust Anchor module," that may explain why it only considers secure boot to be implicated in the research.

The Red Balloon researchers disagree, though. They note that Cisco's patent and other documentation show that the Trust Anchor implements secure boot. If secure boot is undermined, the Trust Anchor is necessarily also defeated, because all of the tools are in a chain of trust together. You can see it visualized in this Cisco diagram.

"That's why they call it an anchor! It's not a trust buoy," Cui says.

The researcher group, which also includes Jatin Kataria, Red Balloon's principal scientist, and Rick Housley, an independent security researcher, were able to bypass Cisco's secure boot protections by manipulating a hardware component at the core of the Trust Anchor called a "field programmable gate array." Computer engineers often refer to FPGAs as "magic," because they can act like microcontrollers—the processors often used in embedded devices, but can also be reprogrammed in the field. That means unlike traditional processors, which can't be physically altered by a manufacturer once they're out in the world, an FPGA's circuits can be changed after deployment.

FPGAs pull their programming from a file called the bitstream, which is usually custom-written by hardware makers like Cisco. To keep FPGAs from being reprogrammed by mischievous passersby, FPGA bitstreams are extremely difficult to interpret from the outside. They contain a series of complex configuration commands that physically dictate whether logic gates in a circuit will be open or closed, and security researchers evaluating FPGAs have found that the computational power required to map an FPGA's bitstream logic is prohibitively high.

But the Red Balloon researchers found that the way the FPGA was implemented for Cisco's Trust Anchor, they didn't need to map the whole bitstream. They discovered that when Cisco's secure boot detected a breach of trust in a system, it would wait 100 seconds—a pause programmed by Cisco engineers, perhaps to buy enough time to deploy a repair update in case of a malfunction—and then physically kill the power on the device. The researchers realized that by modifying the part of the bitstream that controlled this kill switch, they could override it. The device would then boot normally, even though secure boot accurately detected a breach.

"That was the big insight," Red Balloon's Kataria says. "The Trust Anchor has to tell the world that something bad has happened through a physical pin of some sort. So we started reverse engineering where each pin appeared in the physical layout of the board. We would disable all the pins in one area and try to boot up

the bitstream.

The researchers did this trial-and-error work on the motherboards of six 1001-X series routers. They cost up to about $10,000 each, making the investigation almost prohibitively expensive to carry out. They also broke two of their routers during the process of physically manipulating and soldering on the boards to look for the reset pin.

An attacker would do all of this work in advance as Red Balloon did, developing the remote exploit sequence on test devices before deploying it. To launch the attack, hackers would first use a remote root-access vulnerability to get their foothold, then deploy the second stage to defeat secure boot and potentially bore deeper into the Trust Anchor. At that point, victims would have no reason to suspect anything was wrong, because their devices would be booting normally.

“The exposure from this research will hopefully remind the companies out there beyond just Cisco that these design principles will no longer stand as secure,” says Josh Thomas, cofounder and chief operating officer of the embedded device and industrial control security company Atredis. “This is proof that you can’t just rely on the FPGA to do magic for you. And it’s at such a low level that it’s extremely difficult to detect. At the point where you’ve overridden secure boot, all of that trust in the device is gone at that point.”

Even Bigger Problems

Thomas and the Red Balloon researchers say they are eager to see what types of fixes Cisco will release. They worry that it may not be possible to fully mitigate the vulnerability without physical changes to the architecture of Cisco’s

this attack.

LILY HAY NEWMAN COVERS INFORMATION SECURITY, DIGITAL PRIVACY, AND HACKING FOR WIRED.

And the implications of this research don't end with Cisco. Thomas, along with his Atredis cofounder Nathan Keltner, emphasize that the bigger impact will likely be the novel concepts it introduces that could spawn new methods of manipulating FPGA bitstreams in countless products worldwide, including devices in high-stakes or sensitive environments.

For now, though, Red Balloon's Cui is just worried about all of the Cisco devices in the world that are vulnerable to this type of attack. Cisco told WIRED that it does not currently have plans to release an audit tool for customers to assess whether their devices have already been hit, and the company says it has no evidence that the technique is being used in the wild.

But as Cui points out, "Tens of thousands of dollars and three years of doing this on the side was a lot for us. But a motivated organization with lots of money that could focus on this full-time would develop it much faster. And it would be worth it to them. Very, very worth it."

More Great WIRED Stories

- The hacker group on a supply-chain hijacking spree
- My search for a boyhood friend led to a dark discovery
- LA's plan to reboot its bus system using cell phone data
- The antibiotics business is broken, but there's a fix
- Move over, San Andreas: There's a new fault in town