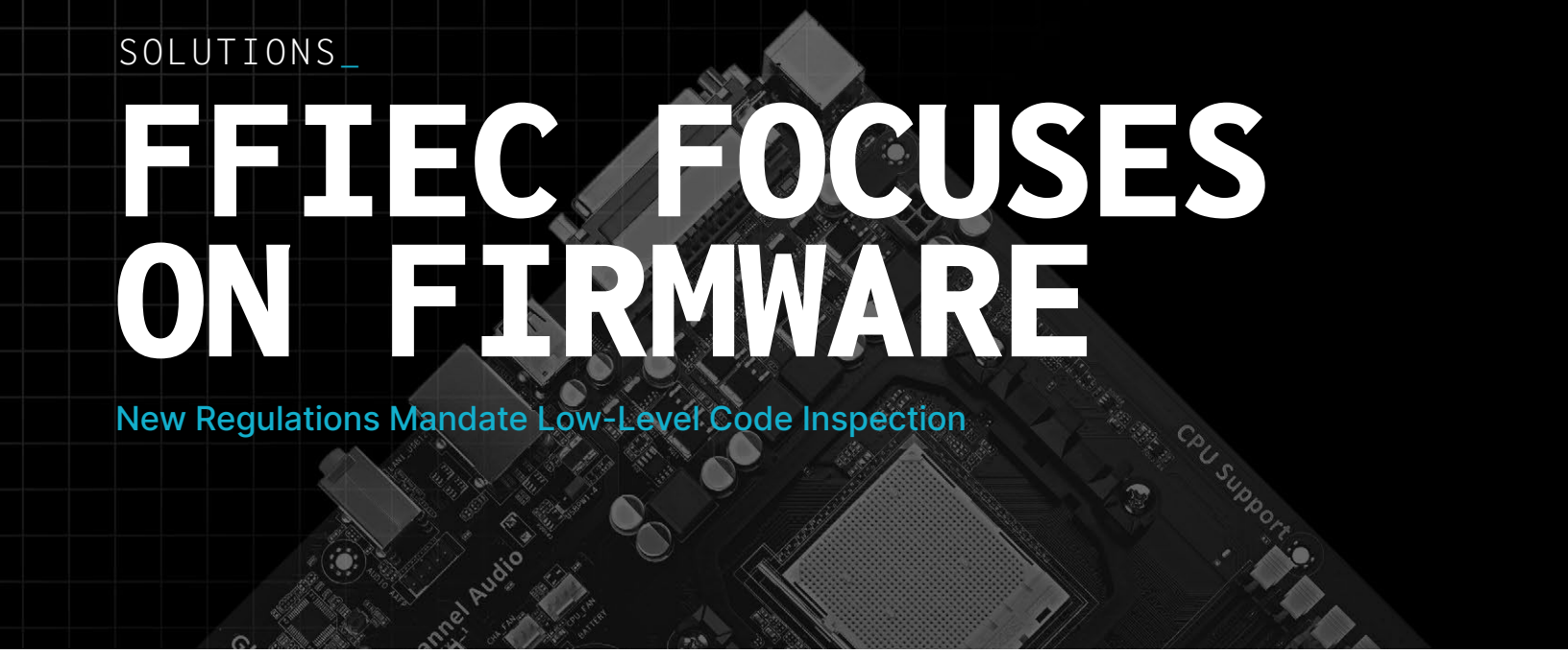
SOLUTIONS_

FFIEC FOCUSES ON FIRMWARE

New Regulations Mandate Low-Level Code Inspection



WHO SHOULD READ THIS_

Cyber security, infrastructure security, and audit leaders in any organization governed by FFIEC regulations, which includes all domestic and international banks, lenders, and credit unions.

WHAT THEY WILL LEARN_

How the foundational documents used by the FFIEC to regulate and audit cyber security controls, like the FFIEC IT Examination Handbook and Authentication and Access to Financial Institution Services and Systems, are forcing inspection and validation of hardware- and firmware-level code.

FURTHER READING_

- Case study, First Financial Fights Cyberattacks by Securing Their Firmware
- White paper, Need Secure Supply Chains? Start With Their DNA
- Solution brief, Zero Trust for Devices

When it comes to charting a course through waves of cyberattacks and storms of digital crime, no group may be better equipped or more influential than the FFIEC. The Federal Financial Institutions Examination Council is a formal U.S. government interagency body composed of six bodies that is "empowered to prescribe uniform principles, standards, and report forms to promote uniformity in the supervision of financial institutions". Founded in 1979 alongside new technologies like personal computing, the Internet, and mobile technologies, the FFIEC has taken point in defining the safeguards demanded of our society's rapid digital transformation.

> *"A technical vulnerability can be a flaw in hardware, firmware, or software that leaves an information system open to potential exploitation."*

In this changing landscape, the FFIEC IT Examination Handbook has become a de-facto standard in the financial services world for cyber security best practices. This document was updated in 2016 to include a number of references to "firmware", the low-level code shipped with computing devices like endpoints, servers and network devices: "A technical vulnerability can be a flaw in hardware, firmware, or software that leaves an information system open to potential exploitation."

Additional references were added to the Handbook that focus on the prioritization of firmware vulnerabilities and on managing and maintaining appropriate firmware configurations in the hardware used throughout a financial services organization.

In 2021 the FFIEC published new guidance on Authentication and Access to Financial Institution Services and Systems, which doubled down and again emphasized the need to assess and update firmware in network devices: "Network security devices and software are securely configured (e.g., implement firewall, router, or end-point security). Software and firmware are updated to address vulnerabilities."

> *"Software and firmware are updated to address vulnerabilities."*

But "firmware" – low-level control code inserted by manufacturers into their systems via persistent chips – has been around since the first personal computers. Why this sudden emphasis on the need to secure foundational code? There are two primary reasons:

- A marked increase in attacks coming through device supply chains
- The sheer power of firmware-level exploits to compromise systems and inflict organizational harm

STUBBORN SUPPLY CHAIN CHALLENGES_

Successful, damaging attacks on our digital supply chains have made headlines in recent years. By now, everyone has heard of the Solar Winds breach that delivered compromised code to up to 18,000 downstream customers of a major cyber security supplier. Most have also heard of the ASUS "ShadowHammer" attacks, where compromised code was delivered to up to 50,000 of the computer manufacturer's downstream customers.

But supply chain attacks have become far more frequent than these few oft-repeated examples: cyber security equipment makers like Fortinet and Pulse Secure have been caught in supply chain compromises. The largest vulnerability scare of 2022 – the Log4j vulnerabilities that have resulted in 10 million exploit attempts per hour in some cases – is focused on code libraries used extensively throughout our software and device supply chains.

The way to address the problem is better visibility and control over the code and devices that make up our digital supply chains. The FFIEC has mandated that this visibility and control extends not just to software libraries used in applications, but all the firmware and microcode that arrives with every new device the IT team unpacks:

- Every endpoint – whether laptop or desktop or "dumb" terminal – comes with 15-20 firmware componets, according to research from Gartner
- Every server comes with 30 or more firmware components to control inputs and outputs, drives, sound and video, chip functions, and more

Every network device, as we see with the Fortinet and Pulse Secure examples above, comes with firmware, and in most cases this is the only kind of code that makes the machine work – there's no other drive to store operating systems and applications

To complicate this problem, all this low-level code comes from different sources: chip makers, drive assemblers,

memory providers, drive manufacturers, and designers of specialized controllers. This plethora of device code comes from developers in different countries with different levels of oversight and with a different set of security best practices, which makes it critical to fully inspect and validate the structure and capabilities of this device-level firmware and software.

The new "firmware focus" in FFIEC guidance is simply recognition of a porous, fast-moving and previously invisible IT manufacturing process. This process not only makes "computer gear," but also creates and distributes the critical code that runs deep within the devices every financial services organization relies upon.

FIRMWARE BECOMES WEAPONIZED_

Every cyber security administrator, practitioner, and manager in a financial services organization is schooled on the TTPs (tactics, techniques, and procedures) of their cyber adversaries, whether those are enemies backed by nation-states or by criminal enterprises. What is new in this picture is the sheer destructiveness of some of the newer firmware-oriented tactics.

Because firmware is foundational code that has high privileges and is active before even the operating system boots up, compromising or damaging this code can irreversibly damage the IT equipment it supports. At the start of hostilities in the Russian campaign against Ukraine a new weapon was introduced: destructive wipers. Computers and network systems throughout Ukraine were inundated with code snippets bearing attacks that defensive teams labeled "WhisperGate", "WhisperKill", "GrimPlant", "IsaacWiper", or "HermeticWiper". These were a class of exploit called a wiper, a class of malware designed to erase the hard drive of the computer it infects, deleting data and programs and making the machine useless to defenders. And most of these wipers did their work at the firmware level.

Another class of highly destructive firmware-based weapons appeared at about this time: implants. In January 2022, an Iranian cyber security firm disclosed how threat actors were actively using BMC implants (baseboard management controllers, a component unique to servers) against HPE Servers in the wild. Known as iLOBleed, the implant affected HPE Gen8 and Gen9 servers and could not only continually erase the drives, but make these expensive and critical servers inoperative.

The FFIEC knew that if technologies like wipers or implants were used in the battlefield in Ukraine, they would soon be available for use against the banks and credit unions it protected. In a March 2022 meeting of the National Credit Union Association (NCUA), immediately following the start of Russia-Ukraine hostilities, NCUA chairman Chairman Todd Harper was direct in his warnings about these threats: "I cannot stress this enough: All credit unions and vendors, regardless of size, are vulnerable to cyberattacks." He also urged that "all parties within the system must maintain the highest level of alertness."

Firmware and low-level software code is clearly pervasive, as it appears in all our devices in increasing quantities, and it's incredibly destructive in its ability to "brick" or compromise systems from servers to network devices. These are the reasons the defense of firmware has come into focus at the FFIEC. But what should financial services organizations do about it?

A CHECKLIST FOR FIRMWARE LIFECYCLE MANAGEMENT_

Firmware is a mostly secret "black box" of encoded bits that tell hardware components, from chips to silicon to drives, how to act and when to do it. Operations teams have been hesitant to upgrade firmware because of the complexity and the fear of unknown downstream consequences –. Therefore in many cases firmware has been left unchanged, without upgrade, on even critical devices until they experienced end-of-life.

Fortunately, there are tools and best practices available for the inspection and protection of the previously-invisible firmware and microcode that runs throughout modern hardware. Today's practitioners use an Identify, Verify and Fortify process to ensure firmware is treated with the same kind of lifecycle management that other kinds of code receive.

- **Identify** - Discover, inventory, and classify your organization's devices and device-level firmware whether in endpoints, servers, network devices, or embedded and hard-to-track IT supply chains
  - Gain visibility: create a firmware inventory across the enterprise
  - Include firmware-level inspection of servers, VMs, endpoints, networked devices, connected devices

- Assess across vendors of all kinds
- Gain deep insight into hardware and software supply chains
- Assure IT has visibility down to the sub-OS hardware component level

- **Verify** - Validate current firmware and device configurations by comparing them against a database of known-good and up-to-date hardware and firmware profiles.
  - Verify for current firmware versions
  - Verify for appropriate and recommended firmware configurations
  - Maintain an always up-to-date database across the entire firmware ecosystem
  - Enable automated device scanning, analysis, and reporting of embedded code

- **Fortify** - Patch, configure, update and repair firmware as needed.
  - Automated remediation of vulnerable or misconfigured firmware components
  - Hardens systems in conjunction with existing patch, remediation, and threat analysis tools
  - Intelligent automation helps answer the questions “should I update” and “how do I update”?
  - Coordinate investigation and response via REST API
  - An update is available, but should you apply it?
  - Work with existing deployment and asset management tools, like Microsoft SCCM, Tanium, BigFix