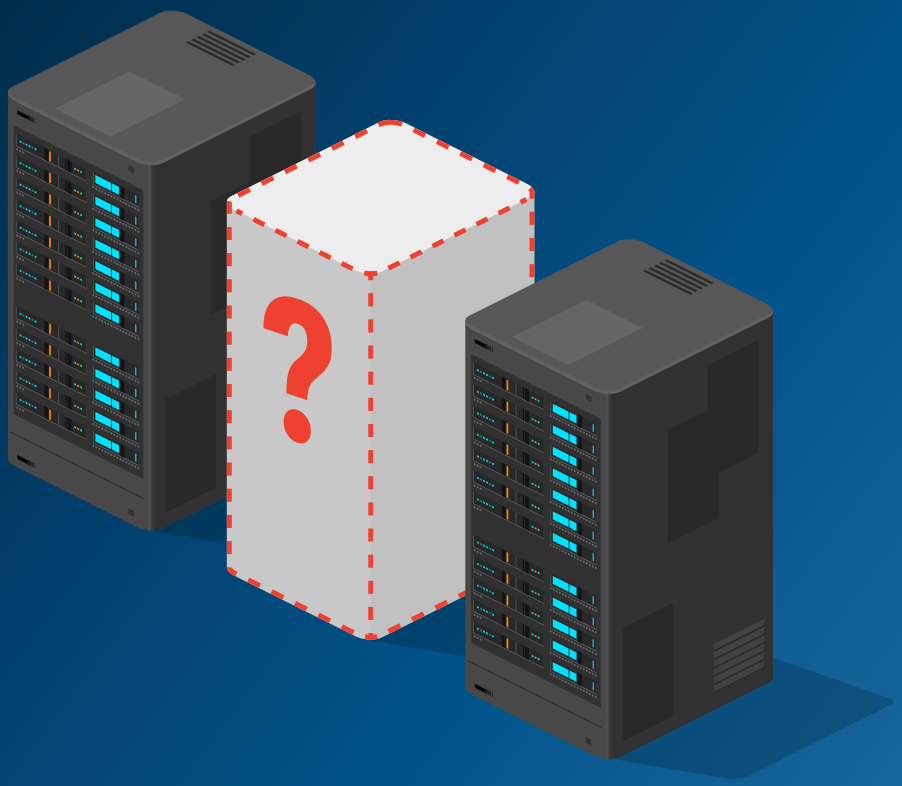


A SECURE SUPPLY CHAIN REQUIRES INDEPENDENT VISIBILITY INTO FIRMWARE

Once again, supply chain risks are in the news, with Bloomberg reporting attacks compromising servers via malicious firmware updates. While we don't have many technical details about the attacks reported in the Bloomberg article, the risk associated with the supply chain remains a serious concern for both the public and private sectors. Organizations today face ongoing attacks via compromised updates from SolarWinds, which itself comes after the disclosure of the ShadowHammer and CCleaner supply chain attacks. The technology supply chain underpins virtually every aspect of modern organizations, from software and services to their servers, switches, laptops, and virtual machines. Any compromise or vulnerability in the supply chain can serve as a modern-day trojan horse, bringing threats and risk into an organization under the guise of a trusted asset.

The firmware layer is often overlooked but is a single point of failure in devices and is the stealthiest way an attacker can compromise devices at scale. Taken together, a firmware attack in the supply chain ensures that the attacker's code is the first to run and has the highest privileges from the moment a device is first powered on. These techniques are in active use today, both by state-backed attackers as well as in widespread malware such as TrickBot. Like these examples, firmware supply chain attacks reported by Bloomberg are remote attacks, not requiring any sort of physical access.

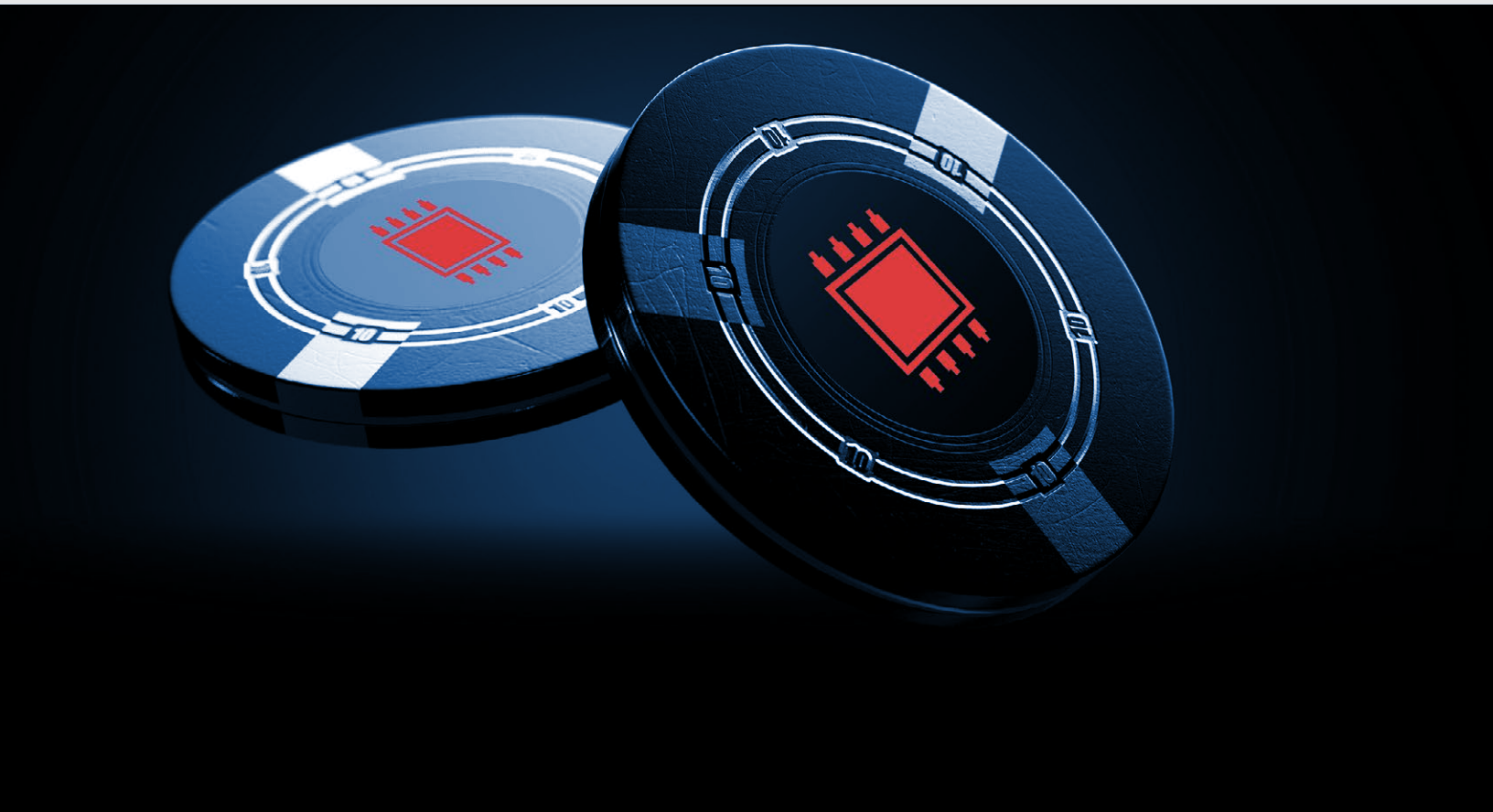
Understanding the risk and verifying the integrity of firmware in the supply chain presents unique challenges. OEM tools and capabilities vary widely depending on the vendor, model, and type of device in question, making it almost impossible for security teams to take a standardized approach. Furthermore, supply chain security introduces a more fundamental circular problem – **how can an organization trust a vendor's tools and checks when the vendor itself (or one of its upstream component providers) may be compromised?** This makes it critical for organizations to have an independent and consistent way to verify the integrity and posture of the firmware in their devices.

A HIGH STAKES GAME ALREADY IN PROGRESS

While the recent SolarWinds attack provided a painful demonstration of supply chain attacks and their impact, the risk has been ongoing. The recent Breaking Trust project documents over 130 supply chain attacks and disclosures, including firmware supply chain events affecting Lenovo devices, the Microsoft kernel, IoT devices, and peripheral components. Security teams must also be aware that the SolarWinds Orion platform itself has the ability to update firmware on critical systems and network devices. This means that many organizations are already in recovery mode and need to be able to actively validate the integrity of any recovered or replacement systems.

Organizations can and must address these challenges head on by taking the following steps:

- **Automate firmware security** – Managing and analyzing firmware can be a particularly technical and time-consuming task. Purpose-built firmware security tools can do the heavy lifting to automatically ensure device security without putting a burden on staff.
- **Verify the integrity of firmware** – Ensure that the firmware in devices has not been modified from the original vendor-approved firmware. Check firmware for signs of firmware threats. Pay special attention to verifying any newly acquired replacement systems or recovered systems following a supply chain attack.
- **Identify vulnerable firmware or misconfigured devices** – Vulnerable firmware can make devices susceptible to modification in the supply chain or after deployment. Identify any vulnerabilities on arrival, and incorporate firmware security posture as part of technology selection decisions.
- **Establish device baselines** – Gain visibility into firmware within devices and components and their behavior. This provides fine-grained visibility that newly acquired devices can be compared against, as well as during ongoing monitoring. Organizations can then track their progress towards securing their infrastructure and end user devices.



THIRD-PARTY VERIFICATION VS. SELF-REPORTING

Supply chain security has an innate need for third-party visibility and verification, and this is particularly pronounced when it comes to firmware. Technology vendors naturally play a critical role in supply chain security by developing secure systems that are resistant to tampering and developing tools and processes to verify the integrity of their products and suppliers.

However, customers can't simply rely on a vendor to verify their own integrity when the vendor itself may be compromised, or when the vendor can't provide enough component level resolution or analysis to effectively detect threats. At a minimum, organizations need the ability to independently assess their vendors' products and updates. **Without this ability, there is no "verify, then trust" (the modern-day premise for zero trust architectures), but only blind trust**. There are logical and technical reasons why security teams will need independent methods to verify their devices, including:

- **The threat may be "valid"** – The Sunburst attack against SolarWinds highlighted a key issue with supply chain security. Attackers were able to infiltrate the vendor and add malicious code into valid, properly signed software. In this case, even rigorously checking to see that code wasn't modified would not catch the problem because the code was modified before it was signed. This same core strategy was employed in the ShadowHammer attack against ASUS customers and in malware embedded in CCleaner software. This type of attack requires more sophisticated forms of detection than the simple integrity checks typically performed at a single point of time.

- **Self-reporting is unreliable** – If a system is compromised at the firmware level, its self-reporting function may be jeopardized. Most tools will simply query the resident operating system for information, which can be easily fooled. This makes it important to have multiple ways to directly verify the state of firmware and components.

HOW INDEPENDENT FIRMWARE VISIBILITY CAN HELP

- **Multiple independent perspectives** – A third-party solution gives a truly independent view into the device and its firmware. Purpose-built solutions use multiple perspectives and techniques to avoid deception from malicious implants.

- **Behavioral analysis** – When valid code is compromised, you can no longer rely on matching firmware to known "good" versions because the good is already compromised. Purpose-built tools can analyze the code and actions of firmware to identify heuristic signs of compromise that would not be seen based on signatures or whitelists.

MANY DEVICES, MANY COMPONENTS

The firmware layer presents a particularly broad attack surface for attackers to target. Every hardware device relies on firmware at some level, and the vast majority of devices will include components from an extensive and ever-changing network of suppliers, each with its own firmware.

This creates a daunting problem both in terms of supply chain security as well as ongoing management. Organizations should consider the following issues in the content of the firmware supply chain:

- **Many types of devices** – Any firmware can have vulnerabilities, and virtually all types of devices have had their firmware targeted in the wild. This includes laptops, servers, network devices and VPNs, and IoT devices. All of these devices may have different processes for acquisition yet must all be assessed in terms of supply chain security.

- **Many vendors with different tools** – Even when considering a specific type of device such as a laptop or server, an organization will typically have multiple vendors and use multiple models. The tools available to check or manage the firmware of a specific device will often vary not only between

vendors but also between individual models from a single vendor. This can make it almost impossible to establish a consistent approach to assessing and verifying the firmware of newly acquired or updated devices.

- **Many components and subsystems** – A single laptop, server, or network device typically consists of scores of components, systems, and subsystems sourced through a variety of suppliers developing their own firmware or sourcing it through other Nth party suppliers. Each component can have its own firmware that may be developed in-house or reused from open source projects. The Ripple20 vulnerabilities highlight how vulnerabilities in reused projects can permeate the supply chain and impact a wide range of devices.

HOW INDEPENDENT FIRMWARE VISIBILITY CAN HELP

- **Consistent coverage for critical enterprise devices** – Ensure that all types of critical devices can be checked for vulnerabilities and tampering, including laptops, servers, and networking infrastructure.
- **Consistent coverage across vendors and models** – Establish a consistent, automated way to assess many devices and vendors instead of relying on separate OEM tools or developing custom processes for each type of device.
- **Visibility into underlying components** – Newly acquired or updated devices should be assessed down to the component level to confirm integrity or identify vulnerabilities. Special attention should be paid to critical components such as motherboards, drives, network interfaces, BMCs, and add-on components.

SECURE YOUR SUPPLY CHAIN

Supply chain risk management is a challenging discipline because it forces organizations to closely consider and challenge where they have implicit trust. Historically, many organizations implicitly trusted that new devices they acquired were "clean" when they were unboxed or when updates were delivered. Attacks in the supply chain have demonstrated the fallacy of that assumption. Within a specific device, firmware is tightly bound to the root of trust of the device by controlling the boot process and potentially controlling all the code that runs after it.

ECLYPSIUM CAN HELP

To secure their supply chains, organizations must have the ability to assess and verify their technologies down to this fundamental firmware level. It is a process that should be performed consistently across vendors and devices and be performed independently. Eclypsium specializes in this area of cybersecurity and has helped many enterprises and technology vendors to better secure their supply chains. To learn more, contact Eclypsium at info@eclypsium.com.