Don't overlook device integrity

Securing what is below the operating system helps uncover vulnerabilities, bolster supply chain security

Protecting devices all the way down to the firmware and hardware level adds a critical, yet often overlooked, layer of protection to an organization's supply chain.

There are multiple types of supply chain attacks that can affect an organization's ability to operate effectively and deliver on its mission. Software and hardware are often targets for attack, but different components within a device are also vulnerable.

Typically, an organization will "put devices under management and look for vulnerabilities" in order to improve their security posture, said John Loucaides, VP, R&D, Eclypsium. There are probably hundreds and thousands of end points or user systems that are included in this scenario.

This approach, however, can miss the dozens of additional components that run their own operating systems which can be as big and complicated and "have the same problems as the one you are managing for the end user to use," he said.

These include different hardware devices that are part of the motherboard, the out-of-band management devices, the network card, the hard drive, and the processor's microcode. These all have an operating environment that supports the activities of host operating systems, and attackers know this.

"As we over the last few decades beefed up the attention and security

"As we over the last few decades, beefed up the attention and security of the host operating system, it's become easier for an attacker to target the hardware and firmware below the operating system."

– JOHN LOUCAIDES, VP, R&D, ECLYPSIUM

Article Source: FCW Supply Chain Workshop | January 19, 2021

SPONSORED BY :

eclypsium

of the host operating system," he said, "it's become easier for an attacker to target the hardware and firmware below the operating system."

Firmware is a favored target because when attackers try to destroy a device at the motherboard level, they can remain unnoticed even after a reboot, restore and hard drive replacement. It also gives them higher privilege than the regular operating system would, and allows them to evade host security controls.

It's easy for attackers to do this because the attack surface overall includes different operating systems, software, applications and network stacks located in each one of the different components inside a device.

"So if you have an operating system with thousands of device drivers and libraries, each of which has a software supply chain problem of its own, you now take all that and multiple that dozens of times and that is what is inside the box," Loucaides said.

At any point in the process,s the device could be tampered with or have a vulnerability. "The problem here is that no one is looking," he said. "At the end of the da, this stuff flies under the radar because it is part of the assumptions of an operating system."

> **"Understanding what you have allows you to start finding vulnerabilities, moving that watermark of where the environment is just a little bit better one step at a time."**
>
> **– JOHN LOUCAIDES, VP, R&D, ECLYPSIUM**

Organizations have to establish visibility, find and fix vulnerabilities, and detect threats and compromises, he said. Eclypsium helps organizations do this by managing and protecting devices down to the firmware and hardware level in their supply chain and beyond.

The company starts by building a database of devices and the components inside those devices. That helps determine risk in the form of vulnerabilities and updates, to create a cycle of risk management, and provides indicators of compromise for a known attack and integrity failures that show something has been tampered with. It also detects anamolies.

Every organization should keep track of what version of firmware and what manufacturer model they're using. "Understanding what you have allows you to start finding vulnerabilities, moving that watermark of where the environment is just a little bit better one step at a time," Loucaides said.

Eclypsium also is working with NIST on supply chain security to help identify different areas where manufacturers can disclose and share information on what their subcomponents should look like. This allows agencies to verify that the system as a whole hasn't been tampered with.

As organizations buy the most secure devices they can, and establish their baseline and risk management process by informing it at the component level, they will be better able to respond to incidents.

"You still have all sorts of problems above the OS, you still have network issues," he said. "All those things are important, but this way you cannot miss everything below the OS."

SPONSORED BY :

eclypsium®

Thank you for downloading this Eclypsium article! Carahsoft is the Master GSA Distributor for Eclypsium Cybersecurity solutions available via ITES-SW, MHEC, NJSBA, and other contract vehicles.

To learn how to take the next step toward acquiring Eclypsium solutions, please check out the following resources and information:

For additional resources:
carah.io/EclypsiumResources

For upcoming events:
carah.io/EclypsiumEvents

For additional Eclypsium solutions:
carah.io/EclypsiumSolutions

For additional Cybersecurity solutions:
carah.io/Cybersecurity

To set up a meeting:
Eclypsium@carahsoft.com
888-662-2724

To purchase, check out the contract vehicles available for procurement:
carah.io/EclypsiumContracts