SUPPLY CHAIN SECURITY FOR 5G NETWORK INFRASTRUCTURE

THE CHALLENGE OF SECURING 5G INFRASTRUCTURE_

The recent collision of technological advances and global, socio-economic crises have pushed 5G networks to the front of the line for technology strategies. Many business plans, supply chain resiliency initiatives, and go-to-market opportunities rely on dependable and trusted 5G networking to succeed. At the same time, the complex 5G landscape has been actively targeted by financially motivated and nation-state cyber adversaries, raising security concerns from security strategists and compliance teams. Traditional risk assessment approaches do not provide a view of the risk 5G infrastructures may face, because they do not include visibility into the lowest layers of manufacturer-created software, firmware and hardware code.

Research has shown, however, that attackers have already pivoted to this layer of technology. Exploiting chip-level software and firmware is now their preferred approach to maintaining persistence, bypassing security measures, and disrupting operations. The increasing complexities of the 5G supply chain continue to expand these opportunities. To defend against this level of attack, deeper visibility into the lower layers of a device hardware is required, and traditional methods for securing these lower layers generally do not scale to a wide variety of manufacturers all over the world. A new approach maximizes both the depth of analysis and the breadth of support for this low-level code in software and firmware, enabling a wide variety of options for infrastructure and supply chain resiliency while allowing practitioners to quickly detect and respond to threats.

WHO SHOULD READ THIS:

Cybersecurity leaders, including CISOs and CIOs, in telecom and 5G manufacturing; security and network architects; teams responsible for infrastructure security or network security who are planning and executing projects dependent on 5G technologies.

WHAT THEY WILL LEARN:

How and why 5G networks require strong chip-level supply chains, how the lowest level of hardware security is essential for network resiliency, and how these principles need to extend down to the network's underlying chips, processors and system components.

FURTHER READING:

Eclypsium white paper, "Need Secure Supply Chains? Start With Their DNA"

Eclypsium Platform Overview product brief

Satellite networks under attack blog post, "Defending Firmware in the Firmament"

HARDWARE-BOURNE FIRMWARE AND SOFTWARE IS UNDER ATTACK_

As organizations have improved their abilities to patch, update, and mitigate OS- and application-level vulnerabilities, adversaries have dug deeper into the stack to find their toehold. Firmware backdoors and implants have been a tool of choice for sophisticated attackers for years, but in recent years firmware threats have become far more widespread due to the ready availability of tools, firmware knowledge, and a wealth of vulnerabilities for attackers to target.

- VPN and Networking Vulnerabilities Targeted in APT and Ransomware Campaigns: In 2022, VPN vulnerabilities were a top target of state-sponsored actors most notably from China, Russia, and Iran, and ransomware campaigns including REvil, Sodinikibi, NetWalker, and Maze. These vulnerabilities often directly involve the firmware of networking devices and have quickly been exploited by attackers after discovery.
- The widely attacked CVE-2019-19781 affects the firmware of Citrix devices: attackers quickly began exploiting the vulnerability in January 2020 after it was disclosed in December of 2019.
- Other vendors have been targeted including Cisco, Pulse Secure, and F5: these attacks took advantage of the increased need to support employees working from home and provided attackers with an ideal way to deliver malware to enterprise users.

VULNERABILITIES AND BREACHES IN HARDWARE SUPPLY CHAINS_

Unfortunately, there are many examples of breaches in the technology supply chain. The Breaking Trust project provides a detailed analysis of 115 supply chain attacks and disclosures over the past ten years. Of note, backdoors have been found in enterprise firewalls, Huawei telecom gear, and even IP security cameras. Supply chain concerns are increasingly causing governments to ban certain technologies in sensitive areas or critical infrastructure.

Threats can also infiltrate the supply chain in the form of updates. In the recently disclosed SUNBURST campaign, attackers were able to compromise the software update infrastructure of SolarWinds Orion software in order to deliver a malicious backdoor to over 18,000 SolarWinds customers. In the case of the ShadowHammer attacks, attackers were similarly able to compromise ASUS's Live Update servers, which led to the company unwittingly pushing malware to hundreds of thousands of customers.

The supply chain also introduces new vulnerabilities. System components are often chosen based on price as opposed to security. Even worse, counterfeit devices such as fake Cisco gear are quite common and typically contain a wide array of vulnerabilities. Even firmware within valid components will often contain vulnerabilities that can easily be passed on and reused within a variety of products. For example, the Ripple20 vulnerabilities refer to a set of vulnerabilities found within a widely used TCP/IP software library. Over 30 vendors reused this code in devices ranging from laptops and servers to printers, medical devices, and critical infrastructure.

NIST and the National Cybersecurity Center of Excellence (NCCoE) have made Supply Chain Risk Management (SCRM) a top priority. The NCCoE recently published the Supply Chain Assurance project, and provided details in the document Validating the Integrity of Computing Devices. This report, co-developed by Eclypsium along with experts from Intel, HP, Dell, RSA and others, defines the risks associated with modern technology supply chains. It aims to develop example security solutions to verify that the devices and components have not been altered during manufacturing or distribution.

SPECIAL 5G THREATS_

What sort of threats require special consideration in 5G infrastructure?

- **Hardware Supply Chain Risk (Counterfeit, Substitution, Sabotage)**
  Given the difficulty with finding trusted manufacturing, transportation, and distribution, adversaries may not find a significant barrier to attempts to alter hardware physically as it moves through component and system level design, manufacturing, transport, and deployment.

©2024 Eclypsium, Inc

- **Firmware and Software Supply Chain Risk**
  Like IT environments, the firmware of 5G communication infrastructure contains software libraries that are subject to the same vulnerabilities and deliberate subversions as other software. At the time of manufacture or deployment, such issues may not have been known, and updates will be needed to correct vulnerabilities that are subsequently discovered.

- **Update Risks**
  In addition, attackers sometimes target the update process to form a pervasive software supply chain compromise. Regardless of the source, vulnerabilities or compromise of these software components will affect not only a single device or model/series of devices. These issues regularly affect many models from many manufacturers that were released over many years.

- **Physical Access Tampering**
  Once deployed, much of the infrastructure will require physical proximity to large groups of people in order to meet the demand for high bandwidth and low latency. While some locations may offer good physical protections, the expected deployment of 5G devices will likely exceed what can be secured physically. Whether opportunistic breakdown of procedures or sophisticated attacks break the security boundary, the resulting physical access hides from most monitoring techniques and leaves systems compromised.

- **Common Vulnerability and Exploitation**
  Regardless of supply chain, the usual bugs in software and firmware continue to affect all manner of computing platforms. New techniques leveraging common and difficult to eliminate microarchitectural side channels are starting to become better understood. Organizations can expect to see such issues manifest in terms of both 0-day exploits and novel exploits based upon older vulnerabilities that remain unpatched across many systems.

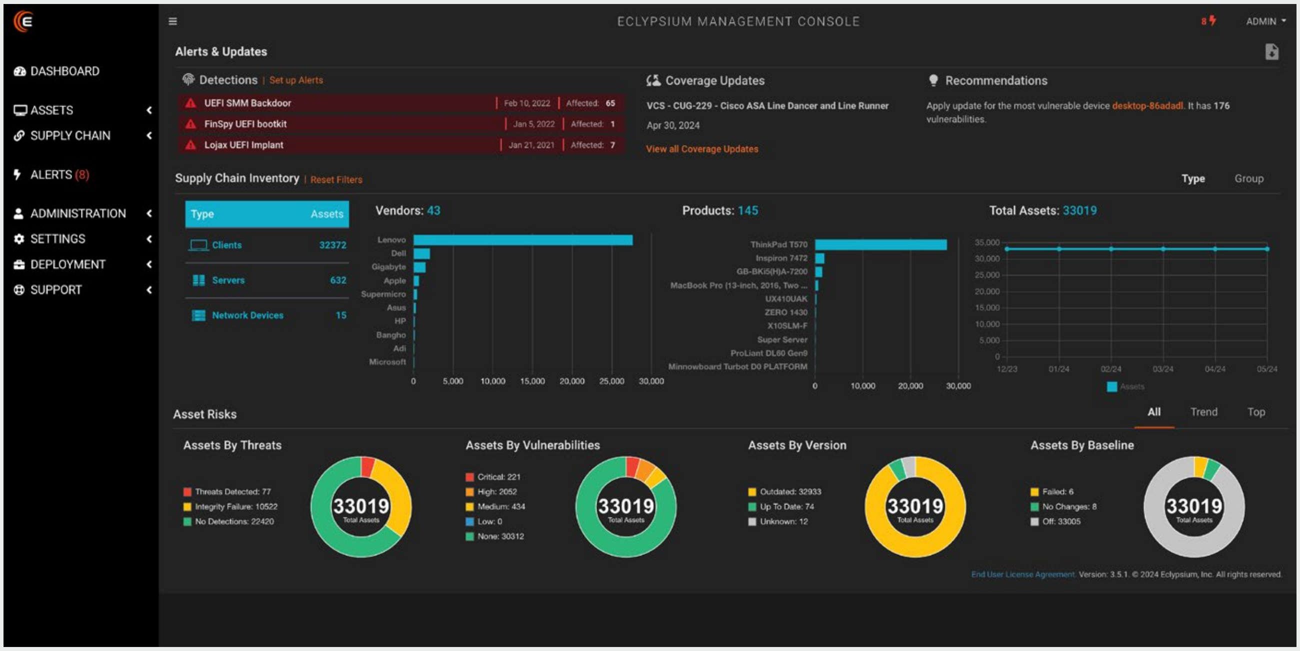
A CHECKLIST FOR SECURING FIRMWARE AND HARDWARE_

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 are often hesitant to upgrade firmware because of the complexity and the fear of unknown downstream consequences, and so in many cases firmware has been left unchanged, without upgrade, on even critical devices until they experience 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 need an Identify, Verify and Fortify process to ensure firmware is treated with the same kind of lifecycle management that other kinds of code receive.

Eclypsium has built this approach and this expertise into the Eclypsium Platform: the world’s first security solution purpose-built to identify, verify and fortify the low-level firmware and software embedded in the chips, processors and technology components that enable 5G networking.

- □ **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



UEFI SMM Backdoor	Feb 10, 2022	Affected: 65
FinSpy UEFI bootkit	Jan 5, 2022	Affected: 1
Lojax UEFI Implant	Jan 21, 2021	Affected: 7

VCS - CUG-229 - Cisco ASA Line Dancer and Line Runner
Apr 30, 2024
View all Coverage Updates

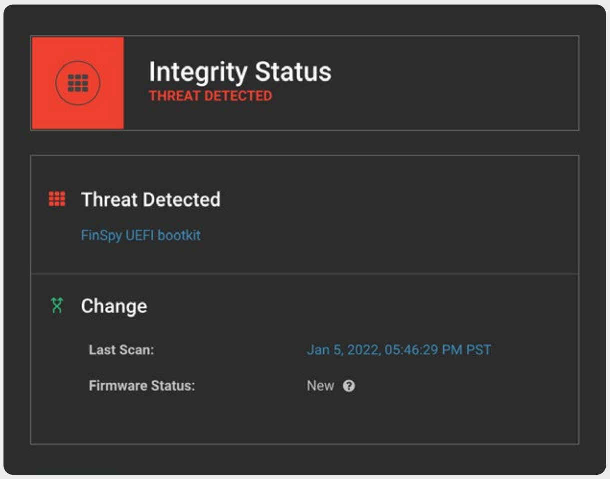
Apply update for the most vulnerable device desktop-86adadl. It has 176 vulnerabilities.

Type	Assets
Clients	32372
Servers	632
Network Devices	15

End User License Agreement. Version: 3.5.1. © 2024 Eclypsium, Inc. All rights reserved.

Identifying organizational firmware through a centralized dashboard

- □ **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
  - □ Gain deep insight into hardware and software supply chains
  - □ Enable automated device scanning, analysis, and reporting of embedded code



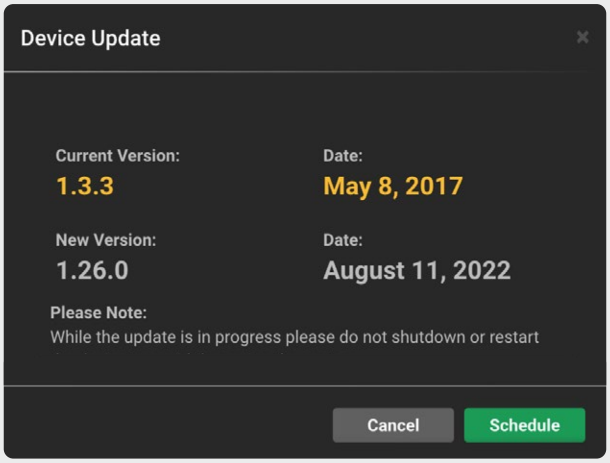
Integrity Status
THREAT DETECTED

Threat Detected
FinSpy UEFI bootkit

Change
Last Scan: Jan 5, 2022, 05:46:29 PM PST
Firmware Status: New

New requirements establish the need to Verify embedded device firmware is free from implants and back doors

- □ **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?



Device Update

Current Version: 1.3.3
Date: May 8, 2017
New Version: 1.26.0
Date: August 11, 2022
Please Note:
While the update is in progress please do not shutdown or restart

“Fortifying” firmware means patching and updating as need, using automated tools and processes

ABOUT ECLYPSIUM_

Eclypsium is a supply chain security platform that enables organizations to build trust in every device by identifying, verifying and fortifying software, firmware and hardware throughout enterprise IT and OT infrastructure, including all third-party components. Eclypsium’s SaaS platform provides comprehensive visibility into every device, discovers vulnerabilities, ensures integrity, and enables management of critical updates across entire device fleets.

©2024 Eclypsium, Inc