eclypsium

BELOW THE SURFACE

# THREAT REPORT

## SUMMER 2023

NETWORK INFRASTRUCTURE UNDER CONTINUED ATTACK

TETRA:BURST

UNINTENTIONAL THREATS: LEADERSHIP

AND MORE ...

# TABLE OF CONTENTS_

# BELOW THE SURFACE_

## SUMMER 2023

Welcome to the Summer 2023 edition of the Below the Surface Threat Report.

During a summer of wildfires and hot weather, we have seen how the threat landscape has expanded and vulnerabilities targeting the supply chain are not slowing down. When it comes to ransomware and criminal actors, we'll look at how incidents affecting the IT supply chain are rapidly resulting in material impact and class-action lawsuits, and we'll dive into how the patch for the BlackLotus UEFI bootkit campaign isn't enough to mitigate threats that can bypass Secure Boot going forward.

Then there is the recently uncovered backdoor in Gigabyte that presents IT Supply Chain Risk for customers of millions of devices, the TETRA:BURST vulnerabilities in mission-critical communications and the ever increasing attacks on network infrastructure.

We have also rounded up the latest federal regulations, including NIST CSF 2.0 Draft, CISA's UEFI security recommendations, the National Defense Authorization Act for 2024, and updates related to CJIS compliance.

As the cybersecurity landscape continues to evolve, it's crucial to stay informed and proactive in defending against emerging threats. We hope this report provides you with valuable insights and strategies to enhance your organization's security posture.

If you're not already subscribed to Below the Surface, you can do so at Eclypsium.com.

# THREAT LANDSCAPE

# IT Supply Chain Rocked by Ransomware Causing Material Impact to Third Parties

A recent spate of ransomware activity has been targeting IT supply chain victims, exposing them to material impact and in some cases, class-action lawsuits. The net impact of these incidents is both diverse and far-reaching, with victims experiencing impacts to productivity, financial accounting, third-party impacts both up and down stream, lawsuits, and public exposure of their most sensitive IP including source code, private signing keys, development frameworks and tooling, documentation, and customer and business data.

Examples include **Western Digital**, **MSI**, **Acer**, and others. In the case of AMI's source code leak, the ransomware incident itself began with one of two ransomware attacks hitting Gigabyte, which further impacted Intel and Nvidia as well.

Beyond just the impact of losing IP in the form of source code, the Gigabyte event also resulted in significant vulnerabilities discovered within that source code, some allowing for remote code execution over the Internet. This presents further cyber risk impact to data centers worldwide. In similar fashion, private keys stolen during a ransomware incident targeting MSI resulted in the weaponization of leaked private certificates within a week of the data being leaked.

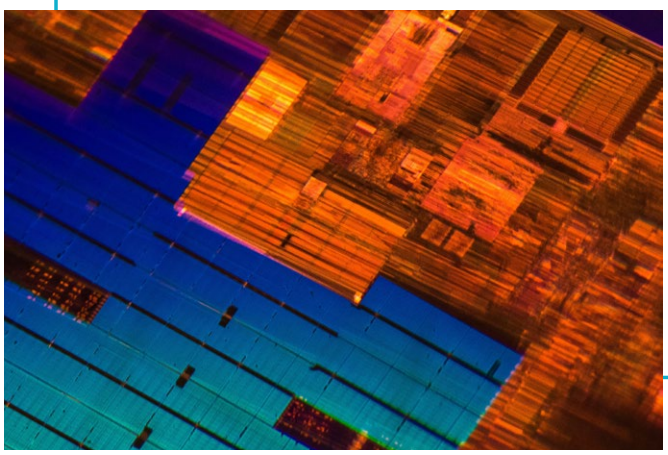


*Photo by Jason Leung on Unsplash*

In another case, MKS was hit by a ransomware attack that resulted in $200m of material impact they reported to the street, while their downstream customer, Applied Materials, reported a projected $250 million impact in the subsequent quarter following the incident. There is already a class-action lawsuit resulting from the MKS incident. The incident affected their shipping, manufacturing, website availability, order management and even their ability to report financial results ahead of their quarterly shareholder call.

In July, TSMC, the world's largest chip manufacturer, was also affected by a ransomware attack on one of its supply chain partners, Kinmax Technology. However, the attackers also posted screenshots that would suggest access to internally facing applications and credentials for other internal systems, and further threatened to leak remote login credentials to TSMC's networks. Screenshots in a tweet (since deleted) initially showed access to a TSMC ESXi environment. Kinmax also supplies to other top tier IT suppliers Aruba, Checkpoint, Cisco, Citrix, Fortinet, Hewlett-Packard Enterprise, Microsoft, and VMware. The ransom being demanded is $70m, one of the highest ever recorded, alongside the demand for ACER to pay $50m, and Kaseya's $70m ransom. In all three cases, attackers enjoyed the additional leverage that comes with the territory when attacking victims that are a part of the IT supply chain.

The IT supply chain will soon need to adapt to both regulatory and legal forces, as the impacts of such ransomware events and their downstream disruption and/or cyber impact directly exposes third parties to increased risk and the potential for material impact. A case that is unfolding as you read this is a class-action lawsuit against IBM for the massive MoveIT extortion campaign still in progress.

Looking forward, it won't just be ransomware events that prompt class-action lawsuits, but also vulnerabilities found in the IT supply chain that cause long-term exposure to data theft and/or significant impacts to performance when patched, such as the latest Downfall processor bugs that may impact performance between 39-50% across billions of devices. A class-action lawsuit is already being assembled.

- Attacks on the IT supply chain continue to rise in both intensity and resulting impacts. The impacts run the entire gamut: extortion payments, source code and development tooling leaks, IP leaks, impacts to third parties up and down the supply chain, increased exposure of vulnerabilities found via analysis of leaked source code, and material impact to victims and 3rd parties, with accompanying lawsuits.

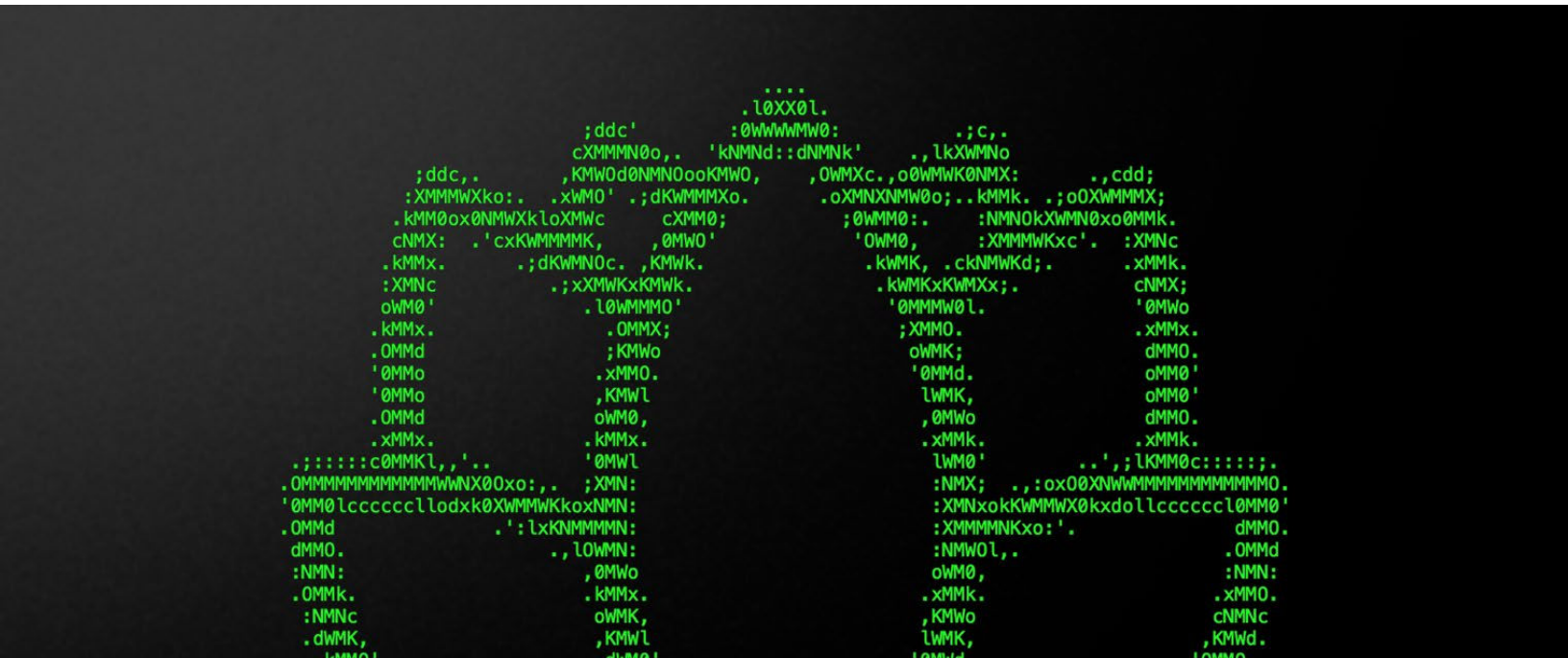
- Organizations should take a proactive approach to mitigating these threats by being able to rapidly assess and patch affected devices in operational environments, find implants and backdoors in associated firmware, and require their upstream suppliers to do the same due-diligence to bring supply chain verticals up to parity in their protections and acceptable risk models.

# Microsoft Patches Vulnerable Bootloader Used by BlackLotus, but There's a Catch

In May, Microsoft released five critical updates and 22 patches for Windows. Five critical patches is a relatively low number for a Patch Tuesday, but the patches also included one for the vulnerable bootloaders associated with the BlackLotus UEFI bootkit campaign. The patch was welcome relief for many users, but had to be released in a staged manner, and performed carefully so as not to brick systems and boot media.

The patched CVE-2023-24932 allows an attacker to "execute self-signed code at the Unified Extensible Firmware Interface (UEFI) level while Secure Boot is enabled." Phrased differently, the vulnerability in Secure Boot (aka "Baton Drop") allows any attacker that brings a vulnerable bootloader (including dozens that are still in the wild, not yet revoked and those yet to be discovered as vulnerable) to bypass Secure Boot and deploy a UEFI bootkit capable of disabling or bypassing arbitrary Windows security controls, and third-party protection agents. While the patch covers the bootloaders observed in the BlackLotus campaign, it is important to note that it does not patch the Secure Boot vulnerability itself, and should not be considered a mitigation for the risk the Baton Drop vulnerability presents to the enterprise. This became very apparent after last year's DefCon talk "One Bootloader to Load Them All".

While the official CVSS score is only 6.7 (mostly due to an attacker needing admin privileges and the 'local' designation), it should be taken with a massive grain of salt: On any given day there are dozens of ways to bypass UAC and elevate privileges for any attacker of any ilk or motive. Over the last five years there have been over 85 CVEs allowing an attacker to escalate privileges on Windows, including three news methods that give SYSTEM level access via NoFilter. Further compounding this, a massive spate of signed-by-Microsoft drivers is allowing actors with this admin-level direct access to the kernel. Moreover, the 'local' designation in the CVSS scoring deserves some color: to the extent an attacker has successfully spear phished or otherwise compromised the device, is the extent to which they can remotely deploy the Black Lotus bootkit (or any other UEFI bootkit, Black Lotus aside). So, if you care about bootkits and Secure Boot bypasses in the first place, don't settle for a patch that doesn't even address the core vulnerability, nor the many other vulnerable bootloaders that can be leveraged by campaigns like Black Lotus. Secure Boot, from here on out, is bypassable. The only mitigation is to have the ability to inspect systems below the OS, and find vulnerable and malicious bootloaders and affected MBRs. Yes, Eclypsium does this and does it well.



If you haven't yet performed the Microsoft patch process, we recommend reading updated guidance for CVE-2023-24932 and our blog.

- The patch issued by Microsoft does not address the core vulnerability in Secure Boot that is leveraged by the BlackLotus campaign.
- It takes months for vulnerable bootloaders to make it into the DBX list published on UEFI's website, and it can take even longer for Microsoft to update Windows to install the new DBX. Even more precarious, DBX updates can only be applied if you have updated your firmware so that your system doesn't depend on any vulnerable bootloaders that are now revoked. If it does, your system is bricked. Catch-22, anyone?
- Once your AV/EDR is bypassed, and an attacker deploys a UEFI bootkit, they will forever have full control of the operating system and applications/agents on it. We've conducted demonstrations showing this, and the explicit advantages to attackers that make it more than worth their effort to do so.
- Going forward, any actor that brings a vulnerable bootloader to their existing malware campaign now has the ability to bypass secure boot and deploy a UEFI bootkit to bypass Windows and 3rd party OS level controls.

# CL0P's MoveIT IT Supply Chain Attack Is Massive and Impactful

CL0P (aka TA505), infamous for leveraging the IT supply chain to compromise hundreds of victims via device level attacks like Accellion's FTA appliance and others, has succeeded in pulling off the most impactful and broad-scope attack in recent memory. Over 60 million victims have been impacted, a third of them in the financial sector and 84% of them in the US. The privacy data related impact cost alone is estimated to be $65B USD. Over a thousand victim organizations have been impacted, and that number is only growing.

The vulnerability and related exploit has been in play for two years leading up to this current mass-exploitation campaign.The actors patiently waited to complete their earlier GoAnywhere MFT Supply Chain attack against 130 victim organizations before beginning mass-exploitation of the MoveIT vulnerability.

## MoveIT IT Cyber Attack Affected Organizations by Country


*Image by KonBriefing*

Importantly, CL0P's primary modus operandi over the last several years has been to leverage the IT supply chain and its unique dynamics to victimize large swaths of organizations at once, and with ease, and low chance of being stopped prior to data exfiltration. The IT solutions they target are often, ironically, those that are meant specifically to provide layers of security above and beyond legacy solutions like FTP, and to meet stringent data-protection requirements such as GDPR, HIPAA, PCI-DSS, FISMA and DPA. The same irony also applies to the massive exploitation of other primary security control devices such as Firewalls and VPN devices. The attackers end up being able to both bypass and leverage these devices for absolute advantage over the victim's other mitigating security controls. Our guess is they are probably listening to a song like this in their headphones, while pulling down 60 million victim's worth of data unimpeded.

- CL0P has paved the way for many criminal actor groups. Their success in leveraging and attacking the IT supply chain at both software and hardware/firmware levels has created a sea-change effect in the overall threat landscape over the last several years. This trend, and the massive impacts associated with such large scale attacks, will likely continue and escalate given the tremendous amount of IT supply chain vulnerabilities discovered every week.

- While the MoveIT vulnerability was at the software layer, the same actor and countless other criminal and nation state actors alike, have been targeting hardware device vulnerabilities en masse, and to great effect. The primary allure of IT supply chain attack strategies is their ability to both scale the campaign,, while simultaneously evading the rest of the entire cyber security stack and relating tooling victim organizations rely upon. This is particularly true of exploits targeting the firmware of Firewalls, VPNs, Load Balancers, Routers and other externally facing devices such as BMC chips (recent high-impact research here), File-transfer devices and medical IOT devices directly connected to the Internet.

- Organizations need the ability to verify and monitor IT supply chain devices for vulnerabilities and threats at every layer, including the hardware and firmware layers modern adversaries are now actively targeting. This requires a fundamental change to legacy vulnerability management programs and tooling, and deep visibility down to the component level software and hardware of devices.

# RESEARCH & VULNERABILITIES

# Gigabyte Backdoor Presents IT Supply Chain Risk for Customers of Millions of Devices


Eclypsium recently discovered a backdoor in one of their customer's devices running a Gigabyte motherboard. Subsequent research into the backdoor exposed several potential attack vectors that this backdoor presents to attackers, including a compromise in the supply chain, a compromise in the local environment targeting the App Center functionality and vulnerable implementation, and the potential for malware persistence via the functionality of this firmware in systems running affected Gigabyte motherboards. The backdoor effectively drops and executes a Windows native executable during the system startup process, and this executable then downloads and executes additional payloads. Just as important, the manner in which it does so, has been implemented insecurely and can itself be leveraged to great effect by local network attackers via man-in-the-middle or DNS spoofing tactics. This backdoor could also be used to install UEFI rootkits and/or implants similar to LoJax (2018), MosaicRegressor (2020), FinSpy (2021), ESPecter (2021), MoonBounce (2022), CosmicStrand (2022), and BlackLotus (2023).

The discovery was made via heuristic detection methods, which play an important role in detecting new, previously-unknown supply chain threats, where legitimate third-party technology products or updates have been compromised. Without this deep level analysis capability, this backdoor could have persisted for many years to come.

- This backdoor uses the same techniques as other OEM backdoor-like features like Computrace backdoor (a.k.a. LoJack DoubleAgent) abused by threat actors and even firmware implants such as Sednit LoJax, MosaicRegressor, and Vector-EDK, which remains as open-source code on github that any actor can easily leverage given its extensive documentation.

- Recommendations for all enterprises and consumers using Gigabyte motherboards include deep scanning and monitoring of systems and firmware updates in order to detect affected Gigabyte systems and backdoor-like tools embedded in firmware. Organizations should update systems to the latest validated firmware and software in order to reduce the impact potential of these threats. Finally, Gigabyte customers should inspect and disable the "APP Center Download & Install" feature in UEFI/BIOS Setup on Gigabyte systems and set a BIOS password to deter malicious changes.

- The ability to perform deep heuristic analysis of firmware binaries is paramount in detecting both known and unknown threats, whether they arrive via the IT supply chain and firmware update processes, or whether they arrive via a spear-phishing email and drop to firmware in the form of bootkits and implants.

# Network Infrastructure Under Continued Attack

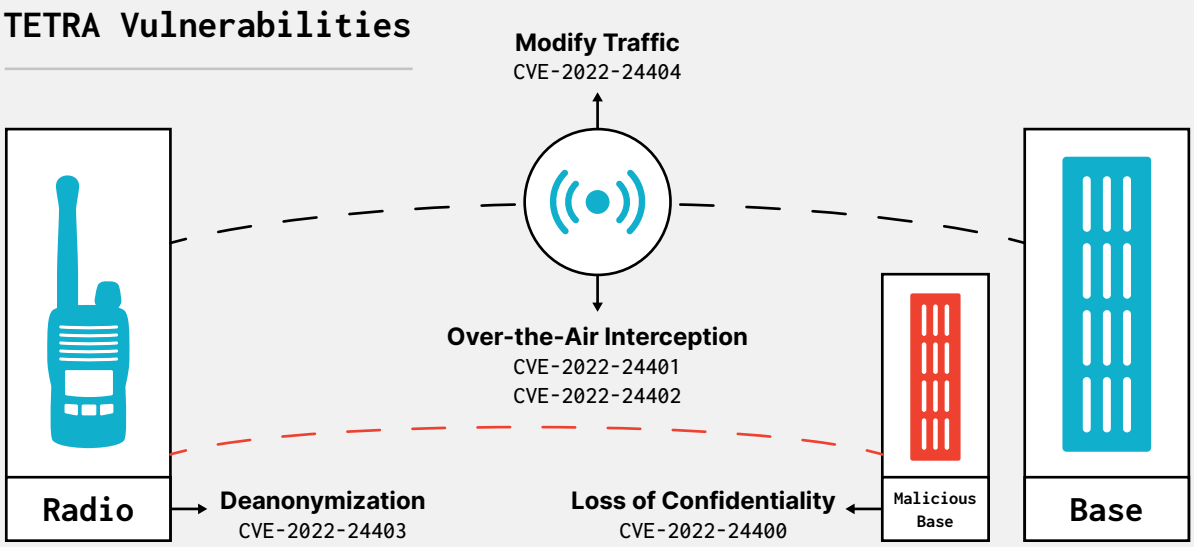
On July 18, Citrix announced a critical remote code execution vulnerability in Citrix ADC which had been observed being exploited in the wild. In the following weeks, the vulnerability was analyzed extensively and proof-of-concept exploits were released by Rapid7, Assetnote and Bishop Fox. Bishop Fox provided additional risk context, noting that, as of July 21st 2023, there were 61,000 affected appliances exposed on the internet, and roughly 53% of them were unpatched. As the vulnerability was exploited as a zero-day, mass-exploitation attempts were not as prevalent as with other network infrastructure vulnerabilities, though Greynoise sensors have detected some indiscriminate attacks. Sophos has moderate confidence attributing much of this activity to the criminal group FIN8.

This vulnerability is one of the more recent high-severity vulnerabilities discovered in network device firmware in 2023. Fortinet, Barracuda and Juniper have all been targeted by advanced adversaries whose tactics have evolved into using network infrastructure as an initial access vector and persistence methodology. In the case of the Fortinet vulnerability, China-nexus actors exploited an 0-Day vulnerability to bring appliance-specific malware to the affected device in order to target a European government entity and an MSP in Africa. Persisting in network infrastructure can provide exponentially longer dwell times due to poor visibility into the device firmware integrity and lack of security tooling as exists for client and server endpoints.


The use of network devices for initial access is not a new technique, but it is becoming more commonplace as attackers adjust to the imposed cost of endpoint security solutions and find gaps in security coverage to “set up shop.” Most of these devices exist in highly privileged parts of an organization, and provide adversaries with a mostly complete Linux or BSD environment, including tools which can be leveraged for living off the land attacks against Active Directory and other infrastructure. In June of 2023, CISA released BOD 23-02: Mitigating the Risk from Internet-Exposed Management Interfaces, requiring government agencies to remove internet access from network device management interfaces. While this is a good start, private sector organizations are not bound by these directives and their effectiveness in the long term remains to be seen. As nation state actors like Volt Typhoon have turned their attention to critical infrastructure, the industry should expect these attacks to not only increase in frequency, but in complexity, as adversaries shift their focus lower in the computing stack.

# TETRA:BURST

One of the more interesting research papers in 2023 was the disclosure of five vulnerabilities in the Terrestrial Trunked Radio (TETRA) standard used globally by law enforcement, military, critical infrastructure, and industrial asset owners in the power, oil & gas, water, and transport sectors and beyond. Depending on infrastructure and device configurations, these vulnerabilities allow for real time decryption, harvest-now-decrypt-later attacks, message injection, user deanonymization, or session key pinning. The vulnerabilities were discovered in the secret, proprietary cryptographic algorithms, the details of which are only disclosed to industry parties under NDA. In an interview with Kim Zetter, the European Telecommunications Standards Institute (ETSI) chair of the technical body responsible for developing the TETRA standard and algorithms stated "There's no evidence of any attacks on ... TETRA that we know of." However, the researchers noted in their DEFCON31 presentation that two of the five attacks are passive, meaning there would be no way to know if they've been exploited in the wild.




This research underlines the risks of proprietary cryptographic algorithms, which are not open for review like other standards and bring the risk of vulnerabilities which have existed for decades in the firmware of mission-critical communications systems. As these systems are commonly used in government and law enforcement, the ability for an adversary to snoop on communications, deanonymize users or inject malicious traffic into legitimate communications brings a different level of impact than a typical system vulnerability. For systems like TETRA, attacks of this nature add a kinetic component to a cyber attack, since infrastructure and first responder communications could be impacted as part of a multi-pronged attack.

# More Processor Vulnerabilities: AMD Zenbleed and Intel Downfall

Both AMD and Intel have suffered from recent processor-level vulnerabilities resulting in significant impacts to their customer base in the form of both cyber risk and performance impacts.

The AMD Zenbleed vulnerability affects their entire line of Zen 2 processors, with the majority of patches to be released sometime later this year in October. The exploit doesn't require physical access to the target device and can be exploited remotely by visiting a malicious website. Just as concerning, the exploit does not require any special system calls or privileges, so detecting it is next to impossible for defenders. What can be stolen? Anything running on the box, including virtual machines, sandboxes, and containers. For now, customers are forced to wait for system motherboard OEMs to author and offer patches, and see whether they impact performance negatively.


*Photo by Olivier Collet on Unsplash*

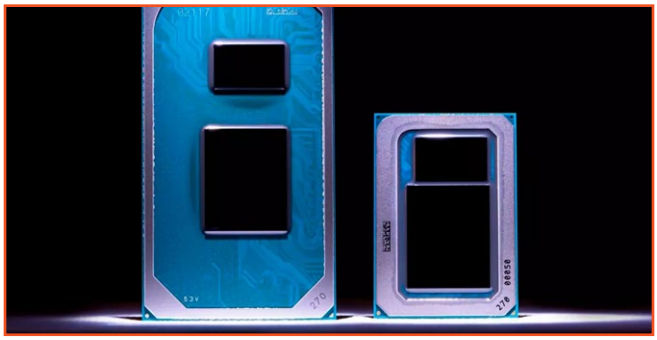


*Photo by Intel*

Meanwhile, Intel's recent Downfall vulnerabilities, falling in the category of speculative execution, impact 6th Skylake to 11th Tiger Lake generation Intel processors (billions of devices worldwide). Attacks leveraging these vulnerabilities include stealing cryptographic keys from OpenSSL, stealing secrets from the Linux kernel, breaking Intel SGX, and implementing high bandwidth covert channels between separate processes. While there have been no known public attacks yet (at the time of writing), the near-term impact on performance of patched devices has been startling. So much so, there is already a class-action lawsuit being put together by impacted customers who have been experiencing between 39% and 50% negative performance. Customers of affected devices are left either leaving the vulnerability open to exploitation, or sacrificing (up to) half of the CPU performance they paid for; neither a good option.

- CPU/hardware level vulnerabilities in the IT supply chain are appearing more frequently, and they are generally difficult to patch without significant impacts to performance.

- Vulnerabilities like these are found in many applications, including Tesla CPUs and other AMD processors.

The first step in mitigating the risks associated with hardware processor vulnerabilities is to know which devices in the enterprise or mission are affected by them via a baseline inventory of all motherboard components and their patch levels on all x86 devices in the environment. This can only be easily done with a solution like Eclypsium's.

# INDUSTRY NEWS

# Federal Regulations Round-Up

**NIST CSF 2.0 Draft** - NIST released the draft of its Cybersecurity Framework (CSF) 2.0 with a new Govern function. The draft is now more general but also more encompassing, and includes guidance on cybersecurity supply chain risk management (C-SCRM). Comments on the new draft are due in November, and NIST expects to release the final version early next year.

**CISA UEFI Security Recommendations** - CISA issued a call to action, asking organizations to pay more attention to UEFI firmware, writing "System owners should be able to audit, manage, and update UEFI components just like any other software that is being acquired."

**National Defense Authorization Act for 2024** - In setting the budget and priorities for the Department of Defense (DoD), the U.S. Senate called out supply chain security and firmware integrity as "Items of Special Interest," and asked the DoD CIO to brief Congress on efforts to secure firmware by March 2024.

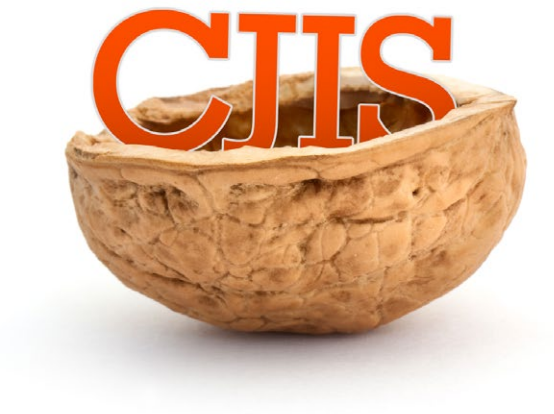
**CISA and NSA Issue Guidance for Hardening BMCs** - Citing the discovery of new BMC vulnerabilities, CISA and the NSA released guidance on hardening baseboard management controllers used for remote management of servers. CISA also issued a binding operational directive to federal agencies, requiring them to either remove management interfaces from the internet or implement compensating zero-trust controls.

**OMB Releases Supply Chain Security Attestation Details** - The OMB provided more detailed guidance to Federal agencies and their vendors about the requirements for supply chain security attestation. The goal is to ensure that technology providers are following NIST's Secure Software Development Framework (SSDF) guidelines.

# CJIS Compliance Notes

In December 2022, the FBI, and the CJIS Advisory Policy Board, updated the Criminal Justice Information Systems compliance policy to align more closely with NIST 800-53 Rev. 5. To do so, this involved an increase of almost 100 pages of controls and additions to the policy. The deadline for implementation of CJIS 5.9.2 is currently October 1, 2023. This means organizations that depend on access to the FBI's criminal database need to act immediately to address the substantial amounts of new controls.

These control changes are a dramatic increase in capabilities required by organizations accessing CJIS data and a substantial amount of these changes will require new tool and platform purchases and implementations. These controls span many different disciplines, such as email spam controls, training, patch management, logging/ monitoring, multi-factor authentication, and software/firmware/information integrity.




This is the first time CJIS controls have used terminology around both firmware and integrity. CJIS organizations are now forced to maintain upgrades and be aware of security notices. Integrity can be interpreted as monitoring for change and validation of change to known good. These integrity control requirements focus around eliminating the risk imposed by supply chain attacks and supplementing other monitoring controls with an additional verification step. Traditionally, if a software upgrade wasn't detected as malicious, it was often ignored until determined to be nefarious in nature. Now, organizations should be working from the opposite direction. Start from known good and continually compare against this baseline of trust.

In speaking with CJIS compliance officers for most organizations, few are prepared and many are unaware to the extent of the new requirements. This has left many organizations either scrambling for solutions, or planning to exist out of compliance until their next on-site review or until budgets can be aligned for these new solution purchases. Currently, Eclypsium's platform provides solutions to a multitude of these new controls allowing CJIS organizations abilities to rapidly conform with minimal lift.

# NON-STANDARD THREATS

# Unintentional Threats: Leadership

Far too often these days, leaders within organizations want to speak to how important cybersecurity is, but do they truly understand or approach cybersecurity with the appropriate level of effort? Cybersecurity is often seen in boardrooms and executive leadership meetings as nothing more than a compliance requirement, or a cost center that they would rather not have to fund. This is understandable as the benefits of a properly defined and proactive cybersecurity program are difficult to truly measure. While it may be difficult, it is not impossible given risk measurements for items such as loss of productivity, loss of intellectual property, or reputational damage. As shown by this Forbes report, leaders in most businesses underestimate the impact of a breach by at least 15x the actual potential cost just for initial recovery. Far too many take no account for reputational damage as well, and do not understand recovery efforts.

This is due to a combination of factors, not least of which is that very few CISOs are evangelizing the message. In most cases CISOs are trying to work in the background and go unnoticed, which is laudable in the effort to reduce friction to the business. However, as potential negative unplanned impacts mount, this approach tends to achieve the opposite of the intended goals. While the security program must always strive to find the balance between the level of risk which is accepted by the business, and the productivity achieved by the business, the difficulty for most lies in the proper expectation of risk. Visibility of the entire attack surface and education of the user base is the only way to further continue improvements.

While it is predicted that cybersecurity spend will continue to increase in amount and percentage of overall IT spend, we continue to see an increase in successful attacks. The approach must be reviewed and a fundamental shift in how risk is analyzed needs to be implemented to reduce potential threat vectors for these organizations. And this starts with CISOs having the ability to properly guide the executive staff and board room in the approach needed to reduce these threats, rather than competing interests minimizing the threat which exists. The C-Suite and board members must act in harmony to achieve the security of the business rather than scapegoating security personnel or simply ignoring the risk as they are not being “forced” to focus on it.

# Small Businesses Believe They Are Less of a Target

Most smaller businesses do not believe they are as much of a target for cyber attackers when compared to larger enterprises. The general thought process is that an attacker will gain much more by attacking a larger enterprise either in regards to intellectual property or customer information. These smaller businesses fail to recognize the upstream and downstream effects of an attack on them. While the direct impact of a compromise carried out on a smaller business could be less productive for an attacker, they can then make use of that compromise to pivot into larger organizations where the target is a customer or provider.

Additionally, the method of attack generally exposes those individuals within an organization who have the most access and tend to be the least protected. In most smaller organizations, cybersecurity is reduced on these VIPs due to the need for an expected ability to work unimpeded in any way. As shown by this study, the focus on cybersecurity in these smaller organizations is limited by an incorrect assumption that the expenditure is more costly than a recovery, the proper hygiene approach makes those would-be targets feel negatively impacted on their ability to perform their jobs. These misconceptions allow for exposure that could otherwise be limited by standard security hygiene measures. Proper updates to devices used by the organization, simple multi-factor authentication, and an assurance to both vendors and customers alike that the environment is protected by these minimal security measures at least.

Most organizations require a vendor security assessment, but few of those require a customer security assessment, allowing for the supply chain of data to be impacted in an upstream way. Corporate responsibility needs to be refreshed to reflect the reality of how interconnected our systems are, and approach the threat landscape from all potential avenues of ingress. A proper holistic assessment of the true threat landscape is needed to approach the new and emerging threats in a more formidable way. If we are blind to our weak spots there is little to no opportunity to improve. This level of visibility is comparable to the adage of an ostrich sticking its head in the sand not willing to see the danger.