BELOW THE SURFACE
THREAT REPORT

WINTER 2023

EAST VS. WEST - THE CHIP WARS

VOLT TYPHOON

CITRIX BLEED

AND MORE ...

East vs. West

The Chip Wars are in Full Effect

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

Every nation state has long realized that whichever nations win the race to quantum computing and AI superiority will likely dominate the global landscape. This has created a race to produce the infrastructure and computing that is fundamentally required to win the race. The US has been bringing chip manufacturing back to CONUS and strong allies like Japan. However, like any war, the Chip Wars have also forced nations to take drastic steps to skirt sanctions in an effort to keep up. "Anything goes" seems to be the mantra, as the US discovers illicit secret chip factories in China, as China lures overseas chip talent to offset its weaknesses in the design phase of the supply chain, and as Chinese hackers continue to steal source code, SDK's and IC designs from western chip manufacturers.

This dynamic also brings with it cybersecurity and cyber supply chain implications, and affects what one might describe as "Digital Supply Chain Safety". Whether it's the Defense Industrial Base worried about "Mutually Unassured Destruction" (MUD) or the West's critical infrastructure withstanding an onslaught of cyber attacks leveraging digital supply chain vulnerabilities, one thing is for certain: it's only going to escalate for the foreseeable future, and now is the time to mitigate the risks before the impact reaches its full potential.

While the theme for this report is East vs. West Chip Wars, we'll also cover other areas such as Compliance, Iranian state actors, Ukraine cyber events, hacktivists and criminal hacker groups.

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

TABLE OF CONTENTS_

THREAT LANDSCAPE

China's Volt Typhoon Campaign Draws Attention as its Scope Expands

Volt Typhoon, a Chinese government sponsored threat campaign active for over two years and likely tied to the Ministry of State Security (MSS), has been increasing in scope and adaptive techniques designed to evade cyber defenses. The actor nexus behind Volt Typhoon, APT41, is normally known for espionage and IP theft activity...until recently. With the specter of a possible conflict in Taiwan, China has been proactively probing and compromising critical infrastructure targets in the West and its allies Guam and Taiwan, with the aim of being able to disrupt communications and other infrastructure including water, should conflict break out. In fact they've hit everything from manufacturing, utility, transportation, construction, maritime, government, information technology, to education sectors in the US. Mandiant's Chief analyst, John Hultquist, commented that "They were found in Guam (as part of a recently discovered 'Flax Typhoon' campaign) but they were also discovered all over the continental United States, including in telecommunications and logistics."

Volt Typhoon has found success across all of its activity by living off the land and gaining entry and persistence by exploiting vulnerabilities in externally facing devices such as routers, firewalls and VPN devices. By taking advantage of these digital supply chain vulnerabilities, they gain particular positional advantage, and can evade most cyber solutions in place and persist for extended periods of time before dropping any subsequent payloads down the line to cause disruption or destruction.

This dynamic has recently garnered significant attention, with recent news of Chinese state-sponsored attacks against a water utility in Hawaii, a major West Coast port, at least one oil and gas pipeline, and many utilities in other countries. China "is sitting on a stockpile of strategic vulnerabilities" it can use in stealthy attacks. "This is a fight for our critical infrastructure. We have to make it harder for them." -Morgan Adamski, director of the NAS Cybersecurity Collaboration Center.

TAKEAWAYS_

- Volt Typhoon actors have been exploiting externally facing devices such as ASUS, Cisco RV, Draytek Vigor, FatPipe, IPVPN/MPVPN/WARP, Fortinet Fortigate, Netgear Prosafe, and Zyxel USG. These devices are found in both SOHO environments as well as in and around critical infrastructure. Many organizations fail to identify and patch these critical vulnerabilities, providing the actors an easy vector into their operations.
- Chinese nation-state actors also exploit dozens of other similar devices, and there's no reason to think the Volt Typhoon campaign won't continue to adapt in exploiting any vulnerable externally facing device as the campaign continues to unfold.
- In defending against Volt Typhoon, organizations should ensure they have an independent, central, digital supply chain continuous monitoring solution in place, taking care not to rely on legacy vulnerability management programs alone.

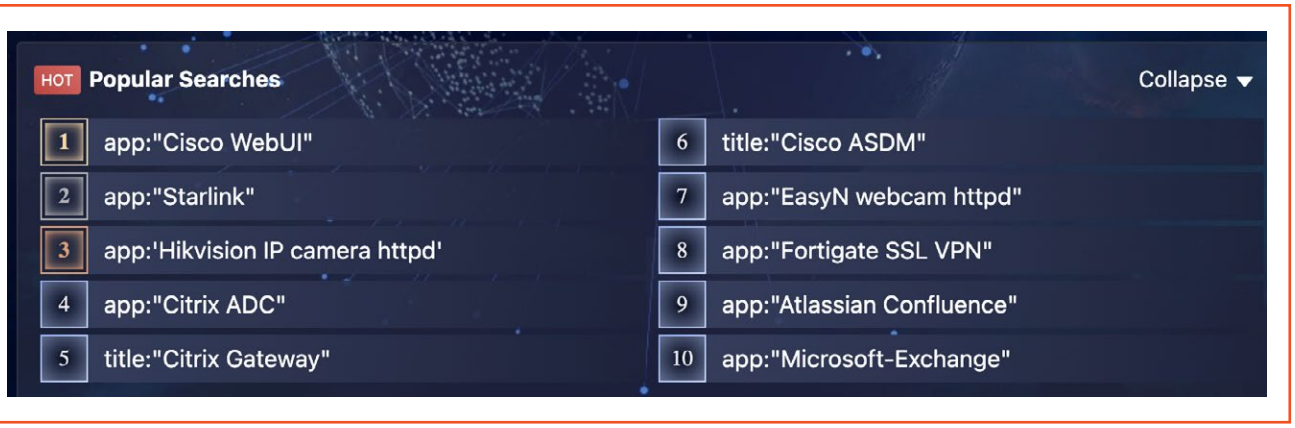
THREAT LANDSCAPE

Chinese BlackTech Group Modifying Firmware on Edge Devices

Chinese BlackTech actors (aka "The Phantom of the Routers") active since 2010 have been modifying firmware on compromised edge devices, gaining footholds in victims in the US and Japan. The BlackTech group has successfully targeted government, industrial, technology, media, electronics, telecommunication sectors, and suppliers to U.S. and Japanese militaries. Much of their activity is tied to the digital supply chain, targeting Technology, Semiconductor, Electronics, Engineering, Construction, and Manufacturing victims. They have also targeted victims in Taiwan, Hong Kong, and Japanese subsidiaries and MSPs within China.

The firmware-based attacks use a rigorous set of 18 different MITRE ATT&CK tactics to compromise and update the firmware on Cisco and/or other network devices. This gives them nearly undetectable persistence and omnipotence on the devices, allowing them to then leverage the trust relationships between US and Japanese subsidiaries in order to move from branch locations to main headquarters.

BlackTech continues to develop and evolve its tactics and malware payloads. It is adept at integrating the latest edge device vulnerabilities into its campaigns, grabbing the latest POC exploits from SeeBug, finding exposed devices from ZoomEye or Shodan, and leveraging attack frameworks like POCsuite3 that easily pull in these POCs. The take-away? On any given Sunday, BlackTech can deploy exploits against whatever the latest edge device vulnerabilities are exploitable.



TAKEAWAYS_

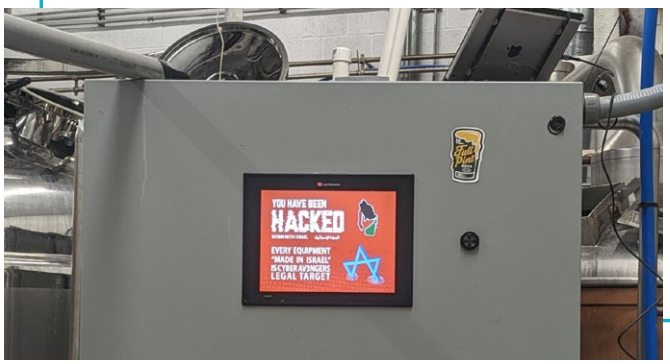
- This prolific actor is able to take whatever the vulnerability du jour is, scan for exploitable devices, and implement the exploit into whatever campaign they've already tooled up for. This emphasizes the importance of identifying and patching vulnerabilities for externally facing devices as quickly as possible.
- Once an externally facing device is compromised, it often results in an ideal attack position for any attacker of any motive/objective.
- The ability to proactively and continuously monitor the device firmware of such edge devices is paramount in countering modern nation-state threats. Relying on legacy vulnerability management programs and technologies is not sufficient.

THREAT LANDSCAPE

Cyber Av3ngers - Iranian Nation State Backed Hacktivist Group

In recent weeks, the cyber threat landscape has seen heightened activity linked to Iran-backed groups, raising concerns for critical infrastructure security. The Iran-affiliated hacktivist group Cyber Av3ngers has stepped up its attacks, particularly targeting Programmable Logic Controllers (PLCs) particularly in water and wastewater treatment plants, but also in the energy, shipping, and distribution sectors. These attacks come on the heels of increased public threats from Cyber Av3ngers to industries utilizing Israeli-manufactured Operational Technology (OT) and Industrial Control Systems (ICS) equipment.

One notable incident occurred when the Municipal Water Authority of Aliquippa lost control of a booster station due to a compromised Unitronics PLC. Weak or default passwords and targeting of the device's programming port were the vulnerabilities exploited. Several other U.S. water authorities, an aquarium, and even a brewery fell victim to similar attacks (screenshot below). Cyber Av3ngers' recent activities, including both true and false claims and threats, have sparked concerns about critical infrastructure security. CISA has recently released an alert highlighting the TTPs associated with this threat actor. Meanwhile Pennsylvania U.S. Senators Bob Casey (D), John Fetterman (D) and U.S. Rep. Chris Deluzio are calling on the U.S. Department of Justice to investigate the incident.



Source

Note that Unitronics PLCs have been hacked in the past. A video of them being remotely activated to open access doors in Feb 2022 shows just how eerie it must feel. In October this year, the group dropped "Crucio" ransomware on a dozen or more servers, security cameras, and smart city management systems in Israel. Many of these victims ran Hikvision cameras that were compromised as part of the campaign.

TAKEAWAYS_

- Iran-backed Cyber Av3ngers are actively targeting U.S. critical infrastructure, focusing on PLCs in water and wastewater treatment plants.
- Weak or default passwords, along with targeting open programming ports, have been exploited in recent attacks.
- Organizations should implement cybersecurity measures recommended by CISA, such as changing default passwords, using Multi-Factor Authentication (MFA), and disconnecting PLCs from the open internet, to mitigate risks in the face of escalating cyber threats.
- This hacktivist group is semi-opportunistic in choosing its victims. It begins with a known vulnerability on a given device, scans for such on the Internet, and then chooses victims that align with its hacktivist mission. The implication: Today it is Israeli-made Unitronics devices. Tomorrow it could be Israeli or US-made firewalls or VPN devices (Iranian government backed actors have already targeted a children's hospital in Boston via a Fortinet device). Any easily exploitable device owned by their intended victimology profile is fair game.
- Today, these actors appear to lack the follow-through and expertise needed to cause material safety impact to OT operations. However, being backed by the ISRG, they may at some point pass off access to these systems to more skilled actors that have the means to impact safety. Note that other ISRG-connected groups have done extensive research into how to blow up fuel pumps or sink cargo ships via cyber attacks. They've also tripped missile warning systems in Israeli cities. The overall Iranian cyber threat to Western countries' infrastructure and operational networks should not be underestimated.

THREAT LANDSCAPE

DPRK's Lazarus Group Continues to Target Supply Chain Vulnerabilities

North Korean state-sponsored hackers have been leveraging the digital supply chain in their attacks for the last several years, and there's no sign of abatement. The primary goals of these supply chain attacks align with DPRK-state priorities, including revenue generation, espionage, and technology theft. Lazarus uses increasingly sophisticated techniques, zero-day vulnerabilities, and third-party software exploits to successfully stay ahead of their victims.

The latest campaign, dubbed "Dream Magic", leveraged a combination of watering hole attack and vulnerable software from MagicLine4NX, a South Korean security authentication software solution made by Dream Security. From there, they exploited a zero-day vulnerability over the network to attack a device and move further into the network.

On the heels of this campaign the UK and South Korea jointly released an advisory highlighting the TTPs the attackers used, along with recommendations on how to prevent and/or respond to such attacks. This advisory is the product of what is a new Strategic Cyber Partnership between the UK and the Republic of Korea. The partnership aims to counter the extensive targeting of the supply chain by DPRK attackers, after years-long activity targeting software development environments, many of which are cyber security solutions. Other software suppliers targeted include CyberLink, (a multimedia software company), 3CX (communications software affecting thousands of user organizations) and a slew of manufacturing, agricultural, and physical security companies via the Log4Shell vulnerability found in publicly facing VMWare Horizon devices. .

TAKEAWAYS_

- Lazarus have found success by attacking the digital supply chain in order to compromise a vast amount of victim organizations that use the software and devices they poison with malware.
- In the case 3CX, we learned that Lazarus successfully strung two back to back supply chain attacks together, resulting in hundreds of thousands of victims. Yet they only singled out specific targets for follow-on payloads and data or crypto-currency theft.
- While the latest attack against "Dream Magic" campaign focused on a software supplier, there is growing concern that Lazarus may eventually turn to hardware/device manufacturers for even longer term persistence and campaign survivability. With the sheer number of victims they have compromised, there is a good chance they may have access to source code and development frameworks for hardware manufacturers or firmware developers.

THREAT LANDSCAPE

Lockbit - Thriving By Exploiting Digital Supply Chain Vulnerabilities

It's no secret that Lockbit has risen to take the mantle in the absence of Conti. Heavily targeting similar victimology, heavy use of Initial Access Brokers (IAB's), robust organizational structure and attack life-cycle handoffs, and bold attacks on some of the most well-resources and largest targets in the world.

At time of writing, they've already surpassed one thousand victims in 2023; more than the number two and three spots combined (Blackcat and Cl0p). Over 40% of ransomware stems from these three groups. The more ransom payments they accumulate, the more powerful they become; able to pay premiums to Initial Access Brokers, and for exclusive zero-day Exploits.

One of their key advantages is their ability to rapidly and mass exploit vulnerabilities found on network edge devices - Firewalls, VPNs, Load Balancers, etc. Once these devices are compromised, the access is handed off to operators with above-par skills and TTPs. Such edge devices give them quintessentially ideal positioning from which to conduct powerful tactics and tools to further gain persistence, deploy ransom payloads, and exfiltrate data for purposes of double extortion. They don't exfiltrate arbitrary data either; they perform extensive reconnaissance and study of the business process and critical data that will give them the highest form of leverage during negotiations. Their negotiation skills are diverse and refined: they might even notify the SEC on your behalf that you've been materially impacted by the event. Or they might present to you a copy of your own cyber insurance policy and draw out legal or contractual challenges you'll have. Or they may inform you on how to work with OFAC to allow ransom payment to a sanctioned country/region they operate from. They'll threaten, and follow through, to notify a victim's 3rd parties, supply chain, or customer base. Nothing is off the table. This allows them to find success in targeting some of the most well-resourced and prepared targets on the planet, ranging from big four consulting firms, the largest mail carrier in the UK, a significant partner/supplier to SpaceX to large scale DIB builders, to the largest bank in the world.

Their secret weapon lies in their ability to adaptively target easily exploitable devices, whether those are a Cisco ADA device, a Fortinet device, or a Citrix ADC or Gateway; giving them omnipotent persistence and access to critical devices and networks on internal networks. The past few weeks, they've leveraged the CitrixBleed vulnerability highlighted in another entry below. But tomorrow there will be another vulnerability on another externally facing critical device, and it might be a zero day for which organizations are unable to anticipate or even patch.

TAKEAWAYS_

- Lockbit has found success in targeting externally facing devices, leveraging easily exploitable vulnerabilities in the digital supply chain to great effect. Once such devices are compromised, Lockbit is set-up to carry out extensive TTPs in order to extract the most critical data and deploy one of several ransomware payloads in their arsenal.
- Lockbit successfully attacks some of the largest and most well-resourced victims on the planet, which emphasizes the need for organizations to immediately identify vulnerable edge devices and patch or otherwise monitor for and mitigate malicious activity and compromise.
- Proactively monitoring for vulnerable firmware and device misconfigurations on such devices is the best mitigation against actors such as Lockbit who thrive on the use of initial access brokers to gain ideal footholds in victim environments.

THREAT LANDSCAPE

Who's Behind the Hack on Ukraine's Largest Telco?

The recent attack on Ukraine's largest Telco (of the three they have) represents either a step-level increase in the destructive capabilities of a hacktivist organization, or a milestone attack by a nation state willing to bring down a telco serving half of Ukraine's population and critical infrastructure services.

On the morning of December 12th, unknown actors carried out a massive attack on Kyivstar. The attack affected mobile and Internet services for over half the country's population, affecting everything from air raid siren warning systems, water, energy and gas substations, banking ATMs, retail PoS, local armed forces, automated systems, EMS, and other critical infrastructure services. Citizens scrambled to swap SIM cards to other carriers and the military fell back to driving around with loudspeakers to warn of incoming missile attacks. This was the most impactful cyber attack of the war since the VIASAT sat-comm attack. The attack is especially worrying because as Illia Vitiuk, head of the cyber department at the Security Service of Ukraine (SBU) said, "If one of [the companies] is out of operation, the other two won't be able to operate because they will be overloaded."

It is not yet known how the attackers got into the network, but several details of their destructive motives have since emerged. Customer databases were destroyed, as well as "Cora", the main control center for the entire network. Making matters worse, the attackers also destroyed critical configurations at transit base stations, requiring workers to travel to and manually attempt restoration. This could take up to a week to complete. Alexander Komarov, the telco's president, noted that the attack had "the maximum possible destruction of the virtual IT infrastructure" as a primary objective.

The Ukrainian SBU immediately began an investigation into the attack, and believes it was carried out by Russian intelligence services. Yet, more than one hacktivist group has now claimed responsibility for the attack. The Solntsepek Russian hacking group claimed they firmly compromised the internal infrastructure of the telco, and that they exfiltrated customer data (meanwhile, Kyivstar's facebook page claims customer data has not been stolen). If it is Solntsepek, then it is likely just one of many front names for Sandworm, a well known Russian GRU actor that is known for destructive and disruptive attacks.

Prior to Solntsepek's claim, Killnet claimed responsibility for the attack. This raised suspicion among cyber threat analysts that were quick to point out how unlikely it would be for Killnet to have the skills and tools needed to do so. They are mostly known for DDOS attacks, renaming scripts as their own, and other methods of claiming attacks that are not their own. Moreover, there would likely be much more bravado from Killnet members had they actually carried this out, along with proof of their attack. But we have yet to see this.

Killnet's post on Telegram indicates they carried out attacks on telcos and banks and that they were excited to see what their "new partners" were capable of. Could these "new partners" be Deanon Club (aka Infinity Team) that they partnered with earlier this year? It's unlikely, as Deanon Club is mostly known for OSINT and doxing style attacks, not destructive ones. Many pro-Russian hacktivists are becoming fed up with Killnet's leader, KillMilk, but often don't call Killnet out taking credit for attacks, for fear of being doxxed or blackmailed by the leader.

At the time of writing several questions still remain unanswered: Who did it? What type of wiper payload was used? How did they gain initial entry? And perhaps most importantly, if it was the Russian government, then why have they played such a heavy hand now? An attack causing this much kinetic and societal impact, affecting over half the population, is most likely tied to a larger strategic initiative underway. Further, if it was a state-backed attack, then why would the attackers not first exfiltrate the customer data before destroying it? This data may even include passport information, and geo-location history; both highly valuable in the context of warfighting.

TAKEAWAYS_

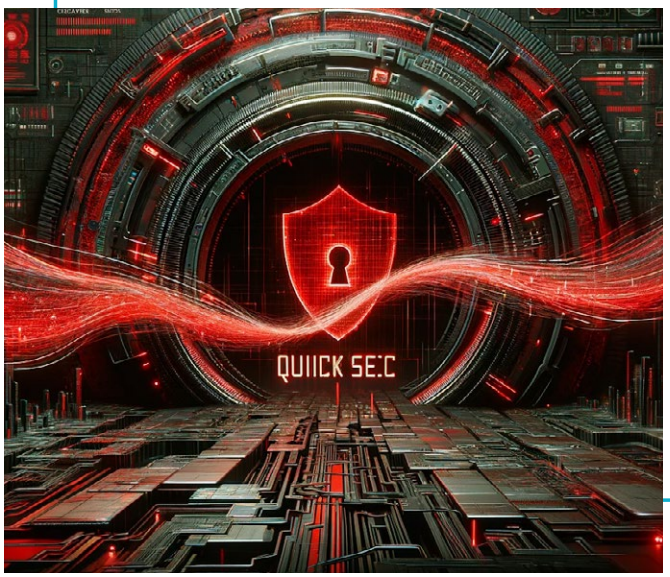
- The attack against Ukraine's largest mobile and Internet provider marks the most destructive cyber attack in the Russia-Ukraine war, matched only by the early attack on the VIASAT satellite control system. It demonstrates just how vulnerable communications systems are, even vigilant organizations under constant attack. This should serve as a reminder for all telcos, that hardening of systems, rapid patching of vulnerabilities, and robust backup and restoration capabilities are of the utmost importance.
- Two top-tier incident response firms, along with the SBU, are working to contain, eradicate, and identify the attackers. Hopefully, samples of the destructive wiper and related TTPs will be documented for public awareness, and strong attribution.
- Should the actor be revealed as Russian Intelligence operations, it should be noted that the same actor is highly adept at targeting device firmware for low-level persistence, and/or device destruction at the motherboard level. DFIR efforts should take care to perform forensics at the firmware level to rule out low-level persistence on critical devices.
- Rumors on Ukrainian Telegram suggest the recovery could take months, although Kyivstar suggests a week should be sufficient. At time of writing, service is still down, and can be checked here.
- Per this Telegram post, the initial vector in may have been through a compromised Kyivstar employee account

THREAT LANDSCAPE

CVEs, Firewalls, and The Complex Supply Chain

Recently threat actors successfully attacked critical infrastructure in Denmark. While reviewing the incident details it was discovered that a remotely exploitable vulnerability was leveraged against Zyxel firewalls implemented in the environment. Further digging revealed that CVE-2023-4398 had been assigned to the vulnerability in Zyxel firewalls, however, specifically it was in the "QuickSec" IPSec component. Turns out, Zyxel did not write their own IPSec stack, but used a commercially available version that has a long history of companies that sold and maintained it and have also been acquired several times over.

The frustrating part of this type of situation is that as a defender you are left at a disadvantage. If a component turns out to contain a vulnerability, how do you know if other systems contain that same component? The CVE process is not helping enough as the vulnerability has been associated with Zyxel firewalls, but could also exist in other systems that use the vulnerable component. There is currently no way to map components like this QuickSec IPSec library to products. This is not the first time this type of supply chain incident has happened, nor is it the last. Validating the supply chain on all of your systems, especially ones that are Internet-facing, is a crucial task given today's threat landscape. You can read more on our blog in the article titled "Zyxel Firewall Vulnerabilities Reveal the Complexity of the IT Infrastructure Supply Chain"



TAKEAWAYS_

- Zyxel firewall vulnerabilities are but one example of supply chain issues that can live below the surface. A vulnerability associated with a single platform may not only be present in that platform. Therefore, you must use supply chain management to determine where the vulnerability may live in your environment.
- The CVE system is only part of the picture. The rules and processes that govern CVE today could leave gaps in your vulnerability management and supply chain programs. Don't solely rely on CVE when trying to discover and prioritize vulnerabilities and threats.
- Attackers are going after Internet-facing targets that have vulnerabilities with known exploits. Be diligent when patching these systems and monitor the devices for suspicious activity and supply chain flaws (such as backdoors).

RESEARCH & VULNERABILITIES

Citrix Bleed Creates Feeding Frenzy for APTs

Citrix Bleed, formally identified as CVE-2023-4966, emerged as a significant cybersecurity threat in October 2023, specifically targeting Citrix NetScaler ADC and Gateway systems. This vulnerability was publicly disclosed by Citrix on October 10, 2023, when the company released security updates to address the issue. The critical nature of Citrix Bleed lies in its ability to allow attackers to bypass standard security measures like password requirements and multi-factor authentication (MFA), granting unauthorized access to affected systems. This flaw poses a substantial risk to the confidentiality and integrity of sensitive information processed by the compromised systems.

In response to the active and targeted exploitation of this vulnerability, the Cybersecurity and Infrastructure Security Agency (CISA) issued guidance on November 7, 2023, to help organizations address the risks associated with Citrix Bleed. The vulnerability garnered considerable attention when the LockBit ransomware group began exploiting it in their attacks, further highlighting the severity of the issue. By exploiting Citrix Bleed, cyber actors could potentially take control of affected systems, making it a critical concern for organizations relying on Citrix NetScaler ADC and Gateway for their operations.

TAKEAWAYS_

1. **Importance of Timely Patch Management:** This incident underscores the critical need for timely application of security patches. Citrix released updates to address the vulnerability shortly after its disclosure. Practitioners should prioritize the installation of these updates to prevent exploitation.
2. **Enhanced Monitoring for Suspicious Activity**: Given that the vulnerability allows attackers to bypass security measures like passwords and multi-factor authentication, practitioners should enhance monitoring systems. This involves looking for unusual user activities or network traffic that could indicate unauthorized access. Eclypsium has developed firmware integrity monitoring for devices like Citrix and can detect public IOCs of Citrix Bleed exploitation.
3. **Awareness of Exploit Trends:** The LockBit ransomware group's adoption of this vulnerability for their attacks highlights the importance of staying informed about current exploit trends. Cybersecurity teams should actively follow threat intelligence reports and advisories from reliable sources like CISA to stay ahead of emerging threats.
4. **Robust Incident Response Planning:** The potential for adversaries to take control of user sessions and systems through Citrix Bleed necessitates robust incident response plans. Practitioners should ensure that they have effective strategies and protocols in place to quickly respond to and mitigate any breaches that might occur as a result of this vulnerability.

RESEARCH & VULNERABILITIES

Cisco IOS XE 0-day

In October 2023, Cisco disclosed a critical zero-day vulnerability in the web User Interface (UI) component of its Internetworking Operating System eXtended Edition (IOS XE) software, identified as CVE-2023-20198. This vulnerability, affecting a wide range of Cisco networking devices including routers, switches, and wireless controllers, was particularly alarming due to its high severity, with a Common Vulnerability Scoring System (CVSSv3.1) score of 10 out of 10. The flaw was characterized as a privilege escalation issue within the IOS XE Web UI, a component that comes as a default in the software. The exploit allowed unauthenticated remote attackers to potentially take full control of the affected devices, making it a significant threat to network security.

The zero-day vulnerability was actively exploited by cyber threat actors, as reported by Cisco's Talos group. The exploit was used to compromise tens of thousands of devices, allowing attackers to install backdoors and gain unauthorized access. This widespread exploitation underscored the criticality of the vulnerability and the need for immediate action by Cisco device administrators. Cisco released a security advisory on October 16, 2023, to address this vulnerability, highlighting the urgent need for customers to apply the provided patches and updates to protect their devices from potential cyberattacks.

TAKEAWAYS_

1. **Comprehensive Vulnerability Scanning and Assessment:** Cisco needs to intensify its vulnerability scanning and assessment practices, especially focusing on components like web UIs that are included by default in their software. This proactive approach can help in identifying potential vulnerabilities before they are exploited in the wild.
2. **Rapid Response and Communication:** The incident highlights the importance of a rapid response mechanism. Cisco's timely advisory and communication with its user base played a key role in mitigating the impact. Continuing and enhancing this rapid response approach is vital for future incidents.
3. **Secure Software Development Lifecycle (SDLC):** Integrating security as a core aspect of the software development lifecycle can significantly reduce the chances of such vulnerabilities. This includes regular security audits, code reviews, and integrating security testing in the early stages of development.
4. **User Education and Awareness:** Given the critical nature of the vulnerability, it's crucial for Cisco to not only provide patches but also to educate its users about the importance of regular software updates and the potential risks of not updating. User education campaigns can be an effective tool in ensuring that customers understand and apply necessary security measures.

RESEARCH & VULNERABILITIES

SLAM: New Exploit Leaks Kernel Data from Userland

Researchers from Vrije Universiteit Amsterdam have unveiled a new side-channel attack named SLAM, posing a threat to the security of Intel, AMD, and ARM CPUs. SLAM leverages a new feature called Linear Address Masking (LAM) in Intel CPUs, along with analogous features in AMD (Upper Address Ignore or UAI) and Arm (Top Byte Ignore or TBI) processors. This exploit enables userland processes to leak sensitive ASCII kernel data, including root password hashes, from kernel memory. It also increases the Spectre attack surface by taking advantage of transient execution attacks, exploiting speculative execution to access restricted information through a cache covert channel. Notably, SLAM targets future CPUs that support LAM, UAI, and TBI, and AMD CPUs vulnerable to CVE-2020-12965.

An attacker would need to execute code on the target system that interacts with the unmasked gadgets. They would then carefully measure side effects using sophisticated algorithms to extract sensitive information, such as passwords or encryption keys, from the kernel memory. ARM states that its systems already mitigate against Spectre v2 and Spectre-BHB and does not plan further action against SLAM. AMD points to existing Spectre v2 mitigations to address the SLAM attack but does not provide additional guidance or updates. Intel plans to provide software guidance before releasing future processors that support LAM, including the Linear Address Space Separation (LASS) security extension, and Linux engineers have created patches to disable LAM temporarily.

TAKEAWAYS_

- SLAM is a novel side-channel attack that endangers the security of Intel, AMD, and ARM CPUs, exploiting features like LAM, UAI, and TBI.
- This attack increases the Spectre attack surface and enables the leakage of sensitive kernel data, including root password hashes.
- While AMD and Intel are working on mitigations, Linux maintainers have developed patches to disable LAM temporarily, and researchers have proposed Quarantine as a software-only approach to mitigate transient execution attacks and enhance physical domain isolation.
- Eclypsium provides organizations with the ability to know, at the component level, what hardware and firmware is on their devices throughout the enterprise, helping them prioritize which vulnerabilities to mitigate or remediate.

INDUSTRY NEWS

Supply Chain Risk Elimination

We have all heard the phrase "Zero Trust." Maybe even 50+ times today. It's a great framework that organizations have started to adopt in many different permutations. We have purchased and implemented different security controls at many different levels to build towards a rock-solid foundation of technology, coupled with processes that ensure there's tight oversight to ensure policy is complied with. Our organizations are largely built towards operational roles that reinforce these functions while not overtly impacting efficiency. We're all moving in the right direction.

There's a kink though. Many organizations still consider their IT equipment manufacturers, their subsidiaries, component suppliers, and third parties to be trusted entities. These organizations have ensured in their contracts that liability clauses exist and cover potential monetary damages. This viewpoint is a reactionary action and wholly against the concepts of a zero trust framework.

We are at a precipice where third-party risk management will grow into supply chain risk elimination, a true zero trust perspective. These third-party entities will no longer be trusted, and our purchases will need to go through a full digital verification to ensure trust. Legislation and leaders have already begun emerging racing toward these objectives. We have the technology pieces available that can ensure integrity of systems, components, and information. It's time to put them together and leverage them.

I call this "Trust through Transparency." A concept that promotes zero trust through transparent, and continuous, validation of integrity. Equipment should tell us what it is, what it's been, and when it changed. Thereby extending trusted computing capabilities into the manufacturing, build, and delivery processes by using integrity measurements at various phases, comparing these to identify changes, and maintaining artifacts that can be independently verified. This enables us to know, and validate, the state of a device long before it enters our environment and can be used as a gate control before a system ever touches critical data. Ultimately, giving us early warning to potential tampering, but also giving us a retroactive view if new information is uncovered in the future to assist in determining risk and blast radius.

For this to be successful, all equipment providers need to adopt capabilities of sharing these generated platform certificates and manifests in ways that provide the transparency necessary for independent verification. Consider investigating what your equipment manufacturers, and your value-added resellers, are doing to allow you to ensure equipment hasn't been tampered, or changed negatively, through the build and delivery processes.

Eclypsium and Intel recently announced a partnership designed to help with this. Leveraging the capabilities and technology of Intel's Transparent Supply Chain, a device's integrity can be measured early in the process and validated independently. Its integrity can then serve as a baseline to measure against as the device changes hands. Additional inspections and measurements via Eclypsium's Supply Chain Risk Platform can be taken at any, and all, additional steps in the process to compare and note any changes to hardware, firmware, or configurations of the platform. This exposes if any tampering, unwanted changes, and risks are introduced before you get your hands on the equipment, or more importantly, before that equipment touches anything in your environment. Validating a largely missed component in many organizations zero trust strategies.

TAKEAWAYS_

- Zero-trust needs to apply before receiving the equipment
- Technology exists to perform this validation, but has not been put together to-date to provide a scalable solution organizations can use
- Validating platform integrity, history, and change can be used to control initial access to critical information
- Eclypsium and Intel are now partnering to help drive transparency in the manufacturing processes of equipment
- Ask your manufacturers, and VARs, what evidence they're providing to ensure integrity of equipment

INDUSTRY NEWS

Compliance Frameworks Normalizing on Integrity Controls

In the last edition of Below the Surface, we mentioned that CJIS Security Policy was updated to align with NIST 800-53 Rev 5's controls in relation to hardware, firmware, and information integrity. Dramatically expanding the control requirements for any organization to access CJIS data.

This trend has continued with the recent updates to the Centers for Medicare & Medicaid Services (CMS) Acceptable Risk Safeguards (ARS), which explicitly defines the minimum security controls required for protecting CMS data. As with the CJIS Security Policy, CMS ARS has lifted SI-7 – Software, Firmware, and Information Integrity controls from NIST 800-53 Rev 5 with slightly adjusted language.

a. Employ integrity verification tools to detect unauthorized changes to software, firmware, and information; and

b. Take the following actions when unauthorized changes to the software, firmware, and information are detected: e.g., parity checks, cyclical redundancy checks, cryptographic hashes.

This alignment of frameworks emphasizes the need for organizations to monitor the hardware, firmware, and configurations of devices for change and known-good states. These new control requirements strive to reduce risk imposed by supply chain attacks and add a layer of monitoring controls to identify indicators of attack in sophisticated attacks.

TAKEAWAYS_

- Many compliance frameworks are adding firmware controls
- Validating integrity and change of all layers is paramount to security baselining
- Organizations that access CMS data need to be prepared to implement these controls