UNC5221's Latest Exploit: Weaponizing CVE-2025-22457 in Ivanti Connect Secure

By Sıla Özeren Hacıoğlu

Published: 2025-04-17 · Archived: 2026-04-29 02:12:34 UTC

Who Is the China-Nexus Group UNC5221?

UNC5221 is a suspected China-nexus cyber-espionage group known for aggressively targeting edge network devices (VPNs, firewalls, routers) with zero-day exploits since at least 2023 [1]. The group has repeatedly compromised Ivanti's Pulse Connect Secure/Ivanti Connect Secure (ICS) VPN appliances through multiple vulnerabilities, demonstrating a knack for quickly leveraging new flaws.

In mid-March 2025, UNC5221 launched a fresh campaign exploiting a critical Ivanti Connect Secure vulnerability (CVE-2025-22457) to gain unauthorized access to organizations' networks. This latest activity involves deploying custom malware on compromised VPN appliances and aligns with a broader trend of Chinese state-sponsored attackers focusing on internet-facing infrastructure for espionage [2]. The campaign has impacted organizations globally (including U.S.-based targets), underscoring the threat to government and enterprise networks.

The Ivanti Connect Secure Vulnerability (CVE-2025-22457) Explained

On April 3, 2025, Ivanti publicly disclosed CVE-2025-22457, a critical stack-based buffer overflow affecting Ivanti Connect Secure VPN appliances (version 22.7R2.5 and earlier) [1]. The flaw also impacts related Ivanti products – Ivanti Policy Secure and Ivanti Zero Trust Access (ZTA) gateways – as well as legacy **Pulse Connect Secure 9.x** devices (which reached end-of-support in late 2024) [3].

Initially, Ivanti had mischaracterized this issue as a non-exploitable product bug due to the buffer being limited to only certain characters (periods and numbers). It was first thought to pose at most a low-risk denial-of-service condition [4]. A patch was quietly issued on February 11, 2025 (ICS version 22.7R2.6), without a CVE at the time [5].

Reassessment as Critical RCE

In reality, CVE-2025-22457 turned out to be exploitable for unauthenticated remote code execution (RCE). Ivanti discovered in late March that a determined attacker could weaponize this buffer overflow despite the character input limitations.

UNC5221 likely reverse-engineered Ivanti's February patch – diffing the code changes in ICS 22.7R2.6 – to understand the underlying vulnerability and devise a sophisticated exploit that works on unpatched versions (22.7R2.5 and earlier).

By mid-March 2025, active exploitation in the wild was detected against vulnerable ICS 22.7R2.5 and Pulse Secure 9.x appliances. Ivanti subsequently upgraded the severity to CVSS 9.0 (Critical) and urged all customers to immediately upgrade to the fixed version 22.7R2.6 or later.

Notably, Ivanti reported that a *"limited number of customers"* running ICS 22.7R2.5 (or older) and Pulse 9.x were breached, while no incidents had (yet) been observed on Policy Secure or ZTA gateways.

Nature of the Exploit

CVE-2025-22457 arises from a memory buffer overflow in the ICS web service code. The exploit requires crafting input within a restricted character set, making development non-trivial.

UNC5221's exploit likely involved **careful manipulation of memory** to achieve code execution without crashing the service. According to security researchers, the adversary's method was complex: by studying Ivanti's patch, they figured out a way to bypass the original input limitations and execute arbitrary code remotely. In practice, the attackers were seen sending repeated HTTP requests to a target appliance – likely probing for the ICS version or vulnerability state – before launching the exploit payload. Once successful, the exploit grants the attacker *unauthenticated* access to run code with high privileges on the VPN appliance, effectively opening the door to the victim's internal network.

Analyzing UNC5221's Advanced Tactics, Techniques, and Procedures (TTPs)

After exploiting CVE-2025-22457 to compromise an Ivanti Connect Secure appliance, UNC5221 employs a variety of tactics, techniques, and procedures (TTPs) to expand their foothold, evade detection, harvest credentials, and ultimately fulfill their espionage objectives.

The following breakdown maps UNC5221's known behaviors to MITRE ATT&CK categories:

Initial Access (TA0001) – Exploiting the VPN Gateway

T1190 – Exploit Public-Facing Application

UNC5221 gains initial access by exploiting the public-facing ICS VPN appliance via the CVE-2025-22457 vulnerability. This technique falls under *Exploitation of Public-Facing Application (T1190)*. The attacker targets an organization's VPN gateway (which is accessible from the internet) and sends a specially crafted request to trigger the buffer overflow and execute code on the device.

Before attempting exploitation, UNC5221 was observed performing reconnaissance of the appliance's version – for example, sending repeated queries to deduce the ICS firmware build – ensuring the target is a vulnerable version (22.7R2.5 or older). Once confirmed, the zero-day (now n-day) exploit is launched, providing the attacker a shell or code execution on the VPN appliance without any valid credentials.

This direct compromise of a network edge device serves as the beachhead for the rest of the intrusion.

Execution (TA0002) – Deploying Malware in Memory

Following successful exploitation, UNC5221 executes a *multi-stage malware deployment sequence* on the compromised device. The initial payload is a **shell script dropper** delivered via the exploit. This script runs directly on the Ivanti appliance and orchestrates the loading of further malicious code:

T1055.002 – Process Injection: Portable Executable Injection

In-memory Dropper: The shell script writes an executable to /tmp/.i (among other temp files) and then launches it. This binary is the TRAILBLAZE dropper – a lightweight implant written in C that uses raw syscalls and exists only in memory. When run, TRAILBLAZE searches for the running ICS web process (named web) and injects a malicious code hook into it, effectively *hollowing out* a portion of the legitimate process to load the next stage.

Backdoor Injection: Upon injecting a hook, TRAILBLAZE reads a payload from the temp files (written by the script) and injects the backdoor into the target process's memory space. The backdoor is a stealthy implant called BRUSHFIRE, which is inserted into a "code cave" of the web process and not saved to disk. This means the malware runs within the context of the legitimate VPN service process.

T1070.004 – Indicator Removal on Host: File Deletion

Cleanup: The shell script and TRAILBLAZE perform cleanup actions after execution. The script deletes the temporary files it created (containing the malware and process info) and even clears the appliance's core dump directory to erase evidence. It then kills child processes of web (likely to restart a fresh instance with the injected code) before removing any remaining markers. This ensures that, aside from the injected code in memory, little trace of the attack files remains on the device.

This entire sequence is non-persistent – the malicious code resides only in memory. However, as long as the appliance is not rebooted or the web service is not restarted, the BRUSHFIRE backdoor will remain active inside the process to execute attacker commands.

In effect, UNC5221 leverages the exploit to run a fileless malware deployment, giving them an active implant on the device while minimizing artifacts on the filesystem.

Defense Evasion (TA0005) – Staying Hidden on the Appliance

UNC5221 demonstrates numerous defense evasion techniques to avoid detection on the compromised ICS appliance:

In-Memory Implants: By using an in-memory dropper and injecting the backdoor into an existing process, the attackers avoid leaving obvious binaries on disk. The TRAILBLAZE dropper and BRUSHFIRE backdoor run in memory only, and the temporary files used are deleted immediately after use. This makes forensic detection more difficult, as traditional file-scans or antivirus on the device may not catch the malware.

Process Injection: Injecting into the trusted web process provides camouflage. The ICS device's VPN service process continues to run normally (handling VPN connections) while also harboring the hidden backdoor thread. Security monitoring that looks for new processes or suspicious services might not notice anything unusual since the malware piggybacks on a legitimate process.

Log Tampering: UNC5221 deploys a log-manipulation tool dubbed SPAWNSLOTH to disable or falsify logging on the appliance. SPAWNSLOTH targets the ICS logging service (dslogserver process) to suppress local logs and syslog forwarding, effectively blinding administrators to malicious activity. By halting log generation, the attacker can operate with reduced chance of triggering alerts.

Clearing Traces: Even prior to deploying SPAWNSLOTH, the attackers take manual steps to clear traces. For example, the malicious shell script issues commands like dmesg -c to clear kernel logs and may purge security audit logs. Researchers also noted that UNC5221 attempted to modify Ivanti's built-in Integrity Checker Tool (ICT**)** – a utility meant to detect appliance tampering – likely to prevent it from reporting the changes made by the attackers. By patching or disabling security controls (like the ICT) on the device, the attackers further evade detection.

Passive Backdoor Communication: The BRUSHFIRE backdoor is designed as a *passive* implant, which is another evasion tactic. Rather than actively reaching out to a command-and-control server (which could be noticed as anomalous outgoing traffic), BRUSHFIRE sits quietly and monitors inbound VPN traffic. It hooks into the SSL/TLS functions of the web process and checks each inbound packet for a secret "trigger" pattern.

Only if a packet contains the attacker's magic string does it decrypt an embedded payload and execute it as shellcode in memory. This means the backdoor does not beacon or create a separate network connection – it blends into normal VPN traffic and *only* responds when the operator sends a specially crafted packet. This stealthy C2 method makes the malware nearly invisible on the network, as an observer would just see typical VPN connection traffic.

Obfuscation of Source: Outside the appliance, UNC5221 also conceals their operational infrastructure. Researchers reports that the group routes its intrusion traffic through a network of compromised intermediary devices – including hijacked Cyberoam VPN appliances, QNAP NAS devices, and ASUS routers – to mask their true origin. By tunneling their commands through these third-party systems, the attackers make it very difficult for defenders to trace the activity back to the operators (a technique akin to using multiple VPNs or proxies). This OPSEC measure is common for nation-state actors and contributes to evading detection and attribution.

Overall, UNC5221's defense evasion ensures that once the ICS device is compromised, the intrusion can persist undetected for a significant time. Disabling logs and security tools deprives defenders of visibility, while the passive, in-memory backdoor and cunning use of trusted processes make the malicious presence extremely hard to spot through normal monitoring.

Credential Access (TA0006) – Stealing Passwords and Keys

Stealing valid credentials is a priority for UNC5221, enabling deeper access into victim networks. The group employs multiple techniques to harvest credentials from the compromised VPN appliance and its connected environment:

T1556.002 – Modify Authentication Process: Network Device Authentication

Authentication Log Hijacking: UNC5221 has deployed a custom Python-based credential stealer, internally named DRYHOOK, on Ivanti appliances. This malware patches the appliance's authentication routines (the DSAuth.pm

Perl module in ICS) to capture usernames and passwords in plaintext as users log in.

Essentially, DRYHOOK inserts a malicious subroutine into the login flow: whenever a VPN user successfully authenticates, their username and password are appended (after RC4 encryption and Base64 encoding) to a hidden file on the appliance (/tmp/cmdmmap.kuwMW). This allows the attacker to silently collect VPN user credentials (including potentially administrator accounts) as they are entered, bypassing any encryption. The malware even remounts the filesystem as read-write to insert its changes and then restores it to read-only to avoid suspicion, before killing processes to apply the new modified authentication logic. By the time it's done, the appliance's login system is effectively trojanized to keystroke-log all future VPN logins for the attacker.

T1056.003 – Input Capture: Web Portal Capture

Web Portal Credential Stealer: In earlier campaigns, UNC5221 leveraged a JavaScript-based sniffer known as WARPWIRE that was injected into the VPN web portal to steal credentials. WARPWIRE would capture usernames/passwords from users' web VPN logins and exfiltrate them. This shows the group's familiarity with multiple methods of credential harvesting on Ivanti platforms.

T1552.001 – Unsecured Credentials: Credentials In Files

Dumping Cached Credentials and Keys: The ICS appliance itself stores session data and authentication artifacts that UNC5221 harvests. Security researchers observed the attackers dumping the appliance's cached database (/runtime/mtmp/lmdb) which can contain VPN session tokens, cached credentials, API keys, and even cryptographic keys or certificates used by the VPN. By obtaining this cache, the attacker might extract things like session cookies (to impersonate users) or password hashes/tokens. Ivanti warned that such cache dumps could contain sensitive credential material and require remediation (password resets, key revocations) if compromised.

T1078 – Valid Accounts

Leveraging Stored Credentials for Lateral Movement: Once the VPN appliance is compromised, any credentials stored on or accessible through it become tools for the attacker. UNC5221 was observed using the appliance's configured LDAP service account (if one was set up for corporate directory integration) to query the organization's Active Directory and even to pivot further into the network.

Specifically, the attacker took the service account username/password (which the ICS uses to look up user entries in AD) and performed LDAP queries to gather information. In some cases, they then used those credentials to move laterally onto Windows systems (e.g., connecting to domain controllers via SMB/RDP). This indicates the appliance was a stepping stone: any privileged account that the VPN had knowledge of was co-opted by the attacker to expand access inside the network. In summary, the ICS device often holds a *key to the kingdom* (service accounts, admin logins, etc.), and UNC5221 wastes no time exploiting those to escalate their reach.

Through these methods, UNC5221 can accumulate a trove of credentials: VPN user logins (for continued access or future phishing), internal directory accounts (for lateral movement), and administrative passwords or keys (for privilege escalation). Credential Access is a critical stage in their operation, as it enables them to authenticate as

legitimate users and persist in the network even if the initial vulnerability is patched or the backdoor is discovered.

Discovery (TA0007) – Reconnaissance of Internal Environment

After compromising the VPN gateway, UNC5221 conducts extensive reconnaissance to understand the victim environment and identify further targets. The compromised ICS appliance, now under attacker control, serves as a vantage point to probe the internal network:

T1046 – Network Service Discovery

Network Scanning: The threat actor uses utilities available on the appliance (or uploads their own) to scan the internal network. In observed cases, UNC5221 executed tools like nmap (for port scanning) and dig (for DNS lookups) directly from the VPN appliance. For example, they ran scans to detect hosts on specific ports (80, 443, 445, etc.) and DNS queries for internal domain names. Since the appliance sits at the network edge (often with access to internal subnets), this allows mapping of the internal IP space, discovering servers, domain controllers, and other critical systems that might be reachable from the VPN segment.

T1057 – Process Discovery & T1007 – System Service Discovery

Process and System Survey: The attackers show detailed knowledge of the Ivanti appliance's processes and files. The initial shell script explicitly **searched for a specific process (/home/bin/web) that is the child of another web process** to target for injection. This indicates they are performing **process discovery** on the device to ensure their payload hooks into the correct service (the one handling incoming connections). They also dumped memory maps and module base addresses (libssl.so, etc.) of processes, likely to assist in calculating offsets for injection. Such actions reveal the attackers are interrogating the system's state in real time. Additionally, by examining configuration files or environment variables on the appliance, they can learn about how it's connected to the network (e.g., learning the internal IP ranges, DNS servers, configured authentication servers, etc.).

T1069.002 – Permission Groups Discovery: Domain Groups

Directory Service Enumeration: Using the stolen or available credentials, UNC5221 queries the organization's directory services. As noted, they performed LDAP queries via a tool (/tmp/lmdbcerr) to retrieve information from Active Directory. The commands show they queried for user and group objects (with filters like (cn=*) or (distinguishedName=*)) and likely pulled large chunks of AD data, saving the outputs to files on the appliance. This suggests they were building a map of user accounts, groups, and possibly computer accounts in the domain – valuable information for understanding the organization's structure and planning further actions. Discovery of such directory info is common in espionage to identify high-value accounts or systems.

T1518.001 – Software Discovery: Security Software Discovery

Environment Observation: The attackers also seek information about security measures. Disabling the ICS Integrity Checker Tool implies they were aware of its presence (which itself is a form of discovery – recognizing active security controls). By inspecting the system, they can determine if additional security agents or monitors

are running (though many VPN appliances lack traditional antivirus or EDR by design). UNC5221's attention to what's running on the appliance (and removal of anything that might report their activity) is part of discovering and neutralizing defensive sensors.

In summary, UNC5221 systematically gathers intel on the network from their beachhead. They leverage the compromised VPN's perspective to scan internally, enumerate critical services (like AD), and learn the layout of the victim network. This Discovery phase sets the stage for selecting targets for data collection and lateral movement.

Collection (TA0009)

As an espionage actor, UNC5221's end goal is to collect valuable information. Once they have a foothold and knowledge of the environment, they move to gather and prepare data for exfiltration:

T1005 – Data from Local System

Capturing VPN Appliance Data: One of the first targets for collection is the VPN appliance itself. UNC5221 archives the VPN appliance's session database cache, which resides in the directory /runtime/mtmp/lmdb. This cache database can contain a wealth of sensitive data: active VPN session details, user authentication records, session cookies, tokens, **API keys**, and even TLS certificates used by the appliance. By stealing this, the attackers potentially obtain authentication session cookies (which could allow them to hijack active sessions or replay them), API secrets (if the VPN was integrated with other systems), and private keys or certificates (which could enable decrypting VPN traffic or impersonating the VPN server). The threat actor bundles up this database – Researchers observed them tar-ing the contents of the lmdb cache – as a convenient package of intel.

T1036.008 – Masquerading: Masquerade File Type

Masquerading Data as Legitimate Files: After archiving the data, UNC5221 masquerades the stolen files to blend in. In a reported case, they took the tarball of the database dump and renamed it with a **.css** extension, placing it in the VPN appliance's web directory (/home/webserver/htdocs/dana-na/css/). By doing so, they stage the data to appear like a harmless stylesheet file on the VPN web portal. This is a clever preparation for exfiltration – the data can be downloaded over HTTPS from the appliance by the attacker (or automatically by their script) without raising immediate suspicion, as it looks like a normal web resource. It also means the exfiltration traffic will be encrypted (since it's pulled via HTTPS from the VPN web server), making it harder for network monitoring to detect sensitive data being taken out.

T1005 – Data from Local System

Extracting System Images: UNC5221 also deployed a tool called SPAWNSNARE on some appliances, which is used to extract the device's Linux kernel image (vmlinux) and encrypt it using AES. Stealing the kernel memory image might not be directly about business data, but it is likely done for technical espionage – for instance, to analyze the kernel for additional vulnerabilities or to assist in developing rootkits. By encrypting the extracted kernel before storing or exfiltrating, the attackers ensure that even if the file is found, its contents are not

immediately obvious to defenders. This indicates a high level of sophistication; the actor is interested not just in organizational data, but also in the underlying technology of the device, possibly to enable future exploits.

T1039 – Data from Network Shared Drive

Internal Data Access: With credentials in hand and knowledge of the network, UNC5221 can also directly collect data from internal systems. For example, if they used the VPN's service account to access a file share or a database inside the network, they might retrieve documents, emails, or database records relevant to their intelligence goals. In earlier incidents, Chinese actors exploiting Pulse Secure devices have been known to deploy web shells or tools on internal servers to gather files. While specific files stolen in the UNC5221 campaign have not been detailed publicly, it is typical for such an actor to siphon any accessible sensitive information (e.g. files on SharePoint, email servers, or databases that the compromised credentials can reach).

By the end of the Collection phase, UNC5221 has packaged up both device-resident data (logs, caches, configs) and potentially business data from the victim's network. The data is staged in a manner conducive to exfiltration – often compressed and placed in known locations or encrypted for safety. This careful staging is a precursor to the final step of exfiltration.

Exfiltration (TA0010) – Extracting Data Without Detection

UNC5221 exfiltrates the collected data through stealthy means to avoid setting off alarms:

T1041 – Exfiltration Over C2 Channel

Using the Victim's Own Infrastructure: As noted, the group often places stolen files on the appliance's web server directory disguised as legitimate content (e.g., a .css file).The attackers can then download this file over HTTPS from the appliance at their leisure. From a defender's view, this might appear as the VPN appliance serving a normal file to an external IP – not immediately suspicious, especially if the request closely follows patterns of legitimate file accesses. By piggybacking on the victim's infrastructure (the VPN's web interface), the exfiltration traffic hides in plain sight.

Passive Backdoor Channel: The BRUSHFIRE passive backdoor also provides a means to exfiltrate data on-demand. Because it executes commands sent via specially crafted packets, the attackers could instruct BRUSHFIRE to read files (such as the cached credentials or collected data) and send the output back, embedded in the response. The backdoor would then use the normal VPN SSL connection to write back the results (it calls SSL_write with the output) to the attacker. This method keeps the exfiltration within the VPN's normal traffic flow. However, using BRUSHFIRE requires the attackers to actively trigger it with a command that says, in effect, "send me the contents of file X," after which the data would be covertly transmitted out in the SSL response.

T1572 – Protocol Tunneling

Tunneling and Proxying: In previous operations, UNC5221 has installed tunneling tools like PySoxy (a Python SOCKS proxy) to channel data through the compromised device. A tunneler can allow the attackers to route traffic from internal systems out through the VPN appliance. For example, they could copy large files from an internal server to the VPN appliance and then out to the internet via an encrypted tunnel. They also utilized utilities like

BusyBox on the appliance to facilitate data transfer and scripting. Combined with their external obfuscation network (compromised proxies), the group can chain connections in a way that the data's path out to their controlled server is non-obvious.

T1020 – Automated Exfiltration

Exfiltration Over Time: Rather than a one-time giant transfer (which might be noticed), UNC5221 likely exfiltrates data in smaller chunks or during times that blend in with normal traffic. For instance, transferring the fake .css file (which contains the cache dump) could be done during off-peak hours or multiple smaller archives could be staged. The attackers can maintain persistence on the device to periodically collect and exfiltrate new data as well, extending the data theft over weeks if undetected.

In essence, UNC5221's exfiltration methods are low-and-slow and camouflaged. By making exfiltration traffic appear routine (HTTPS requests to the VPN, or responses to legitimate-looking sessions), they evade many data loss prevention controls. Any external network monitors would see encrypted traffic that appears to be typical VPN usage or web requests, thus blending the exfiltration with regular operations.

How Does Picus Help Defend Against the China-Nexus Threat Group UNC5221?

We strongly suggest simulating ransomware groups to test the effectiveness of your security controls against their attacks using the Picus Security Validation Platform.

The **Picus Threat Library** includes the following threats related to UNC5221 and the exploitation of Ivanti Connect Secure (CVE-2025-22457).

Threat ID	Threat Name	Attack Module
38486	UNC5221 Threat Group Campaign Malware Email Threat	E-mail Infiltration
81651	UNC5221 Threat Group Campaign Malware Download Threat	Network Infiltration
64333	SPAWNSNARE Utility Download Threat	Network Infiltration
68529	SPAWNSNARE Utility Email Threat	E-mail Infiltration

20144	Ivanti Connect Secure CVE-2025-22457 Exploiting Vulnerability Download Threat	Network Infiltration
39508	Ivanti Connect Secure CVE-2025-22457 Exploiting Vulnerability Email Threat	E-mail Infiltration

Defense Strategies Against the Billbug Threat Group's Attacks

To mitigate the impact of Lotus Blossom attack campaigns, organizations should adopt a layered defense approach:

Patch and Retire Vulnerable Ivanti Appliances Immediately

UNC5221 exploited CVE-2025-22457 in unpatched Ivanti Connect Secure (ICS) and legacy Pulse Secure VPN devices. Organizations should upgrade all ICS appliances to version 22.7R2.6 or later, and decommission unsupported Pulse Connect Secure 9.x devices. Apply vendor-recommended hardening guides, and monitor Ivanti advisories for additional mitigations. If your environment contains affected versions, assume compromise and perform a full investigation, including integrity checks and credential revocation.

Detect Fileless Malware and In-Memory Backdoors on ICS Appliances

UNC5221 deployed in-memory implants (TRAILBLAZE, BRUSHFIRE) that evade traditional disk-based detection. Deploy file integrity monitoring and memory inspection tools where possible. Use the Ivanti Integrity Checker Tool (ICT) to verify the appliance state, and hunt for indicators such as unusual files in /tmp, high-privilege processes modifying web, or unauthorized memory access patterns. Monitor for tools like SPAWNSLOTH that suppress syslog activity.

Continuously Test and Validate Security Controls

UNC5221 follows a clear sequence of behaviors. Implementing Breach and Attack Simulation (BAS) platforms, such as Picus Security Control Validation (SCV), enables security teams to emulate realistic, multi-stage attack scenarios that mirror the tactics, techniques, and procedures (TTPs) observed in UNC5221 campaigns.

By continuously testing your environment against these scenarios, BAS tools can expose blind spots, validate existing controls, and generate actionable insights to improve detection and response capabilities—helping you stay one step ahead of sophisticated adversaries.

Monitor for LDAP Abuse and Credential Theft

UNC5221 leveraged compromised LDAP service account credentials to query Active Directory and move laterally. Monitor for LDAP queries originating from ICS appliances, especially those requesting broad object filters (e.g., cn=*, distinguishedName=*). Use behavior analytics to flag unexpected access patterns and high-

volume directory lookups from non-domain joined systems. Ensure VPN appliances have the least-privileged service accounts with read-only permissions.

Harden and Segment Network Access to VPN Infrastructure

Prevent compromised ICS appliances from serving as lateral movement pivots. **Restrict outbound connectivity** from VPN appliances to only required services. Apply **network segmentation** and isolate appliances from internal subnets that do not require direct access. Monitor for **unexpected outbound HTTPS traffic** and inspect for disguised exfiltration (e.g., .css or .zip downloads from ICS web directories). Enforce strong authentication and regularly rotate credentials stored or cached on appliances.

References

[1] “Suspected China-Nexus Threat Actor Actively Exploiting Critical Ivanti Connect Secure Vulnerability (CVE-2025-22457),” Google Cloud Blog, Apr. 03, 2025. Available: https://cloud.google.com/blog/topics/threat-intelligence/china-nexus-exploiting-critical-ivanti-vulnerability. [Accessed: Apr. 16, 2025]

[2] R. Wright, “CISA adds Ivanti Connect Secure vulnerability to KEV catalog,” Cybersecurity Dive, Apr. 07, 2025. Available: https://www.cybersecuritydive.com/news/cisa-ivanti-connect-secure-vulnerability-kev/744603/. [Accessed: Apr. 16, 2025]

[3] M. Kapko, “China-backed espionage group hits Ivanti customers again,” CyberScoop, Apr. 03, 2025. Available: http://cyberscoop.com/china-espionage-group-ivanti-vulnerability-exploits/. [Accessed: Apr. 16, 2025]

[4] “Website.” Available: https://www.darkreading.com/vulnerabilities-threats/china-linked-threat-group-exploits-ivanti-bug

[5] “Website.” Available: https://www.securityweek.com/rapid7-reveals-rce-path-in-ivanti-vpn-appliance-after-silent-patch-debacle

---