STRATEGIC INTELLIGENCE DIVISION

A disk check cannot see root that stayed in memory

An unknown actor held root on a fully patched Ivanti Connect Secure appliance from 3 October 2026, and the vendor’s Integrity Checker Tool inspects disk only, where this chain left nothing. Ivanti patched the bypass and code execution on 13 October, the privilege escalation on 29 October. Network monitoring caught what the device could not, and the clock that matters is the one to a reader.

Annika Sorensen, Strategic Intelligence Division · 3 November 2026 · 11 minute read

In brief

- 26 days separated the first observed exploitation, on 3 October 2026, from the patch that closed the chain, and for the first 10 of them no fix existed for any part of it.
- The appliance was the entry point and not the prize: the directory query behind it was written to fetch LAPS local administrator passwords and BitLocker recovery keys, so the remediation is a rotation of the endpoint fleet and not a patch window.
- Network monitoring flagged the intrusion at 2 days, because the exploit channel was the command channel and the device had nothing on disk to report.
- An open-source framework moved an operator from agent deployment to domain administrator in three to four days, with persistence and local reconnaissance inside 2 minutes.
- Chainalysis kept transaction monitoring running and took Reactor and Data Solutions offline, so its customers lost reconstruction and kept surveillance, on the vendor’s reading of their obligations.

One appliance, four controls, and the one that could not have seen it

Control	What it establishes
Patch status	Fully patched, version 22.8R2.4, Build 19097
Ivanti Integrity Checker Tool	Inspects disk only: “the tool does not detect any modifications”
Device debug log and Linux audit log	Exploitation entries removed by the payload
Network security monitoring	Suspected malicious activity flagged, 2 days after exploitation began

Volexity, A Series of Unauthenticated Events: Chained Exploitation of Ivanti Connect Secure Zero-Days, 13 October 2026, updated 29 October 2026. The version string, the log removals and the tool’s stated scope are quoted from that report; Mosaic Singularity analysis, November 2026.

Volexity puts the first exploitation on 3 October 2026, against an appliance it records as “fully patched (at the time, version 22.8R2.4)”. Ivanti shipped the fix for the authentication bypass and the remote code execution on 13 October and the privilege escalation fix on 29 October. The arithmetic a CISO inherits is 10 days with no fix for any part of the chain, and 26 before a complete one. The lever inside that window is not a patch cadence. It is whether the appliance answers the public internet at all, and whether the estate can pull memory off it before the evidence is gone.

Control sat with the vendor for 26 days

The chain needed three flaws. An authentication bypass in welcome.cgi routed requests to arbitrary CGI files, including those behind authentication. A file write in wu.cgi became execution through a race between the write and the delete, which the actor won by firing parallel requests at the uploaded script before the handler removed it. A flaw in how the dsinvoked broker trusts DSCache configuration data turned that into root. CVE-2026-104935 covers the first two and was patched on 13 October. The third is tracked as CVE-2026-111357 and had no patch until 29 October.

Volexity states that the exploits affect versions up to 22.8R2.4, Build 19097, “which at the time of writing is the latest version”. That is the sentence a patch report cannot absorb: the device was current, and currency was not the control. Across 26 days without a complete fix, an operator has two moves and neither is a release date. Take the appliance off the public internet, or accept that a three flaw chain has to be caught on the way in.

The alarm came off the wire, not off the disk

Almost nothing durable was written to the device. UTA0576 “passed commands and results through the exploit chain’s HTTPS requests rather than a separate command-and-control (C2) channel, with no backdoor or web shell deployed to the compromised device”, so every command re-ran the chain and the HTTP response carried the output back. After root, the script restored the DSCache entry to the legitimate script and restored the library it had patched in memory, then rewrote the debug log and the audit log.

Volexity states what the tool covers, and not what it returned: the chain “patches library code in memory only and restores configuration store data, the tool does not detect any modifications”. The tool inspects the disk, and this compromise was never on the disk, so it would have had nothing to report on the day it was owned or on the day anyone looked.

Days from the first observed exploitation on 3 October 2026 to each defender milestone



Volexity, 13 October 2026, updated 29 October 2026, and Ivanti’s patch of 29 October 2026. Intervals are counted from 3 October 2026, the date Volexity records as the start of exploitation; Mosaic Singularity analysis, November 2026.

The fastest defender move was the alarm, and it came from outside the device. On 5 October, two days in, Volexity began an investigation into suspected malicious activity at a customer receiving its network security monitoring and identified the appliance as the root cause. What found it was the shape of the traffic the chain had to produce. Volexity advises monitoring for volume against the welcome.cgi path, and more tellingly for mismatches between the URL path and the X-DSCGI-PATH header, because the URL decides whether a request is allowed while the header decides where it goes.

The two controls that could see this intrusion were a packet and a memory image. Patch status and an integrity check are neither, which is why the retrospective question differs from the one most security budgets answer. Volexity reconstructed the chain from memory and disk images and from core dumps generated by the exploitation, and recommends that a suspected compromise be met with network and memory forensics. That is a capability with an acquisition step: a tool that runs on the appliance, somewhere to put the image, and an

analyst who can spot a renamed packet capture in a process table.

The appliance was the entry point, not the exposure

UTA0576 spent its time on credentials, and the directory was the deepest source. Volexity records a custom Python LDAP tool deployed “to search Active Directory for LAPS local administrator passwords, BitLocker recovery keys, and password-bearing attributes”, over an authenticated directory account the appliance held, and Volexity “assesses with high confidence that UTA0576 exfiltrated information that could be queried from the target’s Active Directory”.

The record shows the query, not its return. Both attributes it was written to fetch are the estate’s own recovery paths. A LAPS password is local administrator access on every machine the policy covers. A BitLocker recovery key is the disk of a lost or stolen laptop opened without the user, which is how one compromised appliance becomes a data at rest question about an endpoint fleet.

That distinction is the General Counsel’s before it is the CISO’s. Where recovery material sat within reach of a remote access appliance, the notification assessment is scoped to the endpoints rather than to the VPN. The remediation is not a patch window either: rotating BitLocker recovery keys and LAPS passwords across a fleet is a project with a change calendar, and it lands on the same team that is still closing the appliance.

The vendor decides which of your capabilities stays up

> **Two products off, one product on, and the reason given**
>
> Chainalysis “detected an external actor using offensive agentic techniques to gain unauthorized access to Chainalysis systems and internal tools”. Its 2 November 2026 update states that “out of an abundance of caution, we have proactively taken certain products offline, including Reactor and Data Solutions”, and gives the reason for what stayed: “Recognizing the importance of our compliance transaction monitoring products to our customers’ businesses, particularly their role in detecting money laundering across the ecosystem”. Reactor is described on the same site as the product to investigate and trace funds across blockchains. The tracing stopped. The monitoring did not.

Every regulated customer now has a dated fact to design against: a security vendor’s incident can remove a reconstruction capability and leave a monitoring capability running, and the vendor chooses between them. The 2 November update carried no reinstatement date. A bank or an exchange whose tracing depended on Reactor had, from that moment, the vendor’s judgement as its fallback, and the judgement was that money laundering detection outranks fund tracing. That is a defensible call. It was made by someone else, on your behalf, on a day you did not choose.

An open-source agent moved the skill floor, not the detection rules

Kaspersky’s account of CyberStrikeAI is the document that does not fit the story being written about automation. It describes an open-source framework “in which an LLM orchestrator on the command-and-control server plans actions, selects tools, and generates commands, while an implant executes them on compromised hosts”. The implant carries no model: it is a classic C2 agent with no AI functionality. The operator defines the task in general terms and the model determines how to execute it, and under the framework’s human in the loop mechanism the commands it generates may require manual approval before they run. The gain is not a new attack. It is the price of the operator.

2 minutes	5 hours	1 hour	3 to 4 days
Persistence and local reconnaissance under the agent	Domain reconnaissance that followed	Lateral movement, credential dumping and database export	Agent deployment to domain administrator

Kaspersky SecureList, CyberStrikeAI in the wild: the use of AI in real-world attacks on organizations, 2 November 2026. The timings are from the incident Kaspersky reconstructed, and the 3 to 4 days runs from agent deployment to compromise of the domain administrators; Mosaic Singularity analysis, November 2026.

The final stage, lateral movement by SMB and WMI with mass credential dumping and a database export, took “no more than one hour”, and the whole operation from agent deployment to compromise of the domain administrators ran three to four days. Kaspersky’s own conclusion is why this is not a coverage story: “the introduction of AI into the attack chain does not yet present fundamentally new challenges for detection”, and “since the actions performed by an AI agent on the network are indistinguishable from those of a human, classic, well-tuned correlation and behavioral analysis rules are sufficient to detect it”.

A rule that fires in real time is only worth the shift around it. If the artefact is generated in the first five hours and the domain falls inside four days, the operating question is who reads the queue at 03:00 on a Sunday, and whether the answer is a rota or a hope. The confirmed victims here were education institutions in Africa and Latin America, which is where a lower skill floor lands first and is not evidence about a Fortune 100 estate. What transfers is the cost of the operator, not the difficulty of the attack.

What each seat owes, and by when

- CISO: count every internet facing management appliance, VPN concentrator and out of band controller, name an owner for each, and record in writing which stay reachable. The chain ran on a fully patched build, so the inventory is the control and the version number is not. By 30 November 2026.
- CISO: fund memory acquisition on the edge estate as a standing capability, meaning a tool that runs on the appliance, storage sized for an image, and an analyst who can read a process table. This intrusion was reconstructed from memory and core dumps after the device’s own logs had been rewritten. By 31 January 2027.
- CIO: if an affected appliance held directory credentials, put LAPS passwords and BitLocker recovery keys through a rotation plan and cost it as a project with a change calendar, not as an incident response task. By 31 December 2026.
- General Counsel: before an incident, decide which systems hold recovery material that a remote access appliance can read, and scope the notification assessment to the endpoints rather than the appliance. By 31 December 2026.
- COO: for every security product inside a regulated process, write down what the business does on the day the vendor takes it offline. Reactor and Data Solutions went offline and transaction monitoring did not, on the vendor’s reading of its customers’ obligations. By 31 December 2026.
- Procurement: add a continuity term to the security supplier review that names the products, the notice given before a shutdown and the reinstatement commitment. The 2 November 2026 update carried no reinstatement date, which is what such a term would have supplied. By 31 December 2026.

The board signs the reachability list by 30 November 2026

- Chair and audit committee, by 30 November 2026: resolve which internet facing appliances, VPN concentrators and out of band controllers stay reachable, each with an owner and a business reason, and the retirement date for every other one. The artefact is the CISO’s inventory; the resolution is what makes it a control.
- Chief executive and General Counsel, by 31 December 2026: determine whether the directory query is treated as a credential compromise or an attempt, and record the basis. Volexity records the query and not its return, so the determination rests on the evidence in hand.

- Board, by 31 December 2026: approve or refuse the standing memory acquisition capability that the CISO funds by 31 January 2027. The intrusion was reconstructed from memory after the device’s own logs had been rewritten, and an unfunded capability cannot be exercised on the night.

What to watch, and when

- Ivanti’s advisory page: whether the Integrity Checker Tool is revised to inspect memory rather than disk. If a vendor ships in memory attestation for an edge appliance before 31 March 2027, the blind spot closes at the tool layer and this reading narrows to response time alone.
- EDGAR: whether a Fortune 500 10-K or 10-Q risk factor names exploitation of an internet facing management appliance. The date that settles it is 31 March 2027.
- Chainalysis: the date Reactor and Data Solutions are restored, and whether any customer discloses disruption. Restored before 30 November 2026 with no customer side loss reported would take most of the weight out of the continuity point.
- CyberStrikeAI: whether a second operator appears on a different build fingerprint. The two groups Kaspersky identified share no common command and control infrastructure, and the framework is open source, so the population of operators is the measure.

The four documents this rests on

- Volexity, A Series of Unauthenticated Events: Chained Exploitation of Ivanti Connect Secure Zero-Days, published 13 October 2026, updated 29 October 2026.
- Ivanti, patches for CVE-2026-104935 and CVE-2026-111357, released 13 October 2026 and 29 October 2026.
- Kaspersky SecureList, CyberStrikeAI in the wild: the use of AI in real-world attacks on organizations, 2 November 2026.
- Chainalysis, Updated Nov 2: Chainalysis Security Incident Information, posted 30 October 2026, updated 2 November 2026.