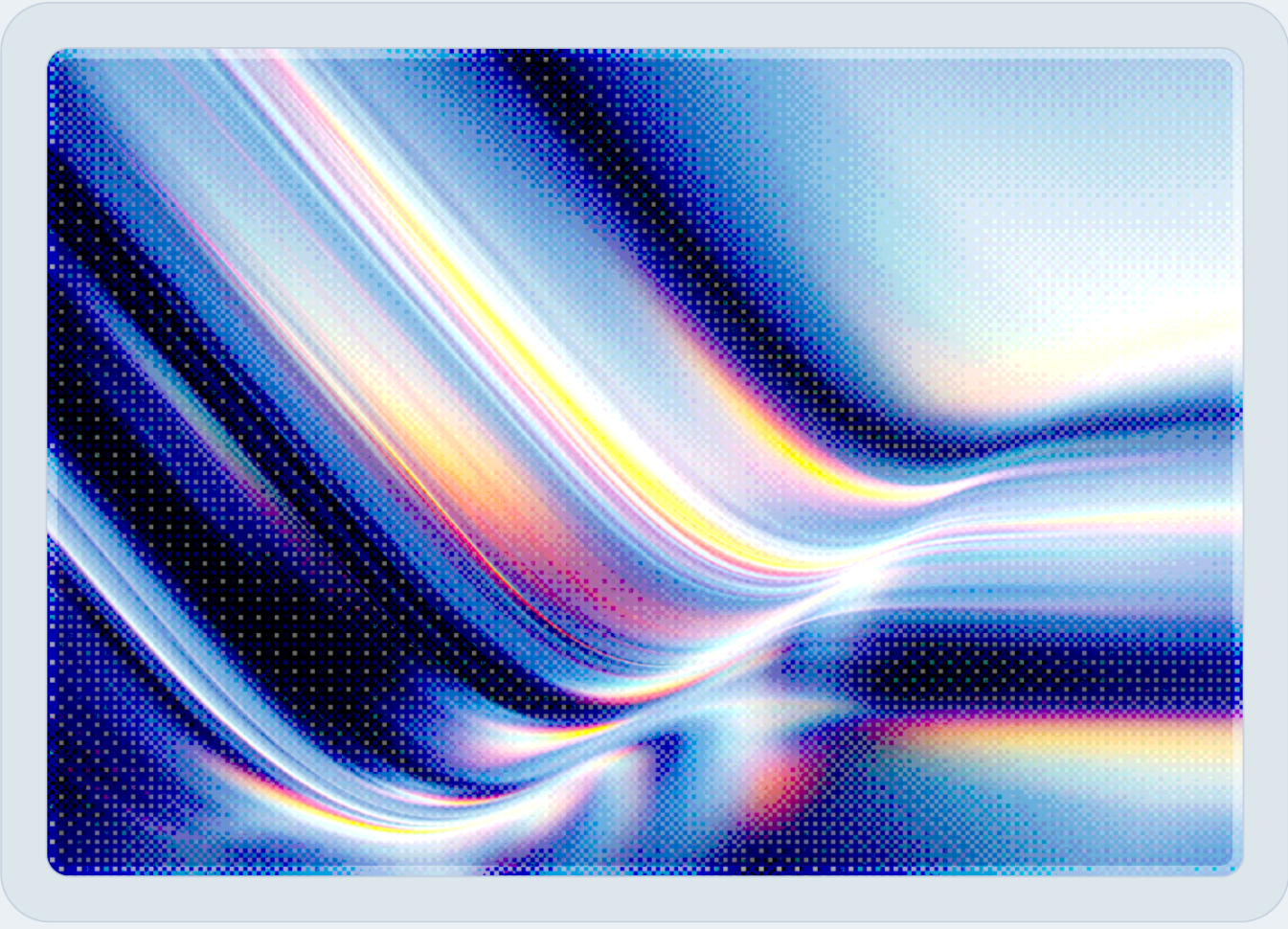
CSAI Foundation | Cloud Security Alliance

ENDLESSDOORS: Factory-Installed Backdoors in Zbtlink Routers

A Trust Problem, Not a Patch Problem

2026-08-06

AI-assisted Rapid Research



CSAI

CSA cloud security alliance®

Key Takeaways

Security firm VulnCheck disclosed on August 5, 2026, that at least twenty consumer and small-business router models manufactured by the Chinese vendor Zbtlink ship with a persistent, factory-installed remote access implant that VulnCheck calls ENDLESSDOORS, tracked as CVE-2026-66747 with a CVSS 4.0 score of 9.3 [1][2][3]. The implant runs as a root-privileged userland process disguised under the name `kworker` to blend in with legitimate Linux kernel threads, and it initiates outbound connections roughly every 35 seconds to four hardcoded command-and-control destinations: two hosted on Alibaba Cloud in mainland China, a third resolving to a separate mainland Chinese cloud provider based in Jiangsu, and a fourth hosted abroad on a Vultr instance [2]. Because the implant calls out rather than listening for inbound traffic, it defeats firewalls and network address translation that would ordinarily shield a device without a public IP address, and because the command channel is unauthenticated and unencrypted, anyone who can reach or spoof those endpoints can obtain an interactive root shell on the router [1][2]. VulnCheck estimates more than 100,000 affected units are in service worldwide under the Zbtlink, ZBT, Wiflyer, and ZBTWiFi brand names, sold through mainstream retail channels including Amazon and Alibaba [4]. Zbtlink has disputed that the code constitutes a backdoor, describing it as an after-sales debugging feature intended only for sample units, even as the company pulled affected firmware from its download portal without a public announcement and posted a notice acknowledging "firmware security vulnerabilities" [1][7]. VulnCheck chose not to pursue coordinated disclosure, arguing that a fix-and-patch timeline presumes an unintentional defect, an assumption the researchers say does not hold here [2]. For defenders, the practical conclusion is that a router carrying this implant cannot be brought back to a trusted state through a firmware update or a password reset; the correct response is identification and replacement [1][2].

Background

Zbtlink is a Chinese original design manufacturer (ODM) that produces routers, gateways, and CPE devices later rebranded and resold by numerous smaller companies under names including ZBT, ZBTWiFi, and Wiflyer, a common arrangement in the budget networking hardware market where a single factory's reference design ships under multiple storefront labels [2][4]. VulnCheck's research team, led by Chief Technology Officer Jacob Baines, purchased an AX3000-class unit from Alibaba to conduct routine firmware analysis and discovered two running processes named `kworker` that, unlike genuine

kernel worker threads, appeared unbracketed in process listings and carried a non-trivial virtual memory footprint, a telltale sign of a userland binary impersonating a kernel thread [2]. Tracing that binary led to a shared library, an init script, and a configuration file consistent across firmware images, and unpacking additional Zbtlink firmware releases going back more than two years showed the same implant present in every version examined, across at least twenty distinct hardware models spanning the CPE2801, WE, WG, and Z8102AX product lines [1][2].

The implant is a lightly modified build of `rctl` ("remote control linux"), an obscure open-source tool uploaded to GitHub in January 2015 that VulnCheck describes as having seen little legitimate adoption [1][2]. The implant was compiled as a startup service, configured to beacon to the four hardcoded command-and-control destinations, and packaged into every firmware image VulnCheck examined, not confined to a debug or engineering build, as Zbtlink's own explanation would suggest [1][2]. The primary destinations, `zbtctl.epplink[.]net` and the raw IP address 47.107.224.89, resolve to Alibaba Cloud infrastructure in Shanghai and Shenzhen respectively; two secondary destinations, `online-string[.]com` and `rbdg4nzqadui.wikaba[.]com`, resolve to a Vultr instance and a Jiangsu-based cloud provider [2]. The protocol itself is minimal by design: the implant sends a 39-byte handshake containing a class identifier and the device's LAN MAC address, and the server can respond with one of exactly two instructions, run an arbitrary shell command as root, or open an interactive reverse root shell on a second port [1][2]. VulnCheck's researchers summarized the entire command set as having only two verbs: "run this as root, and give me a root shell" [1].

VulnCheck disclosed its findings publicly on August 5, 2026, alongside Suricata, Snort, and YARA detection signatures, without first notifying Zbtlink [2][3]. The Hacker News and The Register both sought comment from the vendor; Zbtlink told reporters the functionality is "solely intended for after-sales maintenance" and claimed it is "generally retained only on sample units to assist customers with software debugging," while also stating the company was "working to expedite the implementation of a solution" [1][7]. The Register noted that Zbtlink's download portal began displaying a notice acknowledging "firmware security vulnerabilities affecting selected router firmware releases" and pulled affected images from public download, a step the Wayback Machine shows did not exist as of July 31, in the days before the notice appeared [7]. That timeline is, on its face, in tension with the sample-unit explanation, since the firmware pulled from public download was the same firmware distributed to production customers. Reuters reported that VulnCheck estimates more than 100,000 affected devices are deployed worldwide, though the researchers could not determine how many are active in the United States specifically, and noted that Zbtlink did not respond to its request for comment [4].

Security Analysis

Why This Is Not a Conventional Vulnerability

Router security advisories typically describe a coding defect, a memory-safety bug, an authentication bypass introduced by an oversight, something a vendor did not intend and can therefore patch. ENDLESSDOORS does not fit that pattern. The implant is compiled into every firmware release VulnCheck examined across more than two years and twenty hardware models, uses a persistent init script to survive reboots, and beacons continuously to infrastructure the vendor controls or has selected [1][2]. VulnCheck's advisory classifies the finding under CWE-506, embedded malicious code, rather than under a defect category, and assigned CVSS 4.0 vector AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N, reflecting network-reachable, low-complexity, no-privilege, no-user-interaction access that yields complete loss of confidentiality, integrity, and availability on the device itself [3]. That combination of factors, breadth of coverage across product lines, persistence, unauthenticated remote root, and a vendor denial issued alongside a quiet withdrawal of the same firmware from public download, actions in some tension with each other, is what separates this from a routine unauthenticated RCE finding, and it is why VulnCheck framed its response around identification and replacement rather than coordinated patch timelines [1][7].

The Outbound-Only Design Defeats Perimeter Defenses

Consumer and small-office router security commonly assumes that a device without a public IP address, sitting behind carrier-grade NAT or a firewall, is meaningfully protected from remote compromise. Whether or not by design, ENDLESSDOORS invalidates that assumption directly. Because the implant initiates the connection outward rather than listening for inbound traffic, the session looks, to any conventional firewall or NAT gateway, like ordinary outbound traffic the router itself generated, and it traverses network boundaries the same way a legitimate update check or telemetry call would [2]. VulnCheck illustrated the implication starkly: a unit sitting behind three layers of firewalling in a back office is exactly as reachable as one with a public IP address, provided it can resolve and reach the four command-and-control domains [2]. This is the same operational logic that makes reverse-shell malware effective against enterprise networks, applied here at the factory-firmware level of consumer hardware, and it means that network segmentation and inbound access control lists, while still valuable defense-in-depth, do not neutralize this specific exposure on their own; effective mitigation options are narrow, limited to DNS and egress filtering targeting the known indicators, or removal of the affected device.

Scale, Attribution Ambiguity, and the Broader Chinese Hardware Debate

The scale VulnCheck describes, more than 100,000 units sold globally under at least four brand names through mainstream retail channels, means this is not a niche finding confined to a single product line but a supply chain exposure spanning years of shipping firmware [2][4]. Neither VulnCheck's technical analysis nor subsequent reporting has established who controls the command-and-control infrastructure, whether it has been used to conduct intrusions, or whether the implant reflects state-directed tasking, a contractor's undisclosed debug feature left in production builds, or something else; Reuters explicitly noted that the purpose of the backdoor and whether it has been exploited remain undetermined [4]. That ambiguity does not reduce the operational risk, since the mechanism is functionally identical to a nation-state implant in its operational effect regardless of who controls it or why, a distinction this report deliberately does not resolve, but it should temper attribution claims in downstream reporting and internal risk communications. The disclosure also lands amid an active U.S. policy debate over Chinese-manufactured networking equipment: the Federal Communications Commission banned imports of certain new foreign-made consumer routers in March 2026 citing national security concerns, and the State of Texas sued TP-Link in February 2026 alleging undisclosed access by parties in Beijing, a claim TP-Link has disputed [4]. ENDLESSDOORS offers that broader debate a concrete technical case study of what an unauthenticated, factory-installed remote access mechanism looks like in shipped hardware, not evidence that resolves the debate's underlying attribution question, and organizations evaluating any Chinese-origin networking hardware, not only Zbtlink-derived products, should treat this disclosure as a prompt to scrutinize firmware provenance rather than as an isolated incident.

Recommendations

Immediate Actions

Security and IT teams should inventory their environment for any of the twenty confirmed Zbtlink-derived models (CPE2801, WE1026-5G-WD, WE1326, WE2007, WE2008-DSIM, WE2416, WE3326, WE5927, WE5931, WE5931AC, WE826-T3-DSIM, WG108, WG1602, WG1608-DSIM, WG209, WG2105, WG2107, WG259, WG3526, and ZBT-Z8102AX-2SIM) sold under the Zbtlink, ZBT, ZBTWiFi, or Wiflyer names, keeping in mind VulnCheck's caution that the true affected population may extend beyond the models it was able to test [2]. Any device suspected of carrying the implant should be checked for the filesystem artifacts VulnCheck published, `/usr/sbin/kworker`, `/usr/lib/librctl.so`, `/etc/kworker.cfg`, and `/etc/init.d/skworker`, and for unbracketed `kworker` processes with non-zero memory usage in the process list, since legitimate kernel worker threads appear

bracketed with zero virtual memory size [1][2]. Network and DNS logs should be reviewed for queries to `zbtctl.epplink[.]net`, `online-string[.]com`, and `rbdg4nzqadui.wikaba[.]com`, and for outbound connections to 47.100.190.96, 47.107.224.89, and 43.248.136.125, or to TCP ports 7000 and 7001 generally, using the Suricata, Snort, and YARA rules VulnCheck published alongside its advisory [2][3].

Short-Term Mitigations

Where a confirmed device cannot be removed immediately, organizations should block outbound DNS resolution and IP-level egress to the four known command-and-control endpoints at the network firewall or upstream ISP level as an interim control, recognizing that this blocks known indicators but does not remove the implant itself and does not protect against C2 infrastructure the vendor or operator has not yet been observed using. A password change or factory reset does not remediate this issue, since the implant is embedded in the firmware image itself and will re-establish beaconing after reset; only firmware replacement with a verified clean image, where one exists, or full hardware replacement, addresses the root cause [1][2]. Organizations should also treat any network segment behind a confirmed device as potentially exposed and prioritize monitoring lateral movement from that segment, since the implant's stated command set includes an interactive root shell capable of reaching other hosts on the same LAN [2].

Strategic Considerations

Procurement and asset management teams should build firmware provenance and ODM transparency into vendor risk assessments for networking hardware, given that a single Chinese ODM's reference design here propagated the same embedded implant across at least four downstream consumer brands, a pattern that vendor security reviews scoped to the storefront brand, rather than the underlying manufacturer, can miss. Organizations relying on budget or white-label networking equipment, particularly in branch offices, retail locations, or guest network deployments where hardware refresh cycles are long and monitoring is thin, should treat this disclosure as a reason to inventory device manufacturers, not just device brands, across their estate. More broadly, ENDLESSDOORS reinforces that zero trust principles, verifying and continuously monitoring device behavior rather than extending implicit trust once a device is on the network, apply as much to the network infrastructure itself as to the endpoints and users it connects, since the router in this case is not a trusted enforcement point but the compromised asset.

CSA Resource Alignment

CSA's *Zero Trust Guidance for IoT* directly addresses the assumption this incident breaks: that a network device, once deployed, can be implicitly trusted rather than continuously verified [5]. Its five-step methodology, defining the protect surface, mapping transaction flows, building a Zero Trust architecture, creating policy, and monitoring and maintaining the network, gives organizations a structured way to treat routers and CPE devices as unverified endpoints subject to egress monitoring and segmentation rather than as trusted infrastructure, which is the posture that could plausibly have limited ENDLESSDOORS' reach even before VulnCheck's indicators were public. CSA's *IoT Firmware Update Processes* guidance is equally relevant on the supply chain dimension: it calls for cryptographic signing and integrity verification of firmware images specifically to prevent the class of risk this incident realizes, unverified code embedded in a vendor's shipped firmware, and organizations that had required signed, independently verifiable firmware from Zbtlink-derived products as a procurement condition would have had a stronger basis to detect or reject the implant before deployment [6]. Both artifacts predate this specific disclosure but describe the exact control gaps, implicit device trust and unverified firmware provenance, that would need to be closed to prevent a similar factory-installed implant from shipping undetected in the future.

References

[1] The Hacker News. "Chinese-Made Zbtlink Routers Ship With Backdoor That Opens Unauthenticated Root Shells." The Hacker News, August 2026.

[2] VulnCheck. "ENDLESSDOORS Is Phoning Home. Pick Up.." VulnCheck Blog, August 5, 2026.

[3] VulnCheck. "ENDLESSDOORS: Zbtlink Router rctl/kworker Phone-Home Root Implant (CVE-2026-66747)." VulnCheck Advisories, August 5, 2026.

[4] Reuters (AJ Vicens). "Chinese-made Zbtlink Routers Have Backdoor, Researchers Say." Reuters via Yahoo, August 5, 2026.

[5] Cloud Security Alliance. "Zero Trust Guidance for IoT." Cloud Security Alliance, May 2025.

[6] Cloud Security Alliance. "IoT Firmware Update Processes." Cloud Security Alliance, September 2018.

[7] The Register. "Chinese Router Vendor Denies Its Firmware Contains Backdoors – But Pauses Downloads to Fix Security Issues Anyway." The Register, August 6, 2026.

