Hive Pro

Threat Level

Red

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

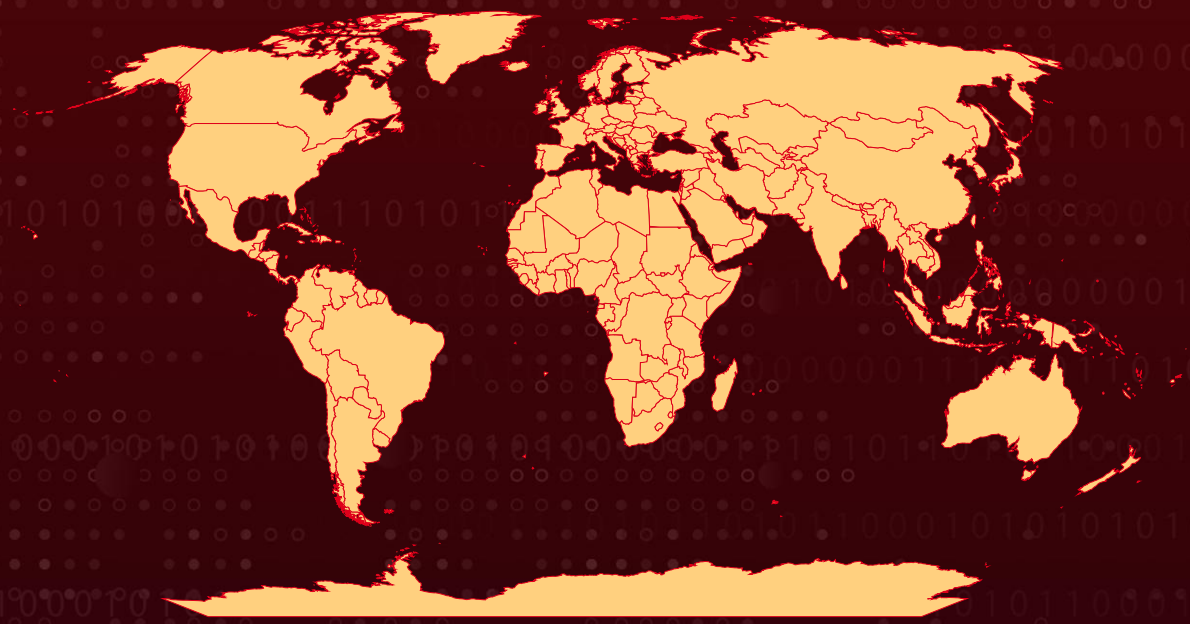
ClingSTUN Backdoor Turns Exposed IoT Devices into Stealthy Proxy Nodes

Date of Publication	Admiralty Code	TA Number
October 09, 2026	A1	TA2026295

Summary

Targeted Regions: Worldwide
Targeted Platforms: Linux (IoT and embedded devices on ARM, Intel 80386, AMD x86-64, MIPS R3000 and PowerPC architectures)
Targeted Products: AVTECH, China Mobile, D-Link, EnGenius, Hytec Inter, Ivanti, KGUARD, Lantronix, LB-LINK, Linear, Linksys, MeiG Smart, MVPower, Realtek, Sunhillo, TBK, Tenda and TP-Link routers, NAS, DVR/CCTV, IP camera, access control and edge gateway devices
Malware: ClingSTUN Backdoor
Attack: ClingSTUN is a multi-architecture Linux backdoor that compromises Internet-facing IoT and edge devices by exploiting 24 known vulnerabilities, then spreads on its own using seven more hardcoded exploits. Once installed, it hides itself, persists through init scripts, kills competing malware, and abuses legitimate public STUN servers to learn its external IP and port mappings, turning hijacked devices into back-connect proxy nodes that can also run attacker commands without any dedicated C2 server.

Attack Regions



Targeted Non-Targeted

Powered by Bing
© Australian Bureau of Statistics, GeoNames, Microsoft, Navinfo, Open Places, OpenStreetMap, Overture Maps Fundation, TomTom, Zenrin

CVEs

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2022-36553	Hytec Inter HWL-2511-SS Command Injection Vulnerability	Hytec Inter HWL-2511-SS	✗	✗	✗
CVE-2025-34035	EnGenius EnShare Cloud Service OS Command Injection Vulnerability	EnGenius EnShare Cloud Service	✗	✗	✗
CVE-2024-23625	D-Link UPnP SUBSCRIBE Code Injection Vulnerability	D-Link Devices	✗	✗	✗
CVE-2021-35394	Realtek Jungle SDK Remote Code Execution Vulnerability	Realtek Jungle Software Development Kit (SDK)	✗	✓	✓
CVE-2023-1389	TP-Link Archer AX-21 Command Injection Vulnerability	TP-Link Archer AX21	✗	✓	✓
CVE-2024-7029	AVTECH AVM1203 Command Injection Vulnerability	AVTECH AVM1203	✗	✗	✗
CVE-2024-10915	D-Link Command Injection Vulnerability	D-Link Devices	✗	✗	✗
CVE-2024-23624	D-Link DAP-1650 Command Injection Vulnerability	D-Link DAP-1650 devices	✗	✗	✗
CVE-2019-17621	D-Link DIR-859 Router Command Execution Vulnerability	D-Link DIR-859 Router	✗	✓	✓
CVE-2019-7256	Nice Linear eMerge E3-Series OS Command Injection Vulnerability	Nice Linear eMerge E3-Series	✗	✓	✓

Note: The ClingSTUN Linux backdoor attacked Internet-facing IoT and edge devices by exploiting the known vulnerabilities listed above. Click the tick mark next to each CVE to open its patch.

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2021-36380	Sunhillo SureLine OS Command Injection Vulnerablity	Sunhillo SureLine	✗	✓	✓
CVE-2024-21887	Ivanti Connect Secure and Policy Secure Command Injection Vulnerability	Ivanti Connect Secure and Policy Secure	✓	✓	✓
CVE-2023-46805	Ivanti Connect Secure and Policy Secure Authentication Bypass Vulnerability	Ivanti Connect Secure and Policy Secure	✓	✓	✓
CVE-2024-46048	Tenda exeCommand Command Injection Vulnerability	Tenda Devices	✗	✗	✗
CVE-2024-35340	Tenda exeCommand Command Injection Vulnerability	Tenda Devices	✗	✗	✗
CVE-2024-32314	Tenda AC500 formexeCommand Command Injection Vulnerability	Tenda AC500	✗	✗	✗
CVE-2024-32292	Tenda exeCommand Command Injection Vulnerability	Tenda Devices	✗	✗	✗
CVE-2024-32281	Tenda exeCommand Command Injection Vulnerability	Tenda Devices	✗	✗	✗
CVE-2022-35555	Tenda W6 exeCommand Command Injection Vulnerability	Tenda W6	✗	✗	✗
CVE-2022-26289	Tenda exeCommand Command Injection Vulnerability	Tenda Devices	✗	✗	✗

Note: The ClingSTUN Linux backdoor attacked Internet-facing IoT and edge devices by exploiting the known vulnerabilities listed above. Click the tick mark next to each CVE to open its patch.

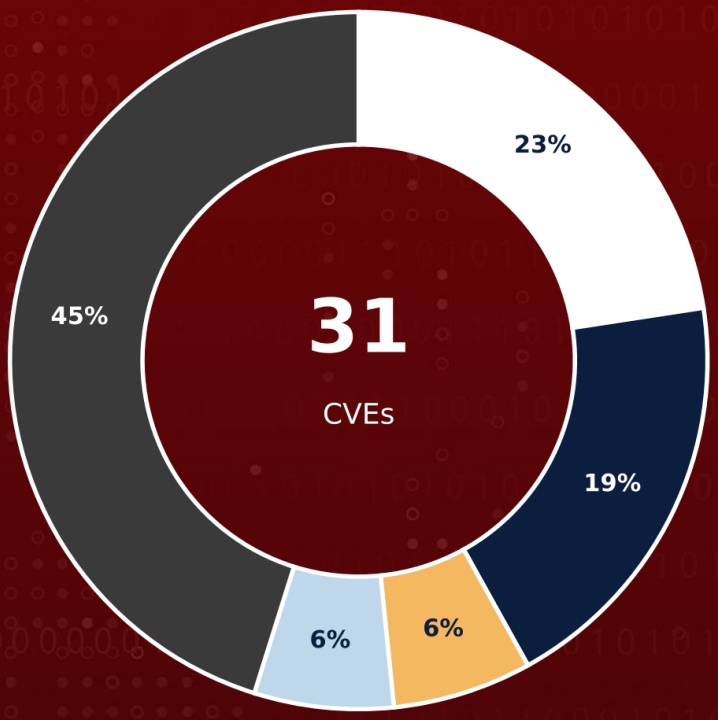
CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2022-37055	D-Link Routers Buffer Overflow Vulnerability	D-Link Routers	✗	✓	EOL
CVE-2024-10914	D-Link NAS Command Injection Vulnerability	D-Link NAS devices	✗	✗	✗
CVE-2026-36356	MeiG Smart FORGE_SLT711 GoAhead Command Injection Vulnerability	MeiG Smart FORGE_SLT711	✗	✗	✗
CVE-2025-67038	Lantronix EDS5000 Code Injection Vulnerability	Lantronix EDS5000	✗	✓	✓

Note: The ClingSTUN Linux backdoor attacked Internet-facing IoT and edge devices by exploiting the known vulnerabilities listed above. Click the tick mark next to each CVE to open its patch.

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2014-8361	Realtek SDK Improper Input Validation Vulnerability	Realtek SDK	✗	✓	✓
CVE-2016-20016	MVPower Remote Command Execution Vulnerability	MVPower tv-7104he_firmware	✗	✗	✗
CVE-2024-3721	TBK DVR OS Command Injection Vulnerability	TBK DVR-4104 / DVR-4216	✗	✗	EOL
CVE-2025-34037	Linksys E-Series Routers OS Command Injection Vulnerability	Linksys E-Series Routers	✗	✗	✗
CVE-2023-26801	lb-link bl-lte300_firmware Command Injection Vulnerability	lb-link bl-lte300_firmware	✗	✗	✗
CVE-2023-41011	China Mobile Intelligent Home Gateway Command Execution Vulnerability	China Mobile HG6543C4	✗	✗	✗
CVE-2026-87827	KGUARD DVR Command Execution Vulnerability	KGUARD DVR	✗	✗	✗

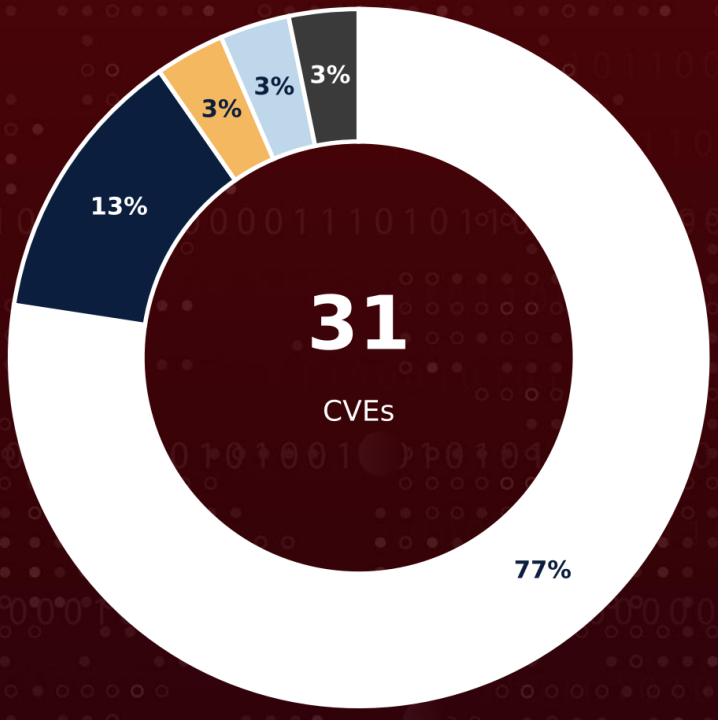
Note: ClingSTUN has hard-coded exploits for seven vulnerabilities. Click the tick mark next to each CVE to oper its patch.

ClingSTUN: CVEs by Vendor



Others: AVTECH, China Mobile, EnGenius, Hytec, KGUARD, LB-LINK, Lantronix, Linear, Linksys, MVPower, MeiG, Sunhillo, TBK, TP-Link

ClingSTUN: CVEs by Attack Type



Attack Details

#1

ClingSTUN is a Linux backdoor built to take over Internet-facing IoT and edge devices, and it runs on all common device architectures. It gets in through 24 known vulnerabilities in products from Hytec Inter, EnGenius, D-Link, Realtek, TP-Link, AVTECH, Linear eMerge, Sunhillo, Ivanti, Tenda, MeiG Smart and Lantronix. Most of these flaws let an attacker inject commands into a device's web or UPnP interface without logging in. In one observed attack, the operator exploited CVE-2022-36553 in a Hytec Inter router to deliver a downloader. The downloader then fetched ClingSTUN builds for the device's architecture.

#2

Newer versions of the downloader prepare the device before ClingSTUN starts. They unmount selected file systems, kill processes running from temporary storage and disable the hardware watchdog, so the device cannot reboot itself and clear the infection. Once active, ClingSTUN checks the running processes and kills any that look like competing malware, which removes rival botnets from the device. To survive reboots, ClingSTUN saves hidden copies of itself and adds itself to the device's startup scripts. It also hides from process listings by showing the details of a legitimate system process in place of its own and by blanking its command line.

#3

ClingSTUN has no dedicated command-and-control server. It uses legitimate public STUN servers, which normally help VoIP and video-call apps work through NAT, to learn the device's external IP address and open ports. It then regularly reports its group ID and port details back to those same servers. Because this traffic looks like ordinary VoIP or WebRTC activity, it blends into normal network noise.

#4

The infected device then works as a proxy node. The operator can route traffic through victim IP addresses, including corporate ones, which hides where an attack really comes from and can get the victim's addresses blocklisted. A special control packet can also tell the backdoor to connect out to an attacker-chosen server, download a command and run it. ClingSTUN spreads by itself using built-in exploits for seven more vulnerabilities in Realtek, MVPower, TBK, Linksys, LB-LINK, China Mobile and KGUARD devices.

Recommendations

Patch or Retire Exposed Edge Devices: Inventory every Internet-facing router, NAS, DVR, IP camera, access controller and VPN gateway from the affected vendors and apply the latest vendor firmware for the CVEs listed in this advisory. Devices that are end-of-life or will not be fixed, such as the affected D-Link DNS-series NAS models, should be isolated or replaced.

Prioritise CISA KEV-Listed Flaws: Treat CVE-2023-1389 (TP-Link Archer AX21), CVE-2019-7256 (Nice Linear eMerge E3), CVE-2024-21887 and CVE-2023-46805 (Ivanti Connect Secure and Policy Secure) and CVE-2022-37055 (D-Link Go-RT-AC750) as top priority, since they are confirmed as exploited in the wild.

Monitor for Unexpected STUN Traffic: Alert on STUN binding requests (typically UDP 3478 and related ports) from devices that have no reason to use VoIP or WebRTC, such as routers, NAS and DVRs, and on recurring keepalive-style UDP traffic to many public STUN endpoints.

Hunt for ClingSTUN Persistence Artifacts: On Linux-based devices you can access, check for /root/.cling and /usr/local/bin/.cling, unexpected entries in /etc/inittab, /etc/init.d/rcS and /etc/rc.d/rc.boot, bind mounts over /proc/PID paths, disabled watchdog timers, and executables running from /tmp.

Reflash Compromised Devices: Because ClingSTUN hides from process listings and persists through boot scripts, reflash any device suspected of compromise with clean vendor firmware and reset its credentials instead of attempting manual cleanup.

Track Device Firmware Lifecycle: Keep an accurate asset register with firmware versions and vendor support status, and add vendor security bulletins for these product lines to routine vulnerability management reviews.

Potential MITRE ATT&CK TTPs

Tactic	Technique	Sub-technique
Resource Development	T1584: Compromise Infrastructure	T1584.008: Network Devices
Initial Access	T1190: Exploit Public-Facing Application	
Execution	T1059: Command and Scripting Interpreter	T1059.004: Unix Shell
Persistence	T1037: Boot or Logon Initialization Scripts	T1037.004: RC Scripts
Defense Evasion	T1564: Hide Artifacts	T1564.001: Hidden Files and Directories
		T1564.013: Bind Mounts
	T1036: Masquerading	
	T1562: Impair Defenses	T1562.001: Disable or Modify Tools
Discovery	T1057: Process Discovery	
	T1016: System Network Configuration Discovery	T1016.001: Internet Connection Discovery
Lateral Movement	T1210: Exploitation of Remote Services	
Command and Control	T1105: Ingress Tool Transfer	
	T1090: Proxy	
	T1095: Non-Application Layer Protocol	
	T1205: Traffic Signaling	
	T1071: Application Layer Protocol	
Impact	T1489: Service Stop	

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	dc892f5013edb0aa1e61e808511387373d8d120348b5be0929621d21e6e9946a, a297eddfa7abea8d411afc0f150f8f6f30e470a77204de87e3b0815fa9bb8a84, 4fbd61cb9181ebbc4fe9a6e59d3c346dc00001da48d66bd890556fc6fad22b07, 121f2050e3c891b29565fd73451fff7ae60199c86eb8d79ec1eb1d9844578487, 48f9b72ce72ab7087794650d6eef10135345088384fbde1482f1c74a02b80302, e6e113783356446aef66e5296db45b244f318292af7cebc2a9bd76f095a95c4c, c1d8e2829ea63b9dc1cf2c3421a5093406adad4d6622e238376e78e908e0e6e8, 48962b3893f2c8261e32e6b95ea7d463d145a529a8b2a6c987dd979454405c73, 76692a23abe718b93e63edefd743971ec627c0cdf3778f856bd5ec88003deaa2, ec199c78c11040fd3127887222fd75a85e5797bf96aa691a117fdd83dd663d81, c0d8ffebfba969b1c1ca76bd9623bb623e9f95155c8ceca77d8fcc521435a497, f49f45303cbfccee14ff193ac9608f860e6d616f08c0ecbef1ec44f7c863d7ec, 9391c6ad17aced1142607c0c623b18d86a7697cc483d204ffac94093e26b8068, e4d12208789f36efc5a1ff765088fed95d6bb5972d1a804a4536fd42366797d4, 284e5ec8748f99fd1b8c331b699a5fe5fd4448bbaae0347a940f427f931c4d14, 6581bf37184bb2db899b9893064d39dd314ea691adf3281cc0aa7e0a31e5138a, 10d83c1748895361e07320f68d44d427b43cadd2cbffe0ab5e607ab03aec83da

TYPE	VALUE
SHA256	2ed54e0f988a62039abed88f6394eb1e3d5ed931f0183556055417fb08844ecf, b90640b392827b4f2d280f6cf67860862953331917d42df23e1653a92f2f98ad, dfba6008a2c828a9cb62342aec53006ae05a60cb8d4c41c3fa216fd727e8c6a3, 5c4e263546fb21f8fe8732789a5b6583eaa8ae11ebeef099462a7c9bf50e022d
IPv4	124[.]163[.]212[.]119, 222[.]223[.]152[.]97, 118[.]145[.]196[.]225
File Path	/root/.cling, /usr/local/bin/.cling

References

https://www.fortinet.com/blog/threat-research/clingstun-linux-backdoor-abuses-public-stun-infrastructure

https://www.thaicert.or.th/en/2026/10/06/clingstun-exploits-more-than-24-vulnerabilities-to-compromise-linux-devices-and-turn-them-into-proxies/

https://www.cisa.gov/news-events/ics-advisories/icsa-24-214-07

https://www.exploit-db.com/exploits/47619

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a Demo of **HivePro**.

REPORT GENERATED ON

October 09, 2026 • 03:30 AM

© 2026 All Rights are Reserved by Hive Pro

More at www.hivepro.com