

Date of Publication
October 13, 2026



HiveForce Labs
WEEKLY
THREAT DIGEST

Attacks, Vulnerabilities, and Actors

05 to 11 OCTOBER 2026

Table Of Contents

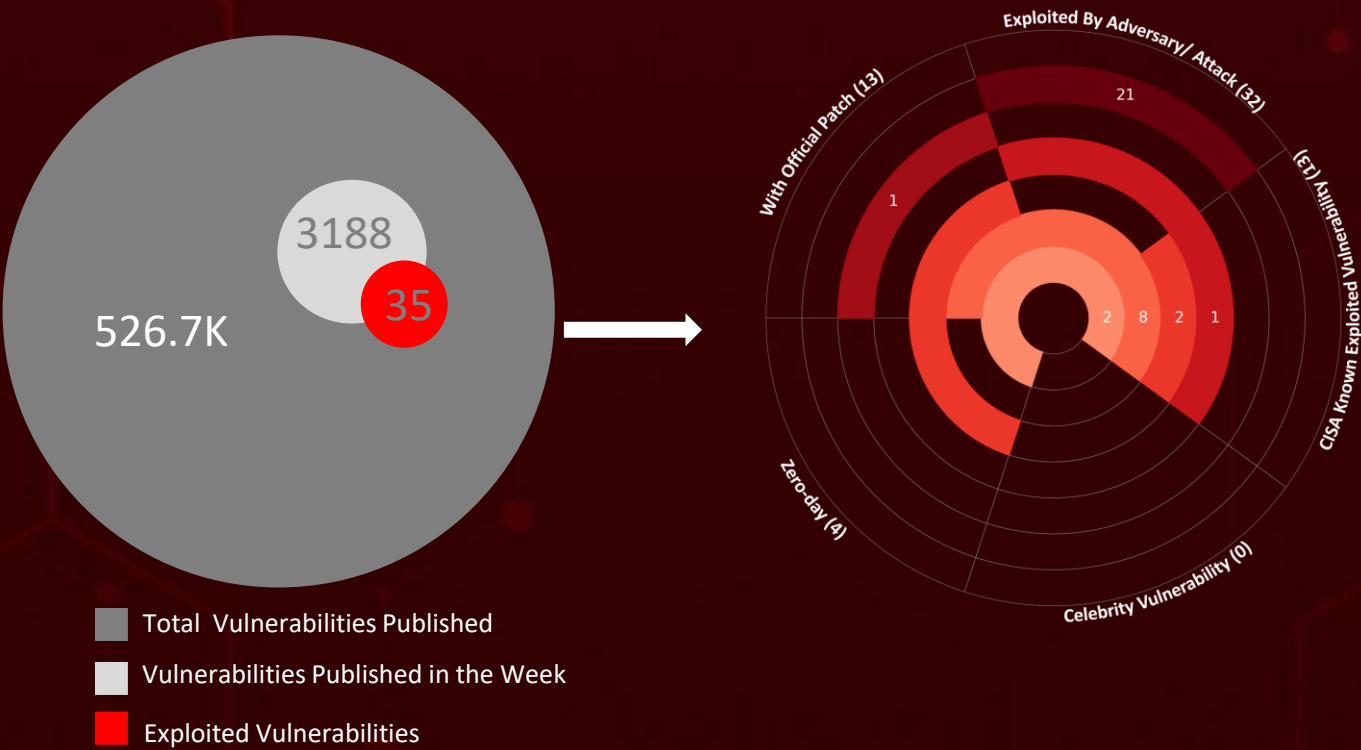
<u>Summary</u>	03
<u>High Level Statistics</u>	04
<u>Insights</u>	05
<u>Targeted Countries</u>	06
<u>Targeted Industries</u>	07
<u>Top MITRE ATT&CK TTPs</u>	07
<u>Attacks Executed</u>	08
<u>Vulnerabilities Exploited</u>	20
<u>Adversaries in Action</u>	40
<u>Recommendations</u>	41
<u>Threat Advisories</u>	42
<u>Appendix</u>	43
<u>What Next?</u>	45

Summary

HiveForce Labs has reported a sharp rise in cybersecurity threats, highlighting the growing complexity and frequency of global cyber incidents. Over the past week, **12** major attacks were detected, and **35** vulnerabilities were actively exploited, signaling a concerning escalation in malicious activity worldwide.

Among the most significant developments, **CVE-2026-73570** is a command injection flaw in Zimbra Collaboration Suite before 10.1.20. If SNMP notifications are on, attackers can run commands without logging in. Over 274 servers have since been hit with web shells, cryptominers, and backdoors, and attackers stole emails and credentials. Meanwhile, **CVE-2026-88779** is a high-severity memory overflow zero-day in NetScaler ADC and Gateway, and it's under active attack on appliances set up as a SAML Service Provider or Identity Provider.

Elsewhere, **CL-STA-1178**, an Iran-nexus threat cluster, is posing as the Dubai Airports IT department and sending a targeted engineer a trojanized Visual Studio coding test. Together, these incidents underscore a growing trend of hybrid cyber operations that combine technical exploitation with social engineering, reinforcing the need for timely patching, continuous monitoring, and layered security defenses.



High Level Statistics

12

Attacks
Executed

35

Vulnerabilities
Exploited

0

Adversaries in
Action

- [Chopper](#)
- [Godzilla](#)
- [CoinMiner](#)
- [Looptik](#)
- [Zimdown2](#)
- [Zimclient2](#)
- [ShelbyLoader](#)
- [ShelbyC2](#)
- [PsProxy](#)
- [Blackwood](#)
- [Shai-Hulud](#)
- [ClingSTUN](#)
- [CVE-2026-73570](#)
- [CVE-2026-88779](#)
- [CVE-2026-104286](#)
- [CVE-2026-21589](#)
- [CVE-2022-36553](#)
- [CVE-2025-34035](#)
- [CVE-2024-23625](#)
- [CVE-2021-35394](#)
- [CVE-2023-1389](#)
- [CVE-2024-7029](#)
- [CVE-2024-10915](#)
- [CVE-2024-23624](#)
- [CVE-2019-17621](#)
- [CVE-2019-7256](#)
- [CVE-2021-36380](#)
- [CVE-2024-21887](#)
- [CVE-2023-46805](#)
- [CVE-2024-46048](#)
- [CVE-2024-35340](#)
- [CVE-2024-32314](#)
- [CVE-2024-32292](#)
- [CVE-2024-32281](#)
- [CVE-2022-35555](#)
- [CVE-2022-26289](#)
- [CVE-2022-37055](#)
- [CVE-2024-10914](#)
- [CVE-2026-36356](#)
- [CVE-2025-67038](#)
- [CVE-2014-8361](#)
- [CVE-2016-20016](#)
- [CVE-2024-3721](#)
- [CVE-2025-34037](#)
- [CVE-2023-26801](#)
- [CVE-2023-41011](#)
- [CVE-2026-87827](#)



Insights

274+ Zimbra
Servers
Breached: Patch
CVE-2026-73570
Now

Citrix NetScaler Zero-Day CVE-
2026-88779 Under Active
Attack

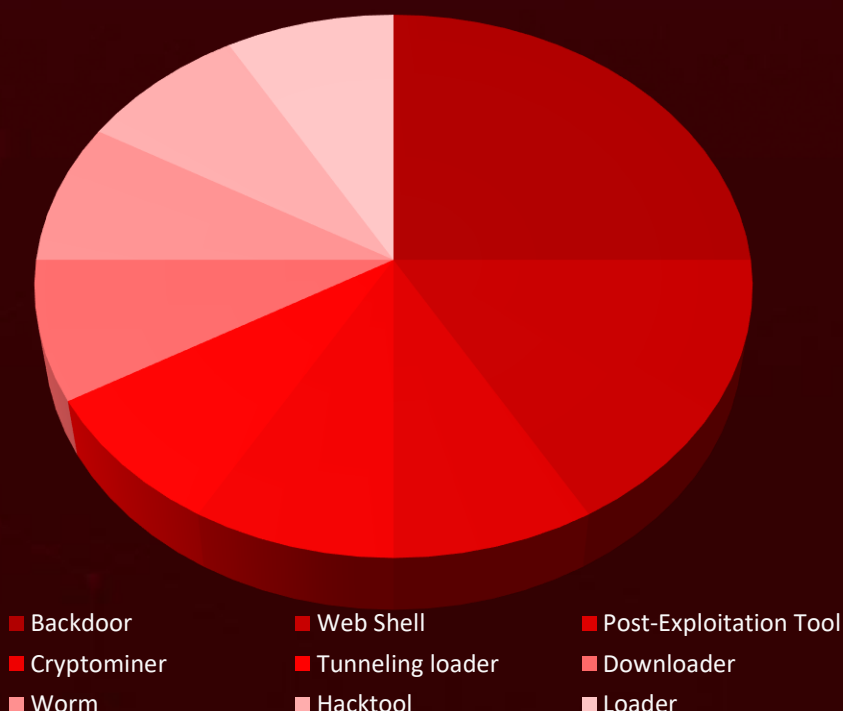
Poisoned tensorlake
npm SDK 0.5.144
Unleashes Shai-
Hulud Worm
Variant

CVE-2026-21589: Critical Flaw
Hits Eight Self-Hosted Atlassian
Products

31 Exploits: ClingSTUN
Sweeps Through Edge
Devices

Open the Project,
Lose the Network:
Iran-Linked
Espionage Targets
Engineers

Threat Distribution



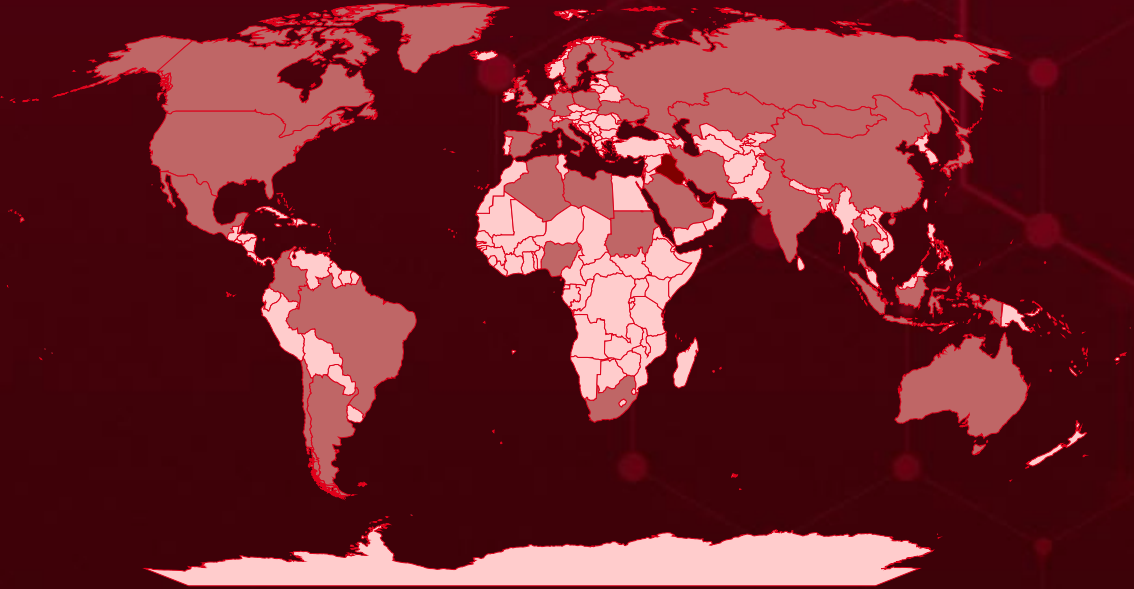


Targeted Countries

Most



Least



Powered by Bing

© Australian Bureau of Statistics, GeoNames, Microsoft, Navinfo, Open Places, OpenStreetMap, Overture Maps Foundation, TomTom, Zenrin

Countries	Countries	Countries	Countries
Iraq	India	Brunei	Bhutan
United Arab Emirates	Poland	Anguilla	Dominican Republic
Israel	Indonesia	Tonga	Montenegro
Thailand	Saudi Arabia	Antigua and Barbuda	Ecuador
Nigeria	Iran	Mauritania	Myanmar
United States	Spain	Comoros	Egypt
Brazil	Algeria	Morocco	Netherland Antilles
South Africa	Sweden	Congo-Brazzaville	El Salvador
Canada	Ukraine	New Zealand	Niger
Kazakhstan	Australia	Costa Rica	Equatorial Guinea
Chile	Italy	Norway	Northern Cyprus
Mexico	United Kingdom	Croatia	Estonia
China	Qatar	Philippines	Pakistan
Russia	Monaco	Cuba	Ethiopia
Colombia	Taiwan	Rwanda	Paraguay
Sudan	Andorra	Curacao	Faroe Islands
Finland	North Korea	San Marino	Portugal
Japan	Canada Quebec	Cyprus	Fiji
France	Serbia	Slovakia	Romania
Argentina	Cape Verde	Czech Republic	Albania
Germany	Cameroon	Swaziland	Saint Eustatius
Libya	Cayman Islands	Democratic Republic of Congo	Armenia
Greenland	Nauru	Tibet	French Guiana
Mongolia	Central African Republic	Denmark	Scotland
	Panama	Turkmenistan	Gabon
	Chad	Djibouti	Sierra Leone
	Saint Lucia	Malta	Georgia
	Angola	Dominica	British Virgin Islands
			Aruba

Targeted Industries



TOP MITRE ATT&CK TTPs

T1059

Command and Scripting Interpreter

T1105

Ingress Tool Transfer

T1190

Exploit Public-Facing Application

T1071

Application Layer Protocol

T1036

Masquerading

T1071.001

Web Protocols

T1543

Create or Modify System Process

T1059.004

Unix Shell

T1552

Unsecured Credentials

T1505

Server Software Component

T1053

Scheduled Task/Job

T1057

Process Discovery

T1552.001

Credentials In Files

T1036.005

Match Legitimate Name or Location

T1505.003

Web Shell

T1567

Exfiltration Over Web Service

T1496

Resource Hijacking

T1059.001

PowerShell

T1546

Event Triggered Execution

T1595

Active Scanning

Attacks Executed

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
<u>Chopper</u>	Chopper is a JSP web shell planted on Zimbra mail servers after exploitation of CVE-2026-73570. Attackers use the command injection flaw to make a web directory writable, decode an encoded payload into a JSP file there, and then restore the original permissions. The web shell gives them ongoing access to the server over HTTP. Copies were spread to other mailbox servers in the same cluster, so deleting one copy does not remove the attacker.	Exploiting Vulnerability	CVE-2026-73570
TYPE		IMPACT	AFFECTED PLATFORM
Web Shell		Remote Access, Command Execution, Persistent Access, Lateral Spread	Zimbra Collaboration Suite servers
ASSOCIATED ACTOR			PATCH LINKS
-			https://wiki.zimbra.com/wiki/Zimbra_Relases/10.1.20#Security_Fixes https://wiki.zimbra.com/wiki/Zimbra_Relases/10.1.0/patch_in_stallation
IOC TYPE	VALUE		
SHA256	13d27ecfbb6b3d55bdabcaa3a2ade83ecfaa3df92dbc22be05e6d9e2d18087b6, dc76d856d42242e58eb8d4b70d5378f42f3ddf0ef7872d2279f2d67c22806e26		

The IOCs (Indicators of Compromise) for the attacks executed are listed in the appendix section at the end of the report.

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
<u>Godzilla</u>	Godzilla is a JSP web shell found on Zimbra mail servers compromised through CVE-2026-73570. Attackers use the command injection flaw to make a web directory writable, write the decoded web shell into it, and then restore the original permissions so the change is harder to spot. Once it's planted, they can come back to the server over HTTP whenever they like. Copies were spread to other mailbox servers in the same cluster, so removing one copy doesn't end their access.	Exploiting Vulnerability	CVE-2026-73570
TYPE		IMPACT	AFFECTED PLATFORM
Web Shell		Remote Access, Command Execution, Persistent Access	Zimbra Collaboration Suite servers
ASSOCIATED ACTOR			PATCH LINK
-			https://wiki.zimbra.com/wiki/Zimbra_Releases/10.1.20#Security_Fixes https://wiki.zimbra.com/wiki/Zimbra_Releases/10.1.0/patch_installation

The IOCs (Indicators of Compromise) for the attacks executed are listed in the appendix section at the end of the report.

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
CoinMiner	CoinMiner is a cryptocurrency miner deployed on Zimbra mail servers compromised through CVE-2026-73570. It is pulled from an attacker-controlled server and saved as a hidden file named to look like a legitimate kernel worker process. Cron entries relaunch it every minute and at every reboot. It kills competing miners and redirects their mining pools by editing the system's hosts file, so the attacker gets the server's full computing power.	Exploiting Vulnerability	CVE-2026-73570
TYPE		IMPACT	AFFECTED PLATFORM
Cryptominer		Resource Hijacking, Persistent Execution, Configuration Tampering	Zimbra Collaboration Suite servers
ASSOCIATED ACTOR			PATCH LINKS
-			https://wiki.zimbra.com/wiki/Zimbra_Releases/10.1.20#Security_Fixes https://wiki.zimbra.com/wiki/Zimbra_Releases/10.1.0/patch_installation
IOC TYPE	VALUE		
SHA256	aea991f694911e321b0ab97534f2ad0291c392c0a43dabff664c563618bd036d		

The IOCs (Indicators of Compromise) for the attacks executed are listed in the appendix section at the end of the report.

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
<u>Looptik</u>	Looptik is a public privilege escalation toolkit hosted on GitHub that attackers turned into a malicious payload on Zimbra mail servers compromised through CVE-2026-73570. It was planted in memory-backed temporary storage under a hidden name, ready to raise the attacker’s access from the limited Zimbra service account toward full system control.	Exploiting Vulnerability	CVE-2026-73570
TYPE		IMPACT	AFFECTED PLATFORM
Hacktool		Privilege Escalation, System Compromise	Zimbra Collaboration Suite servers
ASSOCIATED ACTOR			PATCH LINKS
-			https://wiki.zimbra.com/wiki/Zimbra_Releases/10.1.20#Security_Fixes https://wiki.zimbra.com/wiki/Zimbra_Releases/10.1.0/patch_installation
IOC TYPE	VALUE		
SHA256	65a7576c389326b6cdf9c993d0be6e5d50fed9655d1cdf2a3a50f2c21c8ec435		

The IOCs (Indicators of Compromise) for the attacks executed are listed in the appendix section at the end of the report.

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
<u>Zimdown2</u>	Zimdown2 is a Go-based installer used on Zimbra mail servers compromised through CVE-2026-73570. It downloads the Zimclient2 remote access agent, checks the file's hash before installing it, and picks a writable install location and a file name generated at runtime to suit each host. It reports installation progress to the attackers over a separate WebSocket channel, kept apart from the server hosting the payloads.	Exploiting Vulnerability	CVE-2026-73570
TYPE		IMPACT	AFFECTED PLATFORM
Downloader		Payload Installation, Remote Access, Data Exposure	Zimbra Collaboration Suite servers
ASSOCIATED ACTOR			PATCH LINKS
-			https://wiki.zimbra.com/wiki/Zimbra_Releases/10.1.20#Security_Fixes https://wiki.zimbra.com/wiki/Zimbra_Releases/10.1.0/patch_installation
IOC TYPE	VALUE		
SHA256	bf28f38122bf20d5fac969cc414daa6a890cdea872d389ca93d2092b6b7773cf		

The IOCs (Indicators of Compromise) for the attacks executed are listed in the appendix section at the end of the report.

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
<u>Zimclient2</u>	Zimclient2 is a remote access agent planted on Zimbra mail servers compromised through CVE-2026-73570. It gives attackers an interactive shell, lets them move files to and from the server, and acts as a SOCKS5 proxy so they can reach deeper into the victim's network through the compromised server. It talks to its command servers over WebSocket, TLS or raw TCP and switches between them if one is blocked. To survive reboots and cleanup, it sets up systemd services, OpenRC scripts, cron jobs, shell startup files, SSH keys and new local accounts.	Exploiting Vulnerability	CVE-2026-73570
TYPE		IMPACT	AFFECTED PLATFORM
Backdoor		Remote Control, Persistent Access, Data Exfiltration, Network Pivoting	Zimbra Collaboration Suite servers
ASSOCIATED ACTOR			PATCH LINKS
-			https://wiki.zimbra.com/wiki/Zimbra_Releases/10.1.20#Security_Fixes https://wiki.zimbra.com/wiki/Zimbra_Releases/10.1.0/patch_installation
IOC TYPE	VALUE		
SHA256	b594a42b8f1c6f090327bb9a3361c2d3515537fb7ac8da6b9061b9a3f330e159		

The IOCs (Indicators of Compromise) for the attacks executed are listed in the appendix section at the end of the report.

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
ShelbyLoader	A C# loader (RuntimeBroker.dll) sideloaded through AppDomainManager hijacking. It checks for sandboxes, sets Run-key persistence, fingerprints the host and beacons to GitHub C2, falling back to dead drops hidden in issue comments, before decrypting ShelbyC2 V2.	Trojanized Visual Studio project	-
TYPE		IMPACT	AFFECTED PLATFORM
Loader		Persistence, payload delivery	Microsoft Windows
ASSOCIATED ACTOR			PATCH LINK
-			-
IOC TYPE	VALUE		
SHA256	53f35e49eb9b271fd8cbcd3daacb525328dbf159a03dbd1c7adebe0363daa402, 6e7d9b33f1e72ea1ede71373a604ecdb060dab7d42055179c1eede9ecd1fd239		

The IOCs (Indicators of Compromise) for the attacks executed are listed in the appendix section at the end of the report.

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
<u>ShelbyC2</u>	The primary .NET backdoor (RuntimeBrokerApi.dll), stored AES-encrypted and decrypted in memory with a key derived from GitHub-hosted content. It runs operator commands through PsProxy and stages Blackwood for tunneling.	Loaded by ShelbyLoader V2	-
TYPE		IMPACT	AFFECTED PLATFORM
Backdoor		Remote command execution	Microsoft Windows
ASSOCIATED ACTOR			PATCH LINK
-			-
IOC TYPE	VALUE		
Filename	RuntimeBrokerApi.dll		

The IOCs (Indicators of Compromise) for the attacks executed are listed in the appendix section at the end of the report.

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
<u>PsProxy</u>	An in-memory module that executes PowerShell and has no network or persistence of its own. It hooks System.Management.Automation.dll and runs scripts in a hidden runspace without launching PowerShell.exe.	Invoked by ShelbyC2 V2	-
TYPE		IMPACT	AFFECTED PLATFORM
Post-Exploitation Tool		Stealthy script execution	Microsoft Windows
ASSOCIATED ACTOR			PATCH LINK
-			-
IOC TYPE	VALUE		
SHA256	3fd810a3aa0039993393741b32287c367a9a5037a41e826906440887cdd3ed13		

The IOCs (Indicators of Compromise) for the attacks executed are listed in the appendix section at the end of the report.

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
Blackwood	A .NET loader pulled as Client.zip from GitHub and sideloaded into a signed vshost32.exe. It decrypts and reflectively loads an embedded Chisel DLL, then opens a reverse SOCKS proxy for covert pivoting.	GitHub-hosted ZIP archive	-
TYPE		IMPACT	AFFECTED PLATFORM
Tunneling loader		Covert network pivoting	Microsoft Windows
ASSOCIATED ACTOR			PATCH LINK
-			-
IOC TYPE	VALUE		
SHA256	76273382e4252c1f60a2251141e108942494409c759358320735891762c0682e, d3561bd4aad003dc3e08157b0891860bb496b80cd6e44901692e08ab1d4e8260		

The IOCs (Indicators of Compromise) for the attacks executed are listed in the appendix section at the end of the report.

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
<u>Shai-Hulud</u>	Shai-hulud is a supply-chain worm hidden in compromised packages that executes automatically on install via a bundled bundle.js. Once running, it leverages legitimate tooling to hunt for secrets, scans the host and developer environments for cloud and CI tokens, and validates any credentials it finds, so stolen tokens are immediately usable. The worm then abuses those credentials to propagate, injecting unauthorized GitHub Actions workflows into repositories and moving laterally across accounts, while exfiltrating harvested secrets to a hardcoded webhook. It targets packages from multiple maintainers and automates both secret discovery and repository-level persistence.	Malicious code into the tensorlakeai/tensorlake	-
TYPE		IMPACT	AFFECTED PLATFORM
Worm		System Compromise, exfiltrates data	-
ASSOCIATED ACTOR			PATCH LINK
-			-
IOC TYPE	VALUE		
SHA256	25a0735d0db7dc40e5d45ce42d9c106067e6a66e184d967cfecfab17c3bcb5ef, b50a00900399ba99fb6ce1fc151519cb99d44320ef2a631f2237e1aea0ad6fec		

NAME	OVERVIEW	DELIVERY METHOD
<u>ClingSTUN</u>	ClingSTUN is a Linux backdoor that takes over Internet-facing IoT devices. A shell downloader installs it, and it then persists through system startup scripts and hides its process. It kills competing malware and disables the device watchdog so the device doesn't reboot. It uses public STUN servers to find the device's external IP address and port mappings, then turns the device into a back-connect proxy that can also run remote commands. It spreads to other devices using built-in exploits.	Exploitation of known vulnerabilities
TYPE		IMPACT
Backdoor		Remote Control, Command Execution, Proxy Abuse, Persistent Infection, Process Concealment
ASSOCIATED ACTOR		
-		

The IOCs (Indicators of Compromise) for the attacks executed are listed in the appendix section at the end of the report.

NAME	TARGETED CVE
ClingSTUN	CVE-2022-36553, CVE-2025-34035, CVE-2024-23625, CVE-2021-35394, CVE-2023-1389, CVE-2024-7029, CVE-2024-10915, CVE-2024-23624, CVE-2019-17621, CVE-2019-7256, CVE-2021-36380, CVE-2024-21887, CVE-2023-46805, CVE-2024-46048, CVE-2024-35340, CVE-2024-32314, CVE-2024-32292, CVE-2024-32281, CVE-2022-35555, CVE-2022-26289, CVE-2022-37055, CVE-2024-10914, CVE-2026-36356, CVE-2025-67038, CVE-2014-8361, CVE-2016-20016, CVE-2024-3721, CVE-2025-34037, CVE-2023-26801, CVE-2023-41011, CVE-2026-87827
TYPE	AFFECTED PLATFORM
Backdoor	Linux (IoT devices on ARM, Intel 80386, AMD x86-64, MIPS R3000 and PowerPC)
ASSOCIATED ACTOR	PATCH LINKS
-	https://www.realtek.com/images/safe-report/Realtek_APRouter_SDK_Advisory-CVE-2021-35392_35395.pdf https://www.tp-link.com/us/support/download/archerax21/v3/#Firmware https://www.dlink.com/en/security-bulletin , https://linear-solutions.com/software-downloads/ https://www.sunhillo.com/product/sureline/ https://hub.ivanti.com/s/article/CVE-2023-46805-Authentication-Bypass-CVE-2024-21887-Command-Injection-for-Ivanti-Connect-Secure-and-Ivanti-Policy-Secure-Gateways?language=en_US https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10413 , https://ltrxdev.atlassian.net/wiki/spaces/LTRXTS/pages/2538438657 https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10055
IOC TYPE	VALUE
SHA256	e6e113783356446aef66e5296db45b244f318292af7cebc2a9bd76f095a95c4c, c1d8e2829ea63b9dc1cf2c3421a5093406adad4d6622e238376e78e908e0e6e8

The IOCs (Indicators of Compromise) for the attacks executed are listed in the appendix section at the end of the report.

Vulnerabilities Exploited

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
<u>CVE-2026-73570</u>		Synacor Zimbra Collaboration Suite (ZCS) Before 10.1.20	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEY		
Zimbra Collaboration Suite (ZCS) OS Command Injection Vulnerability		cpe:2.3:a:synacor:zimbra_collaboration_suite:*:*:*:*:*:*	Chopper, Godzilla Web Shell, CoinMiner, Looptik, Zimdown2, Zimclient2
	CWE ID	ASSOCIATED TTPs	PATCH LINKS
	CWE-78	T1190: Exploit Public-Facing Application, T1059: Command and Scripting Interpreter, T1059.004: Unix Shell, T1505: Server Software Component, T1505.003: Web Shell	https://wiki.zimbra.com/wiki/Zimbra_Releases/10.1.20#Security_Fixes https://wiki.zimbra.com/wiki/Zimbra_Releases/10.1.0/patch_installation

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
<u>CVE-2026-88779</u>		Citrix NetScaler ADC and NetScaler Gateway 14.1 (Before 14.1-73.41), Citrix NetScaler ADC and NetScaler Gateway 13.1 (Before 13.1-64.28), Citrix NetScaler ADC 14.1-FIPS (Before 14.1-73.41 FIPS), Citrix NetScaler ADC 13.1-FIPS and 13.1-NDcPP (Before 13.1-37.282)	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEY		
Citrix NetScaler Improper Restriction of Operations within the Bounds of a Memory Buffer Vulnerability		cpe:2.3:a:citrix:netcaler_application_delivery_controller:*:*:*:*:*:* cpe:2.3:a:citrix:netcaler_gateway:*:*:*:*:*:* cpe:2.3:a:citrix:netcaler_application_delivery_controller:*:*:*:*:fips:*:* cpe:2.3:a:citrix:netcaler_application_delivery_controller:*:*:*:*:ndcpp:*:*	-
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-119	T1190: Exploit Public-Facing Application, T1059: Command and Scripting Interpreter, T1059.004: Unix Shell, T1105: Ingress Tool Transfer, T1505: Server Software Component	https://support.citrix.com/external/article/CX697174/citrix-netscaler-adc-and-citrix-netscale.html

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
<u>CVE-2026-104286</u>		Fortinet FortiMail 8.0.0 through 8.0.1, 7.6.0 through 7.6.6, 7.4.0 through 7.4.8, 7.2.0 through 7.2.9	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEY	cpe:2.3:a:fortinet:fortimail:*:*:*:*:*:*:*	-
Fortinet FortiMail Path Traversal Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-22, CWE-158	T1190: Exploit Public-Facing Application, T1059: Command and Scripting Interpreter	https://fortiguard.fortinet.com/psirt/FG-IR-26-175

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
<u>CVE-2025-34035</u>		EnGenius EnShare Cloud Service version 1.4.11 and earlier.	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEY	cpe:2.3:h:engeniustech:esr300:-:*:*:*:*:*:*	ClingSTUN Backdoor
EnGenius EnShare Cloud Service OS Command Injection Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-78	T1190: Exploit Public-Facing Application, T1059: Command and Scripting Interpreter, T1059.004: Unix Shell, T1105: Ingress Tool Transfer	

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
<u>CVE-2026-21589</u>		Atlassian Bitbucket Data Center Version before 9.4.26,10.2.8, 10.5.1, Confluence Data Center Version before 9.2.26, 10.2.19, Jira Service Management Data Center Version before 5.12.40,10.3.26, 11.3.12, Jira Software Data Center Version before 9.12.40, 10.3.26,11.3.12, Bamboo Data Center Versions before 10.2.24,12.1.12, Crowd Data Center Version before 6.3.7, 7.0.3,7.1.7,7.2.4, Crucible Version before 4.9.15 and Fisheye Version before 4.9.15	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSO MWARE
NAME	CISA KEV	cpe:2.3:a:atlassian:bitbucket:*:*:*:*:data_center:*:**, cpe:2.3:a:atlassian:confluence:*:*:*:*:data_center:*:**, cpe:2.3:a:atlassian:jira_service_management:*:*:*:*:data_center:*:**, cpe:2.3:a:atlassian:jira_software:*:*:*:*:data_center:*:**, cpe:2.3:a:atlassian:bamboo:*:*:*:*:data_center:*:**, cpe:2.3:a:atlassian:crowd:*:*:*:*:data_center:*:**, cpe:2.3:a:atlassian:crucible:*:*:*:*:*:*:*:*:, cpe:2.3:a:atlassian:fisheye:*:*:*:*:*:*:*:*:	-
Atlassian Multiple Products Arbitrary File Access Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-552	T1190: Exploit Public-Facing Application, T1552: Unsecured Credentials	https://confluence.atlassian.com/security/cve-2026-21589-arbitrary-file-access-vulnerability-impacts-multiple-products-1870495748.html

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
<u>CVE-2022-36553</u>		Hytec Inter HWL-2511-SS v1.05 and below	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEY	cpe:2.3:o:hytec:hwl-2511-ss_firmware:*:*:*:*:*:*	ClingSTUN Backdoor
Hytec Inter HWL-2511-SS Command Injection Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-77	T1190: Exploit Public-Facing Application, T1059: Command and Scripting Interpreter, T1059.004: Unix Shell, T1105: Ingress Tool Transfer	
CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
<u>CVE-2024-23625</u>		D-Link DAP-1650 devices	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEY	cpe:2.3:o:dlink:dap-1650_firmware:-:*:*:*:*:*	ClingSTUN Backdoor
D-Link UPnP SUBSCRIBE Code Injection Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-77	T1190: Exploit Public-Facing Application, T1210: Exploitation of Remote Services, T1059: Command and Scripting Interpreter, T1059.004: Unix Shell	

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
<u>CVE-2021-35394</u>		Realtek Jungle SDK version v2.x up to v3.4.14B	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEY	cpe:2.3:a:realtek:rtl819x_jungle_software_development_kit:*:*:*:*:*:*:*:*	ClingSTUN Backdoor
Realtek Jungle SDK Remote Code Execution Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-78	T1190: Exploit Public-Facing Application, T1210: Exploitation of Remote Services, T1059: Command and Scripting Interpreter, T1059.004: Unix Shell	https://www.realtek.com/images/safe-report/Realtek_APRouter_SDK_Advisory-CVE-2021-35392_35395.pdf

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
<u>CVE-2023-1389</u>		TP-Link Archer AX21 (AX1800) firmware versions before 1.1.4 Build 20230219	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEY	cpe:2.3:o:tp-link:archer_ax21_firmware:*:*:*:*:*:*:*:	ClingSTUN Backdoor
TP-Link Archer AX-21 Command Injection Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-77	T1190: Exploit Public-Facing Application, T1059: Command and Scripting Interpreter, T1059.004: Unix Shell, T1584: Compromise Infrastructure, T1584.008: Network Devices	https://www.tp-link.com/us/support/download/archerax21/v3/#Firmware

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
<u>CVE-2024-7029</u>		AVTECH AVM1203	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEY	cpe:2.3:o:avtech:avm1203_firmware:*:*:*:*:*:*	ClingSTUN Backdoor
AVTECH AVM1203 Command Injection Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-77	T1190: Exploit Public-Facing Application, T1059: Command and Scripting Interpreter, T1059.004: Unix Shell, T1584: Compromise Infrastructure, T1584.005: Botnet	

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
<u>CVE-2024-10915</u>		D-Link DNS-320, DNS-320LW, DNS-325 and DNS-340L up to 20241028	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEY	cpe:2.3:o:dlink:dns-320_firmware:*:*:*:*:*:*	ClingSTUN Backdoor
D-Link Command Injection Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-707, CWE-74, CWE-78	T1190: Exploit Public-Facing Application, T1059: Command and Scripting Interpreter, T1059.004: Unix Shell, T1105: Ingress Tool Transfer	

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
<u>CVE-2024-23624</u>		D-Link DAP-1650 devices	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEY	cpe:2.3:o:dlink:dap-1650_firmware:-:*:*:*:*:*	ClingSTUN Backdoor
D-Link DAP-1650 Command Injection Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-77	T1190: Exploit Public-Facing Application, T1210: Exploitation of Remote Services, T1059: Command and Scripting Interpreter, T1059.004: Unix Shell	

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
<u>CVE-2019-17621</u>		D-Link DIR-859 Wi-Fi router 1.05 and 1.06B01 Beta01	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEY	cpe:2.3:o:dlink:dir-859_firmware:*:*:*:*:*:*	ClingSTUN Backdoor
D-Link DIR-859 Router Command Execution Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-78	T1190: Exploit Public-Facing Application, T1210: Exploitation of Remote Services, T1059: Command and Scripting Interpreter, T1059.004: Unix Shell	https://www.dlink.com/en/security-bulletin

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
<u>CVE-2019-7256</u>		Linear eMerge E3-Series devices	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEY	cpe:2.3:o:nortekcontrol:linear_emoji_merge_essential_firmware:*:*:*:*:*	ClingSTUN Backdoor
Nice Linear eMerge E3-Series OS Command Injection Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-78	T1190: Exploit Public-Facing Application, T1059: Command and Scripting Interpreter, T1059.004: Unix Shell, T1105: Ingress Tool Transfer	https://linear-solutions.com/software-downloads/

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
<u>CVE-2021-36380</u>		Sunhillo SureLine before 8.7.0.1.1	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEY	cpe:2.3:a:sunhillo:sureline:*:*:*:*:*	ClingSTUN Backdoor
Sunhillo SureLine OS Command Injection Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-78	T1190: Exploit Public-Facing Application, T1059: Command and Scripting Interpreter, T1059.004: Unix Shell, T1105: Ingress Tool Transfer	https://www.sunhillo.com/product/sureline/

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
<u>CVE-2024-21887</u>		Ivanti Connect Secure (9.x, 22.x) and Ivanti Policy Secure (9.x, 22.x)	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEY	cpe:2.3:a:ivanti:policy_secure:- :*:*:*:*:*:*	ClingSTUN Backdoor
Ivanti Connect Secure and Policy Secure Command Injection Vulnerability		cpe:2.3:a:ivanti:connect_secure: :*:*:*:*:*:*	
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-77	T1190: Exploit Public-Facing Application, T1059: Command and Scripting Interpreter, T1059.004: Unix Shell, T1505: Server Software Component, T1505.003: Web Shell	https://hub.ivanti.com/s/article/CVE-2023-46805-Authentication-Bypass-CVE-2024-21887-Command-Injection-for-Ivanti-Connect-Secure-and-Ivanti-Policy-Secure-Gateways?language=en_US

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
<u>CVE-2023-46805</u>		Ivanti ICS 9.x, 22.x and Ivanti Policy Secure	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEY	cpe:2.3:a:ivanti:policy_secure:- :*:*:*:*:*:*	ClingSTUN Backdoor
Ivanti Connect Secure and Policy Secure Authentication Bypass Vulnerability		cpe:2.3:a:ivanti:connect_secure: :*:*:*:*:*:*	
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-287	T1190: Exploit Public-Facing Application, T1133: External Remote Services, T1059: Command and Scripting Interpreter, T1059.004: Unix Shell	https://hub.ivanti.com/s/article/CVE-2023-46805-Authentication-Bypass-CVE-2024-21887-Command-Injection-for-Ivanti-Connect-Secure-and-Ivanti-Policy-Secure-Gateways?language=en_US

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
<u>CVE-2024-46048</u>		Tenda FH451 v1.0.0.9	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEY	cpe:2.3:o:tenda:fh451_firmware:-:*:*:*:*:*	ClingSTUN Backdoor
Tenda exeCommand Command Injection Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-77	T1190: Exploit Public-Facing Application, T1059: Command and Scripting Interpreter, T1059.004: Unix Shell, T1105: Ingress Tool Transfer	

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
<u>CVE-2024-35340</u>		Tenda FH1206 V1.2.0.8(8155)	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEY	cpe:2.3:o:tenda:fh1206_firmware:-:*:*:*:*:*	ClingSTUN Backdoor
Tenda exeCommand Command Injection Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-77	T1190: Exploit Public-Facing Application, T1059: Command and Scripting Interpreter, T1059.004: Unix Shell, T1105: Ingress Tool Transfer	

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
CVE-2024-32281		Tenda AC7V1.0 v15.03.06.44	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEY	cpe:2.3:o:tenda:ac7_firmware:-:*:*:*:*:*:*	ClingSTUN Backdoor
Tenda exeCommand Command Injection Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-77	T1190: Exploit Public-Facing Application, T1059: Command and Scripting Interpreter, T1059.004: Unix Shell, T1105: Ingress Tool Transfer	

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
CVE-2022-35555		Tenda W6 V1.0.0.9(4122)	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEY	cpe:2.3:o:tenda:w6_firmware:-:*:*:*:*:*:*	ClingSTUN Backdoor
Tenda W6 exeCommand Command Injection Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-78	T1190: Exploit Public-Facing Application, T1059: Command and Scripting Interpreter, T1059.004: Unix Shell, T1105: Ingress Tool Transfer	

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
<u>CVE-2022-26289</u>		Tenda M3 1.10 V1.0.0.12(4856)	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEY	cpe:2.3:o:tenda:m3_firmware:-:*:*:*:*:*:*	ClingSTUN Backdoor
Tenda exeCommand Command Injection Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-78	T1190: Exploit Public-Facing Application, T1059: Command and Scripting Interpreter, T1059.004: Unix Shell, T1105: Ingress Tool Transfer	

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
<u>CVE-2022-37055</u>		D-Link Go-RT-AC750 GORTAC750_revA_v101b03 and GO-RT-AC750_revB_FWv200b02	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEY	cpe:2.3:o:dlink:go-rt-ac750_firmware:-:*:*:*:*:*:*	ClingSTUN Backdoor
D-Link Routers Buffer Overflow Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-120	T1190: Exploit Public-Facing Application, T1059: Command and Scripting Interpreter, T1059.004: Unix Shell, T1499: Endpoint Denial of Service, T1499.004: Application or System Exploitation	EOL

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
<u>CVE-2024-10914</u>		D-Link DNS-320, DNS-320LW, DNS-325 and DNS-340L up to 20241028	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEY	cpe:2.3:o:dlink:dns-320_firmware:*:*:*:*:*:*	ClingSTUN Backdoor
D-Link NAS Command Injection Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-707, CWE-74, CWE-78	T1190: Exploit Public-Facing Application, T1059: Command and Scripting Interpreter, T1059.004: Unix Shell, T1105: Ingress Tool Transfer	EOL

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
<u>CVE-2026-36356</u>		MeiG Smart FORGE_SLT711 devices (firmware MDM9607.LE.1.0-00110-STD.PROD-1)	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEY	-	ClingSTUN Backdoor
MeiG Smart FORGE_SLT711 GoAhead Command Injection Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-306, CWE-78	T1190: Exploit Public-Facing Application, T1059: Command and Scripting Interpreter, T1059.004: Unix Shell, T1105: Ingress Tool Transfer	

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
<u>CVE-2025-67038</u>		Lantronix EDS5000 2.1.0.0R3	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEY	cpe:2.3:o:lantronix:eds5008_firmware:*:*:*:*:*:*	ClingSTUN Backdoor
Lantronix EDS5000 Code Injection Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-78	T1190: Exploit Public-Facing Application, T1059: Command and Scripting Interpreter, T1059.004: Unix Shell, T1105: Ingress Tool Transfer	https://ltrxdev.atlassian.net/wiki/spaces/LTRXTS/pages/2538438657

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
<u>CVE-2014-8361</u>		Realtek SDK	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEY	cpe:2.3:o:dlink:dir-905l_firmware:*:*:*:*:*:*	ClingSTUN Backdoor
Realtek SDK Improper Input Validation Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	-	T1210: Exploitation of Remote Services, T1059: Command and Scripting Interpreter, T1059.004: Unix Shell, T1570: Lateral Tool Transfer	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10055

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
<u>CVE-2016-20016</u>		MVPower CCTV DVR models, including TV-7104HE 1.8.4 115215B9 and TV7108HE	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEY	cpe:2.3:o:mvpower:tv-7104he_firmware:-:*:*:*:*:*	ClingSTUN Backdoor
MVPower Remote Command Execution Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-78	T1210: Exploitation of Remote Services, T1505: Server Software Component, T1505.003: Web Shell, T1059: Command and Scripting Interpreter, T1059.004: Unix Shell	

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
<u>CVE-2024-3721</u>		TBK DVR-4104 and DVR-4216 up to 20240412	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEY	-	ClingSTUN Backdoor
TBK DVR OS Command Injection Vulnerability			
	CWE ID		PATCH LINK
	CWE-78	T1210: Exploitation of Remote Services, T1059: Command and Scripting Interpreter, T1059.004: Unix Shell, T1570: Lateral Tool Transfer	EOL

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
<u>CVE-2025-34037</u>		Linksys E-Series Routers	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEY	-	ClingSTUN Backdoor
Linksys E-Series Routers OS Command Injection Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-78	T1210: Exploitation of Remote Services, T1059: Command and Scripting Interpreter, T1059.004: Unix Shell, T1570: Lateral Tool Transfer	

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
<u>CVE-2023-26801</u>		LB-LINK BL-AC1900_2.0 v1.0.1, LB-LINK BL-WR9000 v2.4.9, LB-LINK BL-X26 v1.2.5, and LB-LINK BL-LTE300 v1.0.8	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEY	cpe:2.3:o:lb-link:bl-lte300_firmware:-:*:*:*:*:*	ClingSTUN Backdoor
lb-link bl-lte300_firmware Command Injection Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-77	T1210: Exploitation of Remote Services, T1059: Command and Scripting Interpreter, T1059.004: Unix Shell, T1570: Lateral Tool Transfer	

Adversaries in Action

No threat actor activity was observed or reported during this week.

Recommendations

Security Teams

This digest can be utilized as a drive to force security teams to prioritize the **35 exploited vulnerabilities** and block the indicators related to the malware **Chopper, Godzilla, CoinMiner, Looptik, Zimdown2, Zimclient2, ShelbyLoader, ShelbyC2, PsProxy, Blackwood, Shai-Hulud, and ClingSTUN**.

Uni5 Users

This is an actionable threat digest for HivePro Uni5 customers, and they can get comprehensive insights into their threat exposure and act on it effortlessly over the HivePro Uni5 dashboard by

- Run a Scan to discover the assets impacted by the **35 exploited vulnerabilities**.
- Test the efficacy of their security controls by simulating attacks related to the malware **Mini Shai-Hulud, ClingSTUN Downloader, and BlinderTunnel** in Breach and Attack Simulation(BAS).

Threat Advisories

[274 Mail Servers Down as CVE-2026-73570 Fuels Zimbra SNMP Exploitation Wave](#)

[Citrix NetScaler SAML Zero-Day CVE-2026-88779 Under Active Exploitation](#)

[Fortinet FortiMail Zero-Day Exploited to Write Arbitrary Files](#)

[One Flaw, Eight Products: Atlassian's Critical Pre-Auth File Read \(CVE-2026-21589\)](#)

[Blinder Tunnel: Iran-Nexus Actor Hides Backdoor in Fake Coding Test](#)

[Hostage Token: Shai-Hulud Hijacks Tensorlake's npm SDK](#)

[ClingSTUN Backdoor Turns Exposed IoT Devices into Stealthy Proxy Nodes](#)

Appendix

Known Exploited Vulnerabilities (KEV): Software vulnerabilities for which there are public exploits or proof-of-concept (PoC) code available, and for which there is a high risk of potential harm to an organization's systems or data if left unaddressed.

Celebrity Vulnerabilities: Software vulnerabilities that have gained significant attention and have been branded with catchy names and logos due to their profound and multifaceted impact. These vulnerabilities provide threat actors with opportunities to breach sensitive systems, potentially resulting in unauthorized access and the compromise of critical information.

✂ Indicators of Compromise (IOCs)

Attack Name	TYPE	VALUE
<u>Chopper</u>	SHA256	13d27ecfbb6b3d55bdabcaa3a2ade83ecfaa3df92dbc22be05e6d9e2d18087b6, dc76d856d42242e58eb8d4b70d5378f42f3ddf0ef7872d2279f2d67c22806e26, 5cc6bc95c584d72cc61842f0ee58f38ac4519ec953a2dff3d37e2e8f389f3d54
<u>CoinMiner</u>	SHA256	aea991f694911e321b0ab97534f2ad0291c392c0a43dabff664c563618bd036d
<u>Looptik</u>	SHA256	65a7576c389326b6cdf9c993d0be6e5d50fed9655d1cdf2a3a50f2c21c8ec435
<u>Zimdown2</u>	SHA256	bf28f38122bf20d5fac969cc414daa6a890cdea872d389ca93d2092b6b7773cf
<u>Zimclient2</u>	SHA256	b594a42b8f1c6f090327bb9a3361c2d3515537fb7ac8da6b9061b9a3f330e159
<u>ShelbyC2</u>	Filename	RuntimeBrokerApi.dll
<u>PsProxy</u>	Filename	PsProxy.dll
	SHA256	3fd810a3aa0039993393741b32287c367a9a5037a41e826906440887cdd3ed13

Attack Name	TYPE	VALUE
<u>ShelbyLoader</u>	Filename	RuntimeBroker.dll, RuntimeBroker.exe.config, DubaiAirport_Carrers_IT_Test.zip, FlightManager.csproj
	SHA256	53f35e49eb9b271fd8cbcd3daacb525328dbf159a03dbd1c7adebe0363daa402, 6e7d9b33f1e72ea1ede71373a604ecdb060dab7d42055179c1eede9ecd1fd239, f5b12772db6817f7a765a6fe7565fd3d4f87edc28e42fe3ec0244a372a410fc9
<u>Blackwood</u>	IPv4	91[.]107[.]156[.]29, 65[.]109[.]214[.]145, 87[.]248[.]129[.]239, 65[.]109[.]214[.]145[:.]8080
	SHA256	76273382e4252c1f60a2251141e108942494409c759358320735891762c0682e, d3561bd4aad003dc3e08157b0891860bb496b80cd6e44901692e08ab1d4e8260, f5ba1645694c62f527ed6ceda8c68a5c3dd92b4032439167e8e937e72803b4bd, 7cc571aca6d8715d9aaad3d83e1bcd30467565d583db1dfe73697c5d00a1f875
<u>Shai-Hulud</u>	SHA256	25a0735d0db7dc40e5d45ce42d9c106067e6a66e184d967cfecfab17c3bcb5ef, b50a00900399ba99fb6ce1fc151519cb99d44320ef2a631f2237e1aea0ad6fec
<u>ClingSTUN</u>	SHA256	e6e113783356446aef66e5296db45b244f318292af7cebc2a9bd76f095a95c4c, c1d8e2829ea63b9dc1cf2c3421a5093406adad4d6622e238376e78e908e0e6e8, ec199c78c11040fd3127887222fd75a85e5797bf96aa691a117fdd83dd663d81, dc892f5013edb0aa1e61e808511387373d8d120348b5be0929621d21e6e9946a

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 13, 2026 • 01:40 AM

© 2026 All Rights are Reserved by Hive Pro



More at www.hivepro.com