

Date of Publication
September 7, 2026



HiveForce Labs
WEEKLY
THREAT DIGEST

Attacks, Vulnerabilities, and Actors

31 AUGUST to 6 SEPTEMBER 2026

Table Of Contents

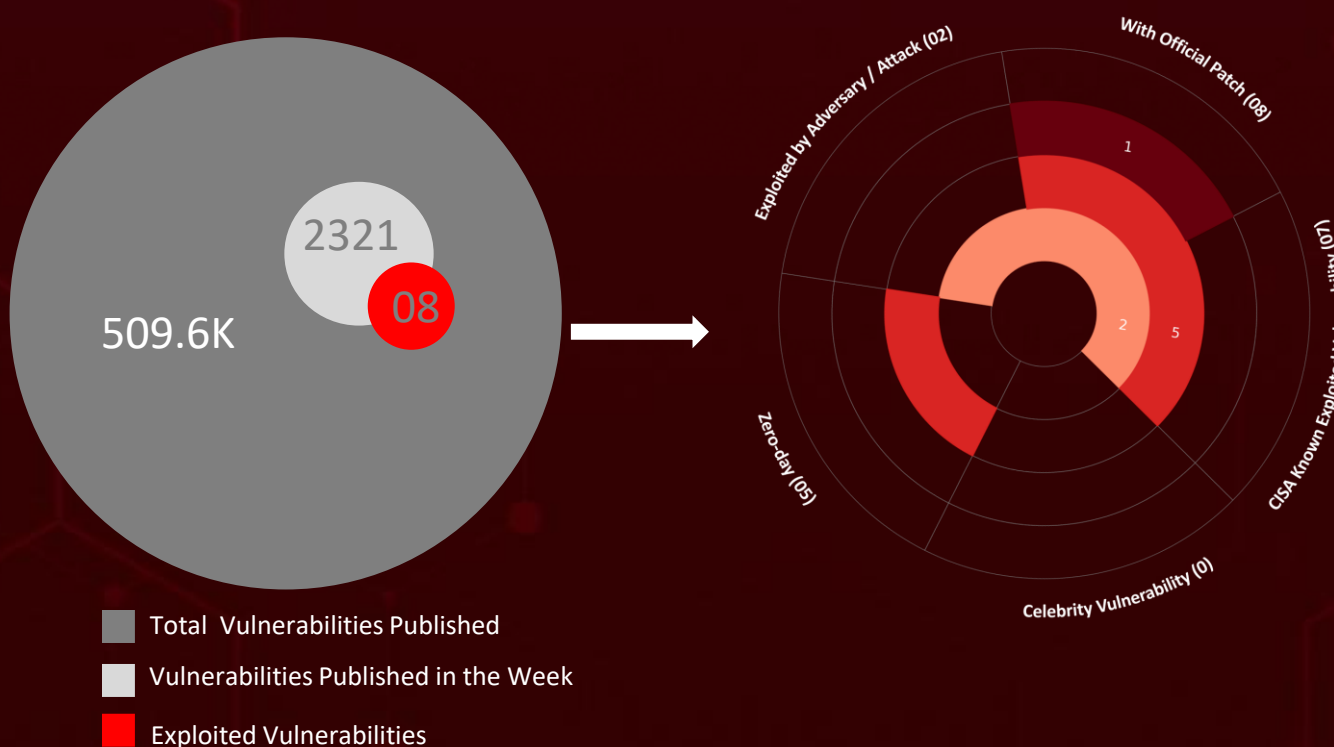
<u>Summary</u>	03
<u>High Level Statistics</u>	04
<u>Insights</u>	05
<u>Targeted Countries</u>	06
<u>Targeted Industries</u>	07
<u>Top MITRE ATT&CK TTPs</u>	07
<u>Attacks Executed</u>	08
<u>Vulnerabilities Exploited</u>	10
<u>Adversaries in Action</u>	18
<u>Recommendations</u>	19
<u>Threat Advisories</u>	20
<u>Appendix</u>	21
<u>What Next?</u>	23

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, **three** major attacks were detected, **eight** vulnerabilities were actively exploited, and **one** threat actor group was closely monitored, signaling a concerning escalation in malicious activity worldwide.

On the vulnerability front, SonicWall confirmed active exploitation of two zero-days in its Secure Mobile Access (SMA) 1000 series. **CVE-2026-83548**, a maximum-severity flaw in the Work Place interface, lets unauthenticated attackers reach sensitive internal functions through server-side request forgery, while **CVE-2026-83549** lets an already-logged-in administrator run arbitrary commands via the Appliance Management Console. SonicWall caught both internally and has already shipped hotfixes. Google, meanwhile, patched a high-severity type confusion bug in Chrome's V8 engine, **CVE-2026-85046**, that was also being exploited in the wild, a compiler bug affecting Maglev and TurboFan that gave attackers arbitrary read/write access to the JavaScript heap through nothing more than a crafted webpage.

On the threat-actor side, the Iran-linked group **Mirage Kitten** (aka Nimbus Manticore) is running a recruitment-themed campaign against aviation, aerospace, and FinTech professionals across the Middle East and Africa, posing as recruiters on LinkedIn and job boards to hand out trojanized coding-challenge files that quietly install two new cross-platform RATs, **NodeRabbit** and **PollCat**, capable of remote access, credential theft, and data exfiltration. Separately, a ClickFix-style campaign dubbed **TerminalFix** tricks victims with a fake Cloudflare CAPTCHA into pasting a PowerShell command that ultimately sideloads malware, sets up persistence, maps out the Active Directory environment, and opens a hidden proxy tunnel for the attacker. Together, these incidents point to a clear pattern: attackers are blending technical exploits with social engineering, making timely patching, vigilant monitoring, and layered defenses more essential than ever.



High Level Statistics

3

Attacks
Executed

8

Vulnerabilities
Exploited

1

Adversaries in
Action

- [NodeRabbit](#)
- [PollCat](#)
- [Retrograde/MiniFa](#)
[st](#)
- [CVE-2026-72529](#)
- [CVE-2026-72530](#)
- [CVE-2026-82078](#)
- [CVE-2026-81578](#)
- [CVE-2026-83548](#)
- [CVE-2026-83549](#)
- [CVE-2026-32475](#)
- [CVE-2026-85046](#)
- [Mirage Kitten](#)



Insights

Two **PaperCut** zero-days chain into an auth bypass and then into RCE, and since the first two emergency patches were bypassable, only Release 3 holds. Patch every server, and treat any exposed one as already breached.

A form field becomes a foothold: Elementor Pro's **CVE-2026-32475** lets attackers upload a PHP file through a contact form and run it as code, 10M+ WordPress sites in the blast radius.

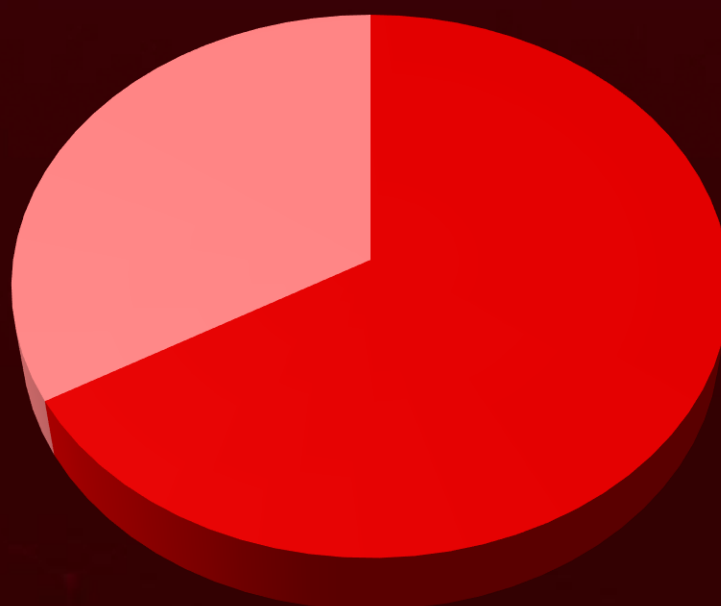
Another V8 zero-day in the wild: Chrome's **CVE-2026-85046** type confusion bug is under active attack; patch to 152.0.7977.82 now, not later.

Two **SonicWall SMA 1000** zero-days chained: one unauthenticated SSRF opens the door, one command injection walks right through to full device takeover.

Iran-linked **Mirage Kitten** baits aviation and FinTech pros with fake LinkedIn recruiters; the "coding challenge" is really cross-platform Node.js RATs hiding C2 behind Azure and Cloudflare.

The CAPTCHA is the con: **TerminalFix** tricks victims into pasting a PowerShell command that daisy-chains DLL sideloading, PNG-hidden payloads, and AD recon into a Python reverse-tunnel backdoor.

Threat Distribution



■ RAT

■ Backdoor

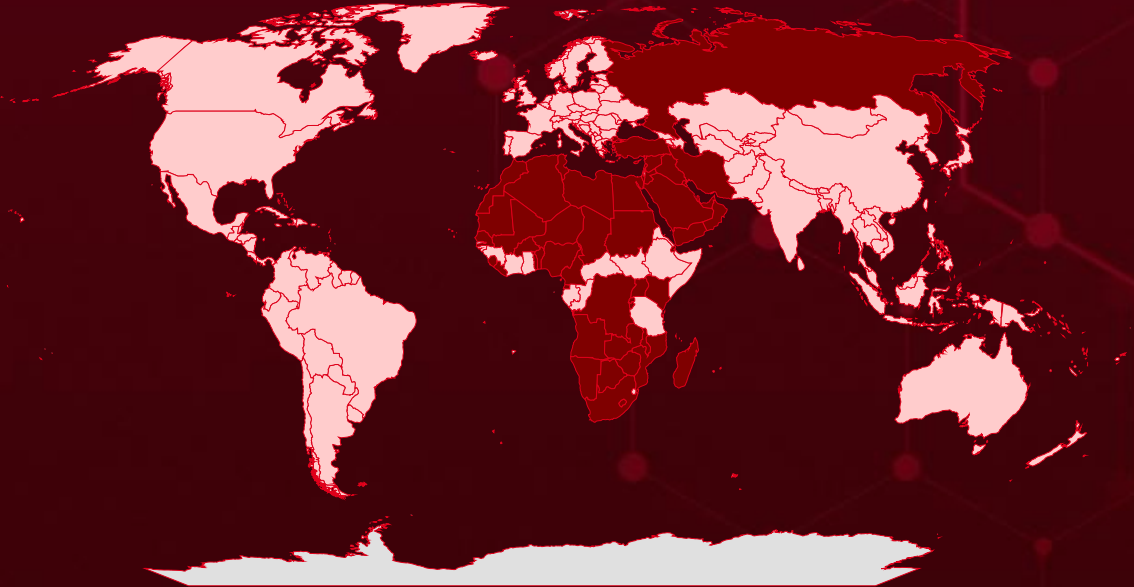


Targeted Countries

Most



Least

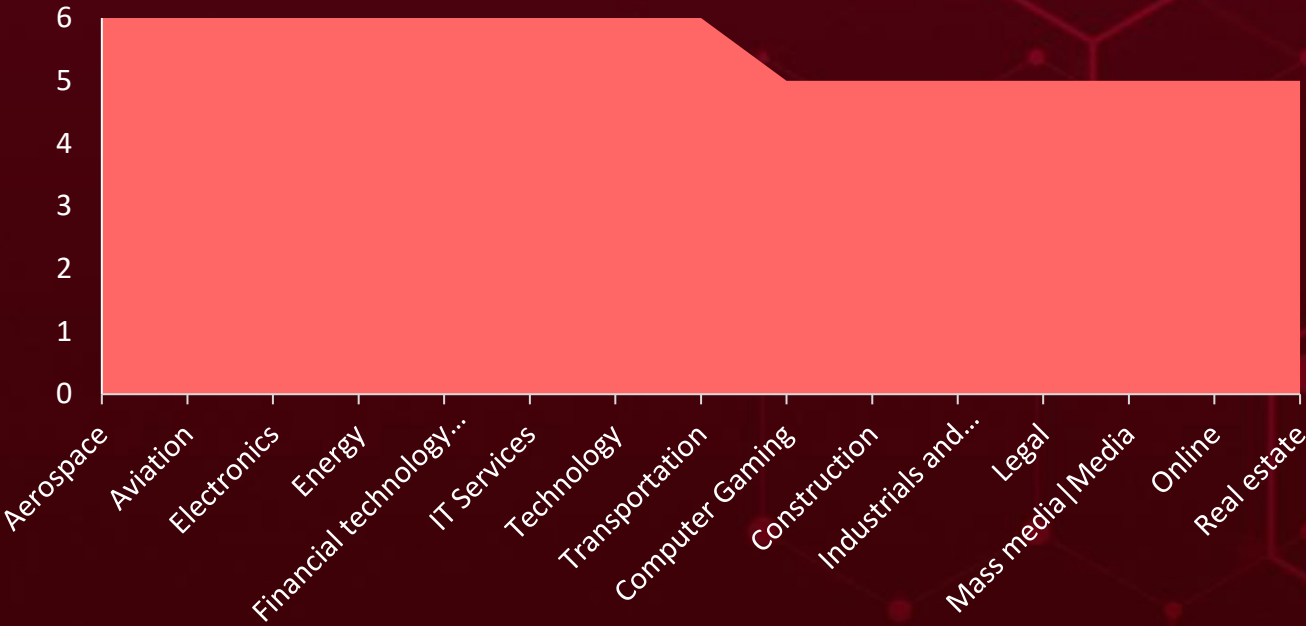


Powered by Bing

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

Countries	Countries	Countries	Countries
Morocco	Cyprus	United Arab Emirates	Faroe Islands
Syria	Mali	Libya	North Korea
Russia	Democratic Republic of Congo	Zambia	Fiji
Algeria	Mauritius	Madagascar	Panama
Zimbabwe	Djibouti	Malawi	Finland
Angola	Mozambique	Lebanon	Canada Quebec
Nigeria	Egypt	Slovakia	France
Bahrain	Niger	Norway	Saint Lucia
Seychelles	Equatorial Guinea	Uruguay	French Guiana
Benin	Oman	Dominica	Serbia
Uganda	Iran	Cayman Islands	Gabon
Botswana	Qatar	Dominican Republic	Spain
Mauritania	Iraq	Tibet	Georgia
Burkina Faso	Rwanda	Ecuador	Taiwan
Namibia	Israel	New Zealand	Germany
Burundi	Senegal	Bahamas	Tonga
Palestine	Jordan	Philippines	Ghana
Cameroon	Sierra Leone	El Salvador	Australia
Saudi Arabia	Kenya	San Marino	Gibraltar
Cape Verde	Sudan	Akrotiri and Dhekelia	Vietnam
South Africa	Kuwait	Swaziland	Greece
Chad	Togo	Estonia	
Tunisia	Lesotho	Turkmenistan	
Comoros	Turkey	Ethiopia	
Yemen	Liberia		

Targeted Industries



TOP MITRE ATT&CK TTPs

T1059 Command and Scripting Interpreter	T1190 Exploit Public-Facing Application	T1588 Obtain Capabilities	T1588.006 Vulnerabilities	T1082 System Information Discovery
T1036 Masquerading	T1505 Server Software Component	T1027 Obfuscated Files or Information	T1547 Boot or Logon Autostart Execution	T1189 Drive-by Compromise
T1543 Create or Modify System Process	T1204 User Execution	T1105 Ingress Tool Transfer	T1068 Exploitation for Privilege Escalation	T1572 Protocol Tunneling
T1070 Indicator Removal	T1546 Event Triggered Execution	T1566 Phishing	T1564 Hide Artifacts	T1102 Web Service

Attacks Executed

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
<u>NodeRabbit</u>	A cross-platform Node.js RAT and Mirage Kitten's first Node.js implant, running on Windows, Linux, and macOS. Launched by a trojanized npm package, it persists by masquerading as legitimate updaters and encrypts C2 traffic with AES-256-GCM. Across three variants it supports up to 23 commands.	Trojanized coding-challenge archives	-
TYPE		IMPACT	AFFECTED PLATFORM
RAT		Remote access, data exfiltration	Windows, Linux, macOS
ASSOCIATED ACTOR			PATCH LINK
Mirage Kitten			-
IOC TYPE	VALUE		
Domains	naturalapplication[.]azurewebsites[.]net, retaildemo[.]azurewebsites[.]net, tubitak[.]azurewebsites[.]net,		

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
PollCat	A cross-platform RAT written in obfuscated JavaScript, delivered via an OTP-gated React coding challenge. It runs independently of the lure, registers with its C2, and profiles the host against 24 security-vendor directories. It declares 22 commands and persists via scheduled tasks, cron, or LaunchAgents.	Trojanized React coding challenge	-
TYPE		IMPACT	AFFECTED PLATFORM
RAT		Remote access, host profiling	Windows, Linux, macOS
ASSOCIATED ACTOR			PATCH LINK
Mirage Kitten			-
IOC TYPE	VALUE		
Domain	lifespotify[.]com, gamebarapp[.]azurewebsites[.]net, gamebarappinformation[.]azurewebsites[.]net		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
Retrograde/MiniFast	A native Windows DLL backdoor previously attributed to Mirage Kitten, used here as PollCat's attribution comparator. It shares an identical C2 handshake, host registration, polling logic, and beacon timing, but implements functional UAC elevation and scheduled-task persistence.	-	-
TYPE		IMPACT	AFFECTED PLATFORM
Backdoor		Remote access, privilege escalation	Windows
ASSOCIATED ACTOR			PATCH LINK
Mirage Kitten			-
IOC TYPE	VALUE		
MD5	810F8E3B88EB05F710C09552941D6F56		

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-2026-72529</u>		TrueConf server versions 5.3.X to 5.3.9, 5.4.X to 5.4.9, 5.5.X to 5.5.5, and earlier	Head Mare
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEY	cpe:2.3:a:trueconf:trueconf_server:*:*:*:*:*	PhantomCore PhantomGraph
TrueConf Server Missing Authentication for Critical Function Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINKS
	CWE-306	T1059:Command and Scripting Interpreter	https://trueconf.com/blog/update/trueconf-server-security-updates-june-2026 , https://trueconf.com/products/tcsf/trueconf-server-free.html

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
<u>CVE-2026-72530</u>		TrueConf server versions 5.3.X to 5.3.9, 5.4.X to 5.4.9, 5.5.X to 5.5.5, and earlier	Head Mare
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEY	cpe:2.3:a:trueconf:trueconf_server:*:*:*:*:*	PhantomCore PhantomGraph
TrueConf Server Code Injection Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINKS
	CWE-94	T1059:Command and Scripting Interpreter	https://trueconf.com/blog/update/trueconf-server-security-updates-june-2026 , https://trueconf.com/products/tcsf/trueconf-server-free.html

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
<u>CVE-2026-82078</u>		All versions of PaperCut NG and PaperCut MF	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEY	cpe:2.3:a:papercut:papercut_ng: *:~*:~*:~*:~*:~*:~* cpe:2.3:a:papercut:papercut_mf: *:~*:~*:~*:~*:~*:~*	-
PaperCut NG and PaperCut MF Unsafe Dynamic Class Loading Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-470	T1190:Exploit Public-Facing Application, T1059:Command and Scripting Interpreter, T1070:Indicator Removal	https://www.papercut.com/kb/Main/security-bulletin-27-aug-2026-urgent-security-advisory/

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
<u>CVE-2026-81578</u>		All versions of PaperCut NG and PaperCut MF	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEY	cpe:2.3:a:papercut:papercut_ng: *.~*.~*.~*.~*.~*.~*	-
PaperCut NG and PaperCut MF Authentication Bypass Vulnerability		cpe:2.3:a:papercut:papercut_mf: *.~*.~*.~*.~*.~*.~*	
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-306	T1190:Exploit Public-Facing Application, T1562:Impair Defenses	https://www.papercut.com/kb/Main/security-bulletin-27-aug-2026-urgent-security-advisory/

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
<u>CVE-2026-83548</u>		SonicWall SMA 1000 (6210, 7210, 8200v) 12.4.3-03453 and 12.5.0-02835 (platform-hotfix) and older versions	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:sonicwall:sma1000:*:*:*:*:*:*	-
SonicWall SMA1000 Appliances Server-Side Request Forgery Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-918, CWE-441	T1190: Exploit Public-Facing Application, T1068: Exploitation for Privilege Escalation	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2026-0016

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
<u>CVE-2026-83549</u>		SonicWall SMA 1000 (6210, 7210, 8200v) 12.4.3-03453 and 12.5.0-02835 (platform-hotfix) and older versions	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:sonicwall:sma1000:*:*:*:*:*:*	-
SonicWall SMA1000 Appliances OS Command Injection Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-78	T1190: Exploit Public-Facing Application, T1059: Command and Scripting Interpreter	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2026-0016

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
<u>CVE-2026-32475</u>		WordPress Elementor Pro (Before 4.2.2)	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:elementor:elementor_pro:*:*:*:*:*	-
WordPress Elementor Pro Unauthenticated Arbitrary File Upload Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-434	T1190: Exploit Public-Facing Application, T1059: Command and Scripting Interpreter	https://wordpress.org/plugins/elementor/

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
<u>CVE-2026-85046</u>		Google Chrome (Before 152.0.7977.82 Linux; Before 152.0.7977.82/.83 Windows, macOS)	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEY	cpe:2.3:a:google:chrome:*:*:*:*:*:*	-
Google Chrome V8 Type Confusion Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-843	T1190:Exploit Public-Facing Application, T1059.007 Command and Scripting Interpreter: JavaScript	https://chromerelease.s.googleblog.com/2026/09/stable-channel-update-for-desktop_01882797386.html



Adversaries in Action

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED REGIONS
 <u>Mirage Kitten</u> (aka <u>UNC1549</u>, <u>TA455</u>, <u>Smoke</u> <u>Sandstorm</u>, <u>Bohrium</u>, <u>DEV-</u> <u>0056</u>, <u>Yellow</u> <u>Dev 13</u>, <u>Subtle</u> <u>Snail</u>, <u>Nimbus</u> <u>Manticore</u>, <u>Screening</u> <u>Serpens</u>, <u>GalaxyGato</u>)	Iran	Aerospace, Aviation, FinTech	Middle East and Africa
	MOTIVE		
	Information theft and espionage		
	TARGETED CVE	ASSOCIATED ATTACKS/RANSOM WARE	AFFECTED PRODUCT
	-	NodeRabbit, PollCat, Retrograde/MiniFast	Windows, linux and mac
TTPs			
TA0042: Resource Development, TA0001: Initial Access, TA0002: Execution, TA0005: Defense Evasion, TA0007: Discovery, TA0009: Collection, TA0010: Exfiltration, TA0011: Command and Control, T1583: Acquire Infrastructure, T1566: Phishing, T1204: User Execution, T1129: Shared Modules, T1059: Command and Scripting Interpreter, T1574: Hijack Execution Flow, T1497: Virtualization/Sandbox Evasion, T1027: Obfuscated/Encoded Files or Information, T1036: Masquerading, T1082: System Information Discovery, T1083: File and Directory Discovery, T1057: Process Discovery, T1113: Screen Capture, T1005: Data from Local System, T1583.001: Domains, T1583.006: Web Services, T1566.002: Spearphishing Link, T1204.002: Malicious File, T1574.002: DLL, T1497.001: System Checks, T1036.005: Match Legitimate Resource Name or Location, T1071: Application Layer Protocol, T1572: Protocol Tunneling, T1090: Proxy, T1105: Ingress Tool Transfer, T1041: Exfiltration Over C2 Channel, T1071.001: Web Protocols			

Recommendations

Security Teams

This digest can be utilized as a drive to force security teams to prioritize the **eight exploited vulnerabilities** and block the indicators related to the threat actor **Mirage Kitten** and malware **NodeRabbit, PollCat, and Retrograde/MiniFast**.

Uni5 Users

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

- Run a Scan to discover the assets impacted by the **eight exploited vulnerabilities**.
- Testing the efficacy of their security controls by simulating the attacks related to the threat actor **Mirage Kitten** and malware **Retrograde/MiniFast** in Breach and Attack Simulation(BAS).

Threat Advisories

[Head Mare Chains TrueConf Server Flaws to Drop PhantomCore and PhantomGraph](#)

[PaperCut NG/MF Zero-Day Under Active Exploitation Across All Versions](#)

[Two SMA 1000 Zero-Days Open SonicWall Appliances to RCE](#)

[Mirage Kitten Turns Job Interviews into a Gateway for Corporate Espionage](#)

[One Empty File to Full Takeover: Elementor Pro Under Active Attack](#)

[CVE-2026-85046: Chrome V8 Type Confusion Zero-Day Exploited in the Wild](#)

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>NodeRabbit</u>	Domains	naturalapplication[.]azurewebsites[.]net, retaildemo[.]azurewebsites[.]net, tubitak[.]azurewebsites[.]net, rgbteller[.]azurewebsites[.]net, wslwebui[.]azurewebsites[.]net, plugplay[.]azurewebsites[.]net, crossdwm[.]azurewebsites[.]net, wdisystem[.]azurewebsites[.]net, wslmenus[.]azurewebsites[.]net, dnshnsdev[.]azurewebsites[.]net, hpjumpsrv[.]azurewebsites[.]net, storview[.]azurewebsites[.]net, healthcomfsdpower[.]com, visitfinancedentists[.]com, kyrasey-f8hfexa5cqamh7fk[.]westeurope-01[.]azurewebsites[.]net, greenyjsgfd[.]azurewebsites[.]net, helptellerbls[.]azurewebsites[.]net, timedrv[.]azurewebsites[.]net, userwellgtfs[.]azurewebsites[.]net, hecowime-aqdphyd4bbdef6es[.]westeurope-01[.]azurewebsites[.]net, msmanagementgrp[.]com, msmanagementgrpmedia[.]com

Attack Name	TYPE	VALUE
<u>PollCat</u>	URL	hxxps[:]//lifespotify[.]com/api/users/b879746e-fed9-4211-a6da-4d8223681267/otp/validate,
	Filenames	RankChallenge-react-6uJSX3-main.zip, requireObject.js
	Domains	lifespotify[.]com, gamebarapp[.]azurewebsites[.]net, gamebarappinformation[.]azurewebsites[.]net, sahi-finance[.]com
<u>Retrograde/M</u> <u>iniFast</u>	MD5	810F8E3B88EB05F710C09552941D6F56
	SHA256	0db36a04d304ad96f9e6f97b531934594cd95a5cea9ff2c9af249201089dc864

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

September 07, 2026 • 08:30 AM

© 2026 All Rights are Reserved by Hive Pro



More at www.hivepro.com