

Date of Publication
November 25, 2024



HiveForce Labs

WEEKLY

THREAT DIGEST

Attacks, Vulnerabilities and Actors

18 to 24 NOVEMBER 2024

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>	11
<u>Adversaries in Action</u>	17
<u>Recommendations</u>	18
<u>Threat Advisories</u>	19
<u>Appendix</u>	20
<u>What Next?</u>	23

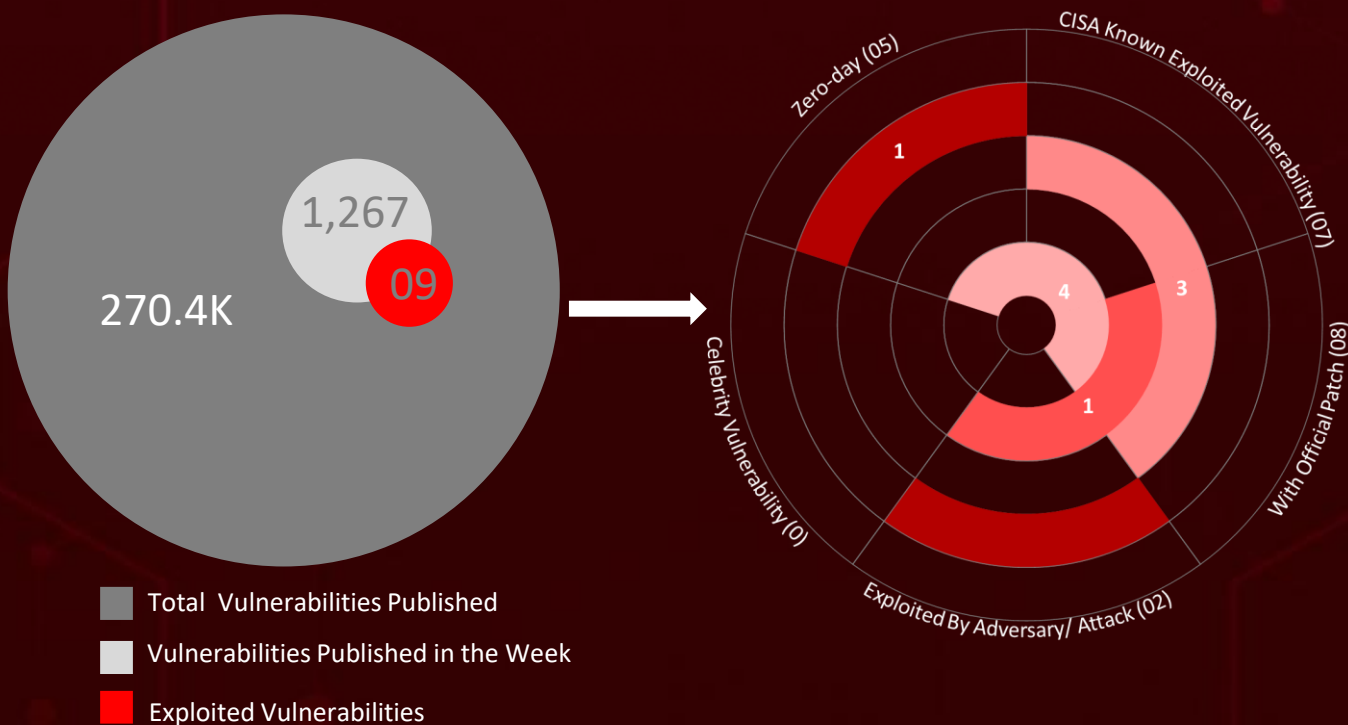
Summary

HiveForce Labs has unveiled a series of significant cybersecurity threats, emphasizing the accelerating pace and complexity of cyber incidents. Over the past week, **five** attacks were identified, **nine** critical vulnerabilities were actively exploited, and **one** active threat group was closely monitored, highlighting an unyielding surge in cyber intrusions.

One standout vulnerability, [CVE-2024-11120](#), represents a critical OS command injection flaw affecting outdated GeoVision devices. Actively weaponized by botnets such as Mirai for DDoS attacks and crypto mining, this flaw presents a severe risk, particularly with no available patches.

In parallel, Palo Alto Networks released essential updates addressing two actively exploited zero-day vulnerabilities, while Apple tackled two critical zero-day flaws, [CVE-2024-44308](#) and [CVE-2024-44309](#), impacting Intel-based Mac systems.

Adding to the urgency, the [Helldown ransomware](#) campaign continues to wreak havoc, compromising over 30 organizations with a double extortion approach encrypting data while threatening to expose it. This campaign exploits vulnerabilities such as [CVE-2024-42057](#) in Zyxel firewalls. These alarming developments underline the escalating sophistication of cybercriminal tactics and reinforce the urgent need for robust global cybersecurity measures.



High Level Statistics

5

Attacks
Executed

9

Vulnerabilities
Exploited

1

Adversaries in
Action

- Mirai
- Helldown
- DEEPDATA
- LIGHTSPY
- NodeStealer

- CVE-2024-11120
- CVE-2024-38812
- CVE-2024-38813
- CVE-2024-0012
- CVE-2024-9474
- CVE-2024-44308
- CVE-2024-44309
- CVE-2024-42057
- CVE-2024-21287

- BrazenBamboo

Insights

NodeStealer

Malware Targets Facebook Ads and Credit Card Data

No Patch, No Peace: CVE-2024-11120 Amplifies Mirai's Power

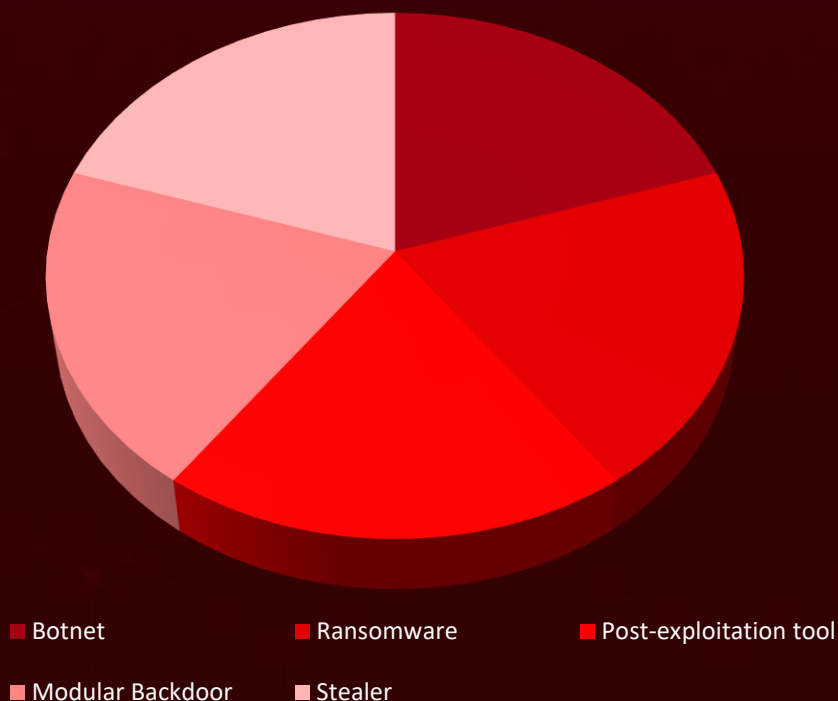
Chinese Threat Actors Leverage **DEEPDATA** Against Fortinet VPNs

IT and Healthcare Face **Helldown's** Dual Threat Impacting **30** Organizations and Counting

Apple Zero-Day Exploits Put Intel-Based Macs in the Crosshairs

File Disclosure Flaw in Oracle Agile PLM Risks Corporate Data Exposure

Threat Distribution



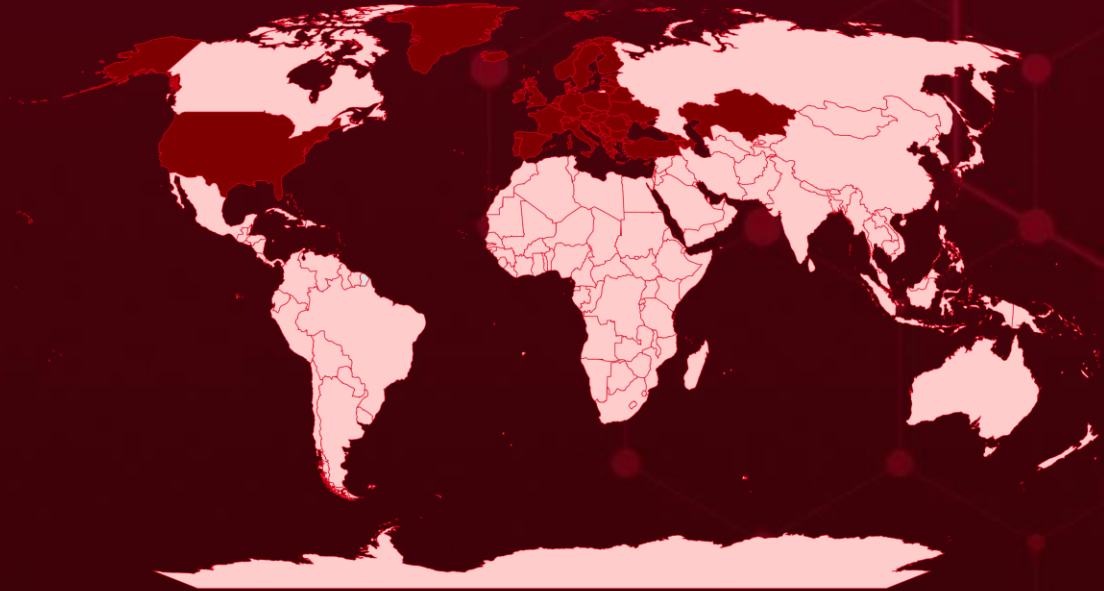


Targeted Countries

Most



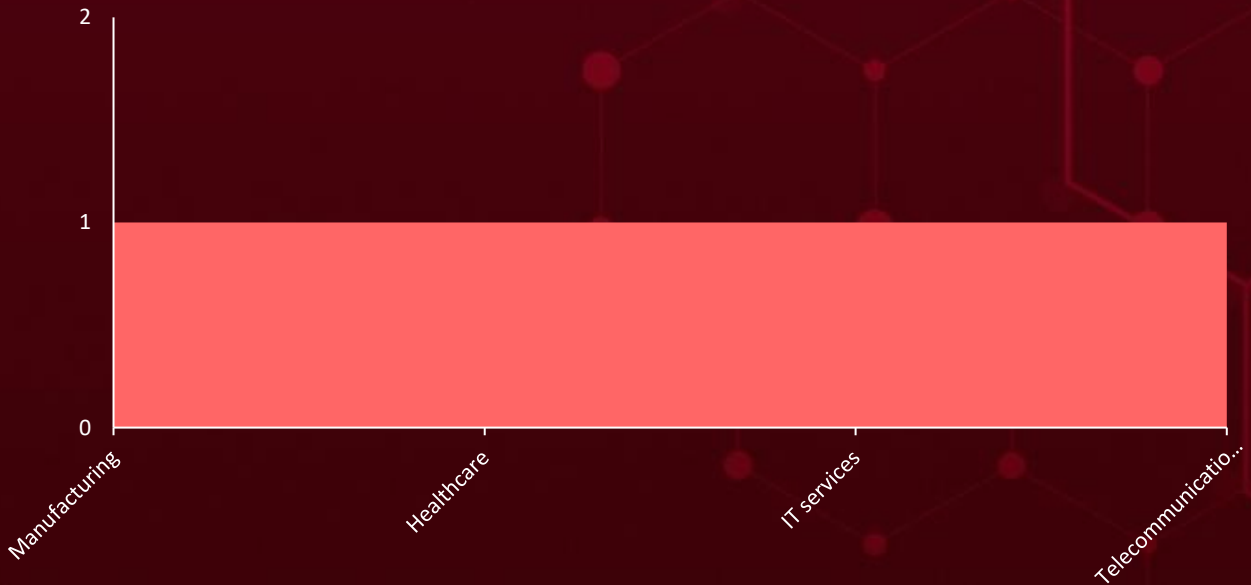
Least



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

Countries	Countries	Countries	Countries
Vatican City	United Kingdom	Ukraine	Paraguay
Portugal	Czech Republic	Isle of Man	Ethiopia
Moldova	Kazakhstan	United States	Saint Lucia
Akrotiri and Dhekelia	Denmark	Italy	Falkland Islands
Svalbard	Abkhazia	Jersey	Senegal
Åland	Estonia	Latvia	American Samoa
Liechtenstein	Lithuania	Saba	Clipperton Island
Albania	Faroe Islands	Vietnam	Fiji
North Macedonia	Malta	Sudan	South Sudan
Andorra	Finland	Palau	Afghanistan
Slovakia	Monaco	Djibouti	Coral Sea Islands
Armenia	France	Singapore	Bahamas
Turkey	Netherlands	Dominica	Tonga
Austria	Georgia	Argentina	Uzbekistan
Kosovo	Northern Cyprus	Dominican Republic	Gabon
Azerbaijan	Germany	Norfolk Island	Zambia
Luxembourg	Poland	East Timor	Gambia
Belarus	Gibraltar	Cayman Islands	Nigeria
Montenegro	Romania	Samoa	Bahrain
Belgium	Greece	Ecuador	Cameroon
Norway	Serbia	South Africa	Bangladesh
Bosnia and Herzegovina	Greenland	Egypt	Oman
San Marino	Slovenia	Tanzania	Ghana
Bulgaria	Guernsey	El Salvador	Panama
Croatia	Spain	United Arab Emirates	Barbados
Switzerland	Hungary	Equatorial Guinea	Philippines
Cyprus	Sweden	Nicaragua	Puerto Rico
	Iceland	Anguilla	
	Ireland	Russia	

Targeted Industries



TOP MITRE ATT&CK TTPs

T1059

Command and Scripting Interpreter

T1588

Obtain Capabilities

T1588.006

Vulnerabilities

T1588.005

Exploits

T1068

Exploitation for Privilege Escalation

T1556

Modify Authentication Process

T1606.001

Web Cookies

T1190

Exploit Public-Facing Application

T1606

Forge Web Credentials

T1569.002

Service Execution

T1555

Credentials from Password Stores

T1590

Gather Victim Network Information

T1071

Application Layer Protocol

T1560

Archive Collected Data

T1071.001

Web Protocols

T1587.004

Exploits

T1074

Data Staged

T1547

Boot or Logon Autostart Execution

T1078

Valid Accounts

T1059.003

Windows Command Shell

🔪 Attacks Executed

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
Mirai	Mirai is a self-replicating malware that scours the internet for vulnerable IoT devices, infecting them to form a botnet. Variants of Mirai leverage lists of commonly used default credentials to gain unauthorized access to these devices.	Exploiting Vulnerability in GeoVision	CVE-2024-11120
TYPE		IMPACT	AFFECTED PRODUCT
Botnet			
ASSOCIATED ACTOR		Distributed Denial of Service (DDoS) Attacks, Information Theft	GeoVision Devices
-	PATCH DETAILS		
			End of Life GeoVision device is affected
IOC TYPE	VALUE		
SHA256	37a59fed3530d15fa1cdf7c0da92530e9477cfda4d943a45146434c760fe4623, b90ee829760f9ed154033b1e3c428368b808cfc9cb161b67f6b618af9a36ee, edd1c8dab9d8821408e1983365de1b5e804771f22a1bb9644ef5a6ed642754cb		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
Helldown	Helldown ransomware utilizes a double extortion approach, encrypting data while simultaneously threatening to expose sensitive information unless the ransom is paid. Although Helldown shares code similarities with LockBit 3.0, it remains a distinct variant and is actively being developed.	Exploitation of vulnerabilities in Zyxel	CVE-2024-42057
TYPE		IMPACT	AFFECTED PRODUCT
Ransomware			
ASSOCIATED ACTOR		Financial Loss, Data Breaches and Reputation Damage	Zyxel ATP series
-	PATCH LINK		
			https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-09-03-2024
IOC TYPE	VALUE		
SHA256	0bfe25de8c46834e9a7c216f99057d855e272eafafdfef98a6012cecbddcfab, 7cd7c04c62d2a8b4697ceebbe7dd95c910d687e4a6989c1d839117e55c1cafd7		

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>DEEPDATA</u> TYPE Post-exploitation tool ASSOCIATED ACTOR BrazenBamboo	The DEEPDATA toolkit is a modular post-exploitation framework crafted to extract sensitive information from compromised Windows systems. Operating through command-line execution, its FortiClient plugin leverages the msenvico.dll library file to exploit a zero-day vulnerability. Upon deployment, the plugin extracts VPN credentials directly from the process memory of the FortiClient application.	Exploiting Vulnerability	-
		IMPACT	AFFECTED PRODUCT
		Information Theft, Post-Exploitation Persistence	FortiClient
			PATCH LINK
			-
IOC TYPE	VALUE		
SHA256	f4e72145e761bcc8226353bb121eb8e549dc0000c6535bfa627795351037dc8e, 041c13a29d3bee8d2e4bd9d8bde8152b5ac8305c1efcc198244b224e33635282		




NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
<u>LIGHTSPY</u> TYPE Modular Backdoor ASSOCIATED ACTOR BrazenBamboo	LIGHTSPY is a multi-platform malware family with documented Android, iOS, and macOS variants. As a modular backdoor, it enables attackers to execute shell commands and manipulate files on compromised devices remotely. Additionally, LIGHTSPY has various modules designed to exfiltrate data from the infected system.	Exploiting Vulnerability	-
		IMPACT	AFFECTED PRODUCT
		Information Theft, Remote Command Execution	FortiClient
			PATCH LINK
			-
IOC TYPE	VALUE		
SHA256	32f2348a5cd8de57f3b1c6b68f4b95c4e1c9d2b55f257bd0c2deca7f81ad1c4c, 98dc1fb1773277bbea2bdeaf88b1ece101b5b0e7aec2857017268001a6996e9f, 2689e08a103682095ef8eba016f28909199cb4365b84c815183be64686a11084		




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>NodeStealer</u>	<p>NodeStealer is a Python-based stealer malware that has evolved with enhanced capabilities to cause greater damage. This version targets not only credentials stored in web browsers but also sensitive credit card information.</p> <p>Furthermore, it has been upgraded to extract additional data from victims' Facebook Ads Manager accounts, significantly increasing its potential impact on businesses and individuals.</p>	-	-
TYPE		IMPACT	AFFECTED PRODUCT
Stealer			-
ASSOCIATED ACTOR			PATCH LINK
-		Credential Theft, Business and Individual Reputational Damage	-
IOC TYPE	VALUE		
SHA256	c5d4e4d9fa2c201d74a14fd1972b670fde243f087451a3a7dc52a9a6db61a1cb, 641f2db9e9fb8255337672fb8da9226225fa8e393b651c7c7ebbb5b555d4b755, ea25dd47b43ddaa3df11e6d16544702a8fabbbcd0031ba11d1df51461704a8973		




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 ACTOR
<u>CVE-2024-11120</u>		GeoVision VS12, GeoVision VS11, GeoVision DSP_LPR_V3, GeoVision LX 4 V2, GeoVision LX 4 V3	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:o:geovision:gvlx_4_v3_firmware:*:*:*:*:*:* cpe:2.3:o:geovision:gvlx_4_v2_firmware:*:*:*:*:*:* cpe:2.3:o:geovision:gv-vs12_firmware:*:*:*:*:*:* cpe:2.3:o:geovision:gv-vs11_firmware:*:*:*:*:*:* cpe:2.3:o:geovision:gv-dsp_lpr_v3_firmware:*:*:*:*:*:*	Mirai
GeoVision OS Command Injection Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH DETAILS
	CWE-78	T1498: Network Denial of Service, T1059: Command and Scripting Interpreter, T1588.005: Exploits	End of Life GeoVision device is affected




CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-38812		VMware vCenter Server: 7.0 - 8.0, VMware Cloud Foundation: 4.x - 5.1.x	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEY	cpe:2.3:a:vmware:vcenter_server:*:*:*:*:*:*	
VMware vCenter Server Heap-Overflow Vulnerability		cpe:2.3:a:vmware:cloud_foundation:*:*:*:*:*:*	-
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-122	T1574: Hijack Execution Flow, T1021.003: Distributed Component Object Model	https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/24968




CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-38813		VMware vCenter Server: 7.0 - 8.0, VMware Cloud Foundation: 4.x - 5.1.x	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEY	cpe:2.3:a:vmware:vcenter_server:*:*:*:*:*:*	
VMware vCenter Server Privilege Escalation Vulnerability		cpe:2.3:a:vmware:cloud_foundation:*:*:*:*:*:*	-
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-78	T1068: Exploitation for Privilege Escalation	https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/24968




CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<u>CVE-2024-0012</u>		Palo Alto Networks PAN-OS Versions Prior to 11.2.4-h1, Versions Prior to 11.1.5-h1, Versions Prior to 11.0.6-h1, Versions Prior to 10.2.12-h2	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEY	cpe:2.3:o:paloaltonetworks:pan-os:*:*:*:*:*:*	-
Palo Alto Networks PAN-OS Management Interface Authentication Bypass Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-306	T1556: Modify Authentication Process	<u>https://security.paloaltonetworks.com/CVE-2024-0012</u>

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<u>CVE-2024-9474</u>		Palo Alto Networks PAN-OS Versions Prior to 11.2.4-h1, Versions Prior to 11.1.5-h1, Versions Prior to 11.0.6-h1, Versions Prior to 10.2.12-h2, Versions Prior to 10.1.14-h6	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEY	cpe:2.3:o:paloaltonetworks:pan-os:*:*:*:*:*:*	-
Palo Alto Networks PAN-OS Management Interface OS Command Injection Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-78	T1059: Command and Scripting Interpreter	<u>https://security.paloaltonetworks.com/CVE-2024-9474</u>


CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<u>CVE-2024-44308</u>		Safari Version Prior to 18.1, macOS Version Prior to 15.1, iOS and iPadOS Version Prior to 18.1, visionOS Version Prior to 2.1	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEY	cpe:2.3:a:apple:visionos:*:*:*:*:*:*:*:* cpe:2.3:a:apple:safari:*:*:*:*:*:*:* cpe:2.3:a:apple:macos:*:*:*:*:*:*:* cpe:2.3:a:apple:ios:*:*:*:*:*:*:*:*	-
Apple Multiple Products Code Execution Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-20	T1059: Command and Scripting Interpreter	https://support.apple.com/en-us/118575 https://support.apple.com/en-us/118481 https://support.apple.com/en-us/108382

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<u>CVE-2024-44309</u>		Safari Version Prior to 18.1, macOS Version Prior to 15.1, iOS and iPadOS Version Prior to 18.1, visionOS Version Prior to 2.1	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSO MWARE
NAME	CISA KEY	cpe:2.3:a:apple:visionos:*:*:*:*:*:* *.* cpe:2.3:a:apple:safari:*:*:*:*:*:* * cpe:2.3:a:apple:macos:*:*:*:*:*:* .* cpe:2.3:a:apple:ios:*:*:*:*:*:*	-
Apple Multiple Products Cross-Site Scripting (XSS) Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-79	T1189: Drive-by Compromise	https://support.apple.com/en-us/118575 https://support.apple.com/en-us/118481 https://support.apple.com/en-us/108382

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-42057		Zyxel ATP series	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEY	cpe:2.3:o:zyxel:zld_firmware:* :*:*:*:*:*:*	Helldown ransomware
			
Zyxel ATP series Command Injection Vulnerability	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-78	T1059: Command and Scripting Interpreter, T1133: External Remote Services	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-09-03-2024

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-21287		Oracle Agile PLM Framework Version 9.3.6	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEY	cpe:2.3:a:oracle:agile_plm_framework:*:*:*:*:*:*	-
			
Oracle Agile Product Lifecycle Management (PLM) Incorrect Authorization Vulnerability	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-863	T1565: Data Manipulation, T1068: Exploitation for Privilege Escalation, T1190: Exploit Public-Facing Application	https://support.oracle.com/rs?type=doc&id=3058429.1

Adversaries in Action

NAME	ORIGIN	TARGETED INDUSTRY	TARGETED REGION
 BrazenBamboo	China	All	Worldwide
	MOTIVE Information Theft, Espionage		
	TARGETED CVE	ASSOCIATED ATTACKS/RANSOMWARE	AFFECTED PRODUCT
	-	DEEPDATA, LIGHTSPY	FortiClient
TTPs			
TA0002: Execution; TA0003: Persistence; TA0005: Defense Evasion; TA0006: Credential Access; TA0007: Discovery; TA0009: Collection; TA0011: Command and Control; TA0010: Exfiltration; TA0042: Resource Development; T1059: Command and Scripting Interpreter; T1059.003: Windows Command Shell; T1071: Application Layer Protocol; T1071.001: Web Protocols; T1083: File and Directory Discovery; T1584: Compromise Infrastructure; T1587: Develop Capabilities; T1587.001: Malware; T1587.004: Exploits; T1133: External Remote Services; T1078: Valid Accounts; T1543: Create or Modify System Process; T1562: Impair Defenses; T1212: Exploitation for Credential Access; T1005: Data from Local System			

Recommendations

Security Teams

This digest can be utilized as a drive to force security teams to prioritize the **nine exploited vulnerabilities** and block the indicators related to the threat actor **BrazenBamboo**, and malware **Mirai, Helldown, DEEPDATA, LIGHTSPY, NodeStealer**.

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 **nine exploited vulnerabilities**.
- Testing the efficacy of their security controls by simulating the attacks related to the threat actor **BrazenBamboo**, and malware **Helldown, LIGHTSPY, DEEPDATA, NodeStealer** in Breach, and Attack Simulation(BAS).

Threat Advisories

[Hackers Exploit Zero-Day Flaw in EOL GeoVision Devices](#)

[Active Exploitation of vCenter Server Vulnerabilities](#)

[Critical Zero-Day PAN-OS Flaws Exposing Systems to Full Control](#)

[Apple Addresses Actively Exploited Zero-Day Flaws in macOS and iOS](#)

[New Helldown Ransomware: A Growing Threat Across Cross-Platform Systems](#)

[DEEPDATA Empowers the Exploitation of Unpatched Fortinet Flaw](#)

[Oracle Addresses Agile PLM Flaw Exploited in the Wild](#)

[NodeStealer Reloaded: Targeting Facebook Ads and Credit Cards with New Tactics](#)

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>Mirai</u>	SHA256	37a59fed3530d15fa1cdf7c0da92530e9477cfda4d943a45146434c760fe4623, b90ee829760f9ed154033b1e3c428368b808cfcd39cb161b67f6b618af9a36ee, edd1c8dab9d8821408e1983365de1b5e804771f22a11b9644ef5a6ed642754cb, e4cb3440dcad461a9c2cb9aa0728859efb4ce0f2b94b93e97f3b52de0e5b1447, 8e8f40bb6fa0a14d57b6656b7c020556fca02a721797fb316864460506b9b969, 888f4a852642ce70197f77e213456ea2b3cfca4a592b94647827ca45adf2a5b8, b43a8a56c10ba17ddd6fa9a8ce10ab264c6495b82a38620e9d54d66ec8677b0c, 4f53eb7fbfa5b68cad3a0850b570cbbcb2d4864e62b5bf0492b54bde2bdbe44b
<u>Helldown</u>	SHA256	0bfe25de8c46834e9a7c216f99057d855e272eafafdfef98a6012cecbddcfab, 7cd7c04c62d2a8b4697ceebbe7dd95c910d687e4a6989c1d839117e55c1cafd7, 7731d73e048a351205615821b90ed4f2507abc65acf4d6fe30ecdb211f0b0872, 3e3fad9888856ce195c9c239ad014074f687ba288c78ef26660be93ddd97289e, 2621c5c7e1c12560c6062fdf2eeeb815de4ce3856376022a1a9f8421b4bae8e1, 47635e2cf9d41cab4b73f2a37e6a59a7de29428b75a7b4481205aee4330d4d19,

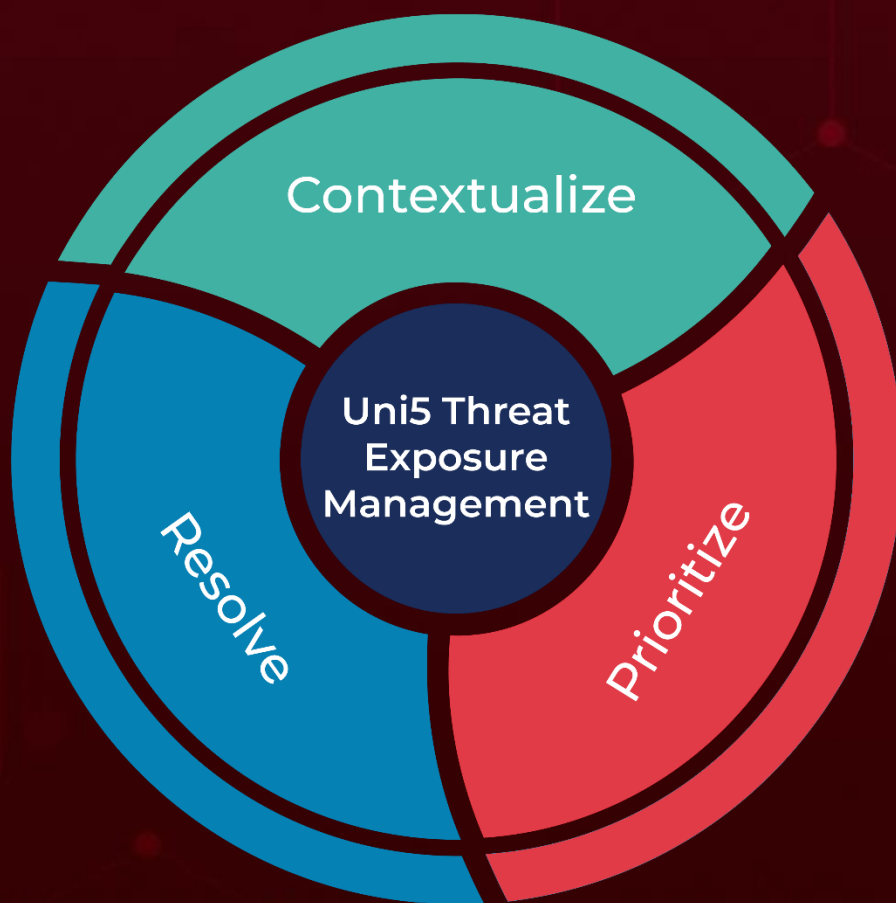
Attack Name	TYPE	VALUE
<u>Helldown</u>	SHA256	cb48e4298b216ae532cfd3c89c8f2cbd1e32bb402866d2c81682c6671aa4f8ea, 67aea3de7ab23b72e02347cbf6514f28fb726d313e62934b5de6d154215ee733, 2b15e09b98bc2835a4430c4560d3f5b25011141c9efa4331f66e9a707e2a23c0, 6ef9a0b6301d737763f6c59ae6d5b3be4cf38941a69517be0f069d0a35f394dd, 9ab19741ac36e198fb2fd912620bf320aa7fdeeeb8d4a9e956f3eb3d2092c92c, ccd78d3eba6c53959835c6407d81262d3094e8d06bf2712fefa4b04baadd4bfe
<u>DEEPDATA</u>	SHA256	f4e72145e761bcc8226353bb121eb8e549dc0000c6535bfa627795351037dc8e, 041c13a29d3bee8d2e4bd9d8bde8152b5ac8305c1efcc198244b224e33635282
<u>LIGHTSPY</u>	SHA256	32f2348a5cd8de57f3b1c6b68f4b95c4e1c9d2b55f257bd0c2deca7f81ad1c4c, 98dc1fb1773277bbea2bdeaf88b1ece101b5b0e7aec2857017268001a6996e9f, 2689e08a103682095ef8eba016f28909199cb4365b84c815183be64686a11084, 6a5d7e2c950960d9a541ff27e9c74185d27564f879d42f261f70f8f7cb70b5ce, c4e5dc5f301a5be652b4cf491c7337dd0d15f4b09982e5a361d06dcbca95a32d, a3fcf7b16ea46100c1cadbbf770492de07633afb4720c78fd1981627aa9f3c6, 3c3aca2a6d4a4f7210c869affe55e05b55c110d53fc3fb9d46cb2847fb115238, ddd950ddceff147922cef44f781c2c4b77b6e803613f83761ee6d5e2bb1450b7, 562ae257506a25de48019cb13947090d164181ba4e107ea19a0ab8274ad696df, 7fe822ef8e51efece5c0c6540aeeb454985ab91518aad12c6bf24c025a0350fe, 8b686507065623248f8292524195c39d4ae94e2a7a1315bb9d8a22178a5b1942, 90ac267222e38ce06724527fb780816db57bef12b939d37d6d827b826fa909d7, bdfb0e52ebb6f79d37736fab0150cfb96e2965d62c242adc830b6aab7b1d37db, 9c86203004ed0a519d8dcc674fd0e4b1b736289ea5f33e37b4dddd111767fd37, aa81f6dc28086656a6e69c7a696e6fedf6e35b242dc072ee7960449c806af7ae, b7dd27414ba4afddaf946e4ab9d8d775a511f3ad99933bde19456216477f3716, c5d84c20a379320bd06ab09ed84c5cd2003cbb0e518f561853fc0c9f9970d49a,

Attack Name	TYPE	VALUE
<u>LIGHTSPY</u>	SHA256	7802b373a8c26211d0c2624910a414555fbc509d46ab9fb8aad5f2686d98dd8e, 5bdcd83c8561255764f91fda531e8cbdda808600eb75758e44e66df3d1ae1311, 2af751cc194213a40aa8b1cd6f589da260cea81c0509bd694ae28dfca87cd160, db66cd7f1a84d29977af4c9eccc36c84e42903766401a2760ea4321b71ba92ff, 15528f109da5ffd687e41eb1a193ff28711bc6054a538b7ba58eef3fbaf10b09, 02f36b26b73cd4fe632e45fc1d668b57045068e167d737f9befa652046880561, 36f72df74306363676488ef2f6842c653fd565b7a50ad6867ceb0b95cab40411, 31466e06d8bea3f2b567be103a630fe2b2249c3818efd45de37f8c3bbe248984, dd08c6f797f068a267f997895651dadf9dda7e0fc5f7cb66302934a7269839af, 1f77953f4ced82c4a5df3e7a85643054ef4bc5fe9dd13f87a9f042c5986b3169, e4e2eccc3a545a3c925fe4f54cb1f9c7d6259098c01659781900876543a89eba, f31b9ca07b9d70aee742d92e2b8f7c9ea6033beff6b85a64900cfd7b8878c3a0, 5cdcb1cacb27c539494e02aba7e264e0959741184215c69da66a11a5815c5025, 3cf03ce0ed2b9840d8d9ed467d105df177dac2818101964c97ba9a281a180558, 0f66a4daba647486d2c9d838592cba298df2dbf38f2008b6571af8a562bc306c
<u>NodeStealer</u>	SHA256	c5d4e4d9fa2c201d74a14fd1972b670fde243f087451a3a7dc52a9a6db61a1cb, 641f2db9e9fb8255337672fb8da9226225fa8e393b651c7c7ebbb5b555d4b755, ea25dd47b43ddaa3df11e6d16544702a8fabbcd0031ba11d1df51461704a8973, 4613225317e768d6d69b412843a314e2af64960856a0cfd798ed52285867bc36, 8dcccc38514c8167c849c1bba9c3c6ef20f219a7439d2fc1f889410e34d8f6c9

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 free demo with HivePro Uni5:Threat Exposure Management Platform.



REPORT GENERATED ON

November 25, 2024 • 10:30 PM

© 2024 All Rights are Reserved by Hive Pro



More at www.hivepro.com