Date of Publication
February 2, 2026

Hive Pro

Hiveforce Labs

WEEKLY

THREAT DIGEST

Attacks, Vulnerabilities, and Actors

26 JANUARY to 1 FEBRUARY 2026

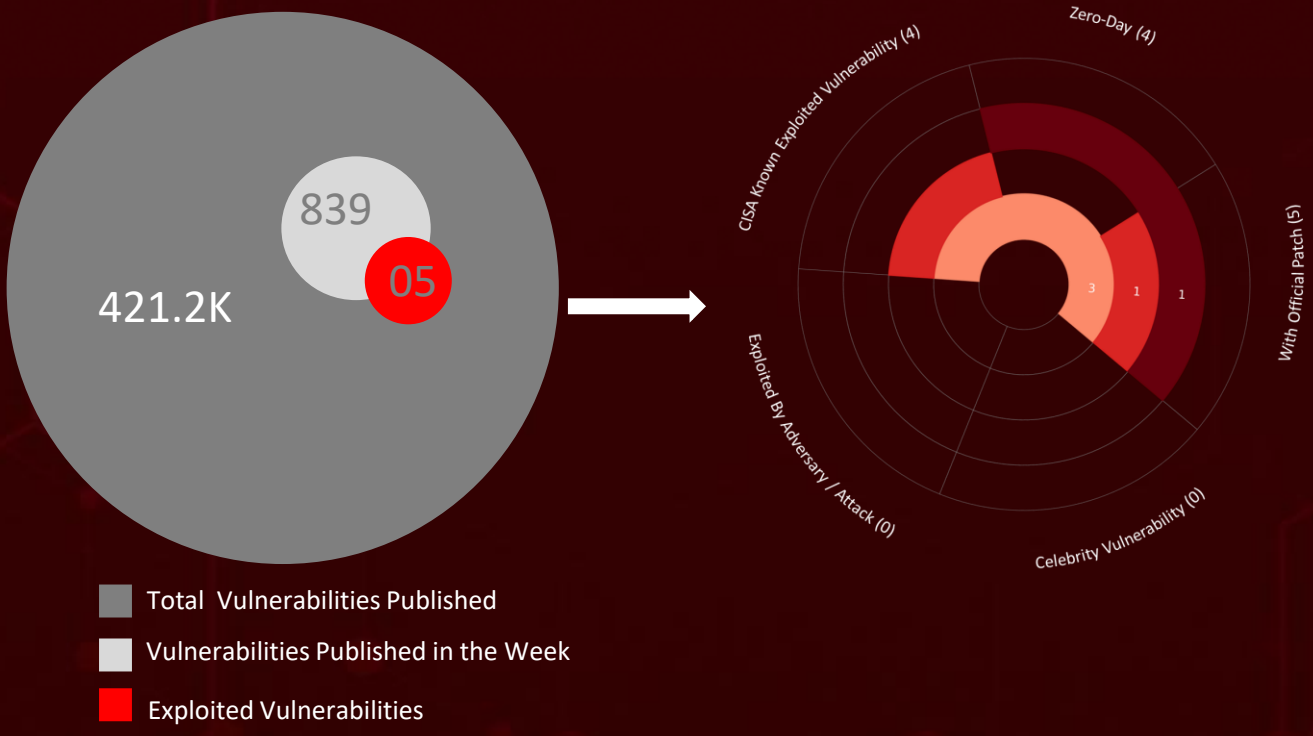
Table Of Contents

Summary

HiveForce Labs has reported a notable surge in global cyber threats, underscoring how both the volume and sophistication of attacks continue to escalate. In just the past week, observed **nine** significant attack incidents, the public disclosure of **five** new vulnerabilities, and operations linked to **two** threat actor groups. Together, these developments point to an increasingly volatile threat landscape, where organizations face mounting pressure to defend against faster, more complex, and more coordinated malicious activity.

A key driver behind this spike is the exploitation of several high-impact vulnerabilities, including active zero-day threats. **CVE-2026-21509**, a high-severity Microsoft Office security feature bypass, enables attackers to evade built-in OLE protections using specially crafted documents and has already been exploited in real-world attacks across multiple Office versions. Meanwhile, **CVE-2026-24061** places organizations running vulnerable GNU InetUtils telnetd services at severe risk, as attackers can gain unauthenticated root access. Adding to the urgency, **CVE-2026-24858**, a critical authentication bypass flaw affecting several Fortinet products when FortiCloud SSO is enabled, allows attackers with any valid FortiCloud account to gain unauthorized administrative access to devices across organizations and has been exploited in the wild since mid-January 2026.

Threat actor activity has further amplified concerns, with a Pakistan-linked group conducting two concurrent cyber espionage campaigns, **Gopher Strike** and **Sheet Attack**, against Indian government entities. Additionally, initial access broker **TA584** continues large-scale phishing operations, leveraging ClickFix social engineering to deliver malware such as **Tsundere Bot** and **XWorm**. Collectively, these developments reinforce the urgent need for rapid patch deployment, proactive monitoring, and layered defensive controls to keep pace with an increasingly aggressive and fast-moving threat environment.



High Level Statistics

9
Attacks Executed

5
Vulnerabilities Exploited

2
Adversaries in Action

- GOGITTER
- GITSHELLPAD
- GOSHELL
- SHEETCREEP
- FIREPOWER
- MAILCREEP
- CoolClient
- Tsundere Bot
- XWorm

- CVE-2026-21509
- CVE-2026-24061
- CVE-2026-24858
- CVE-2026-1281
- CVE-2026-1340

- Mustang Panda
- TA584

Insights

CVE-2026-24061 leaves vulnerable telnet servers wide open, enabling attackers to gain instant root access.

Active exploitation of **CVE-2026-21509** highlights how attackers are bypassing Microsoft Office protections to slip malicious documents past defenses.

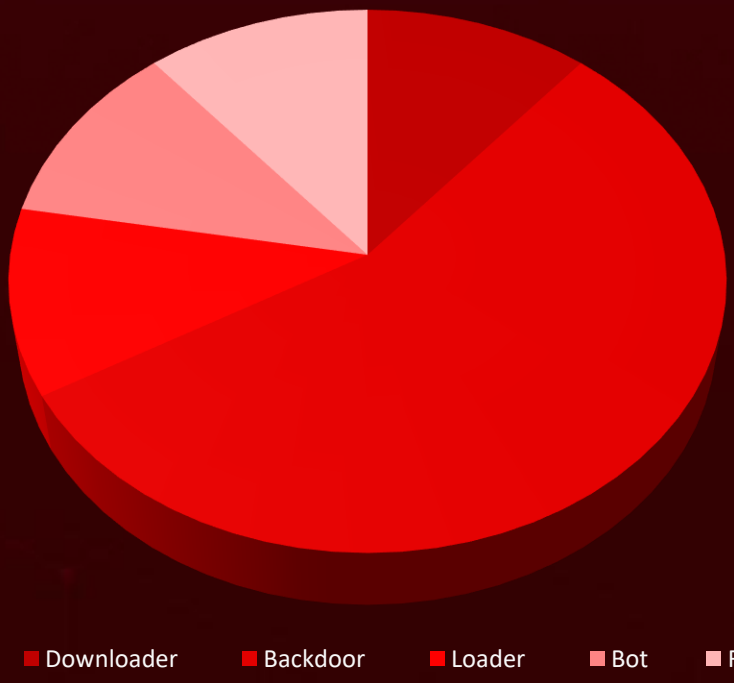
Mustang Panda has stealthily evolved its **CoolClient** backdoor into a quieter, more persistent espionage tool built for long-term surveillance.

CVE-2026-24858 turns Fortinet SSO into an open door, letting attackers hijack administrative control across vulnerable organizations.

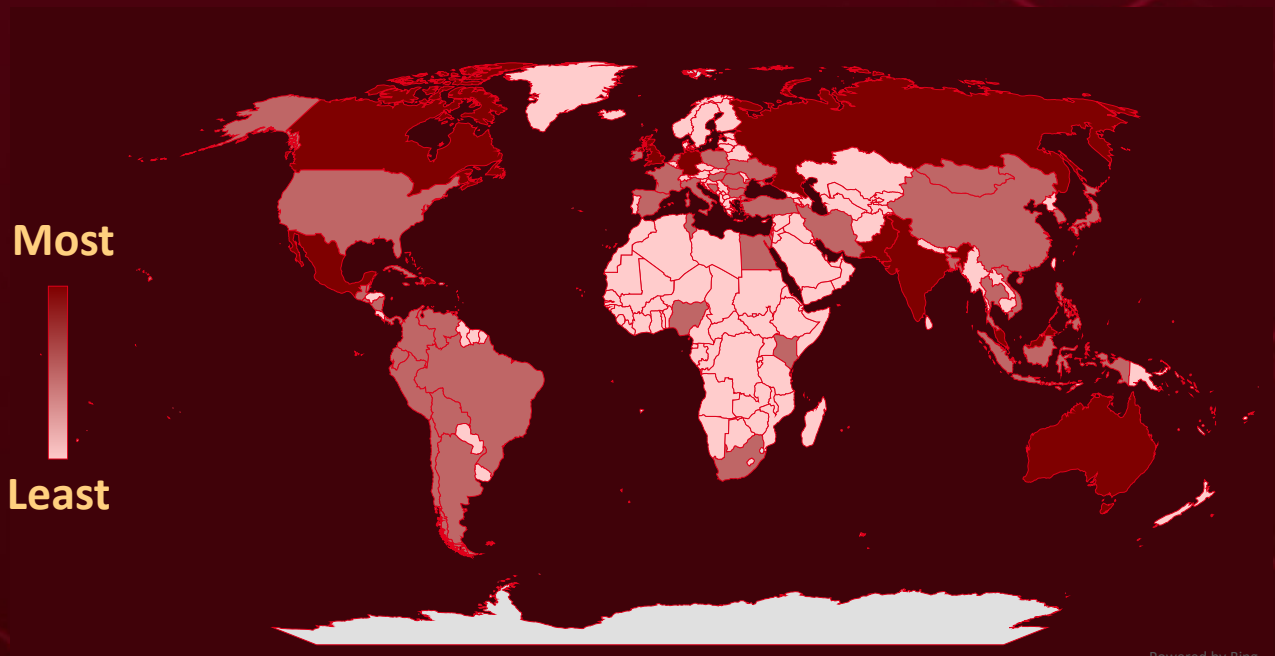
Pakistan-linked operators are running parallel espionage campaigns, **Gopher Strike** and **Sheet Attack**, using fake document lures and cloud-based infrastructure to quietly infiltrate Indian government systems while evading detection.

TA584 keeps refining its phishing playbook, using ClickFix and fake CAPTCHA checks to quietly trick users into unleashing **Tsundere Bot** and **XWorm** infections.

Threat Distribution



Targeted Countries



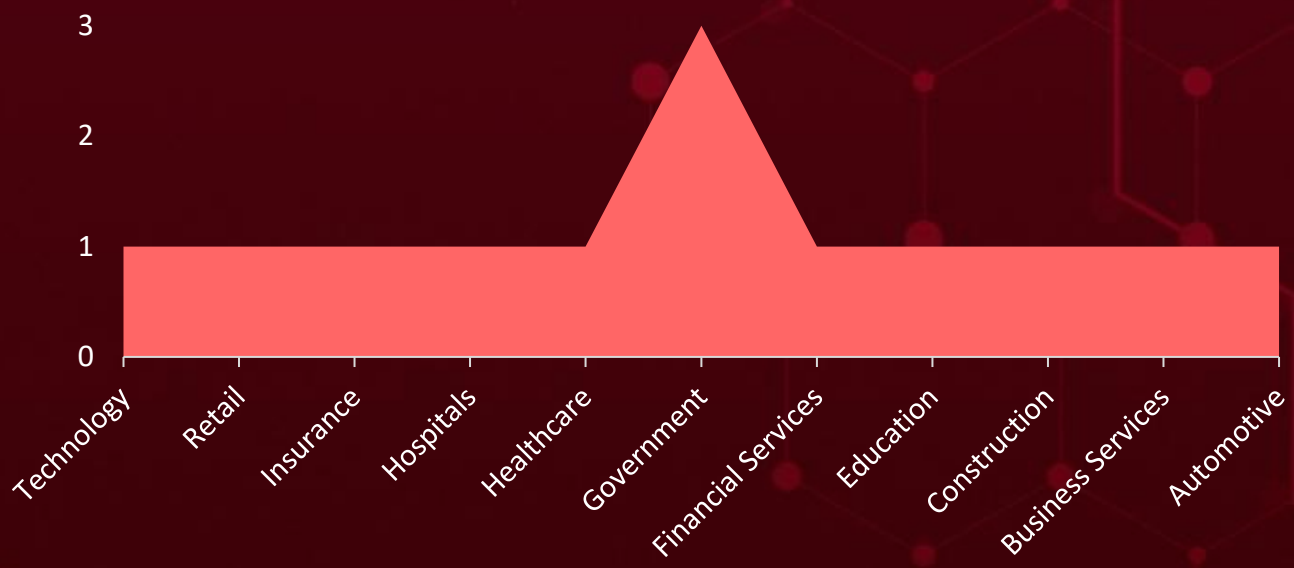
Countries
Mexico
India
Russia
Australia
Malaysia
Canada
Pakistan
Dominican Republic
Germany
United Kingdom
Netherlands
Thailand
Romania
Bulgaria
Vietnam
Argentina
Panama
Chile
Singapore
China
Brazil
Colombia
Belize
Cuba
Nigeria

Countries
South Korea
Egypt
Tunisia
El Salvador
Kenya
France
Barbados
Bahamas
Mongolia
Grenada
Nicaragua
Guatemala
Bolivia
Haiti
Peru
Hungary
Poland
Bangladesh
Bosnia and Herzegovina
Indonesia
Saint Lucia
Ukraine
South Africa
United States
Spain

Countries
Italy
Turkey
Jamaica
Japan
Iran
Ireland
Venezuela
Uganda
Saudi Arabia
Paraguay
Georgia
Suriname
Azerbaijan
North Macedonia
Ghana
Rwanda
Greece
Solomon Islands
Brunei
Timor-Leste
Grenadines
Gambia
Angola
Palau
Guinea

Countries
Cambodia
Djibouti
Cameroon
Bhutan
Iraq
San Marino
Bahrain
Serbia
Central African Republic
Slovakia
Chad
Austria
Albania
Sri Lanka
Algeria
Switzerland
Jordan
Tanzania
Kazakhstan
Tonga
Belarus
Turkmenistan
Kiribati
United Arab Emirates

Targeted Industries



TOP MITRE ATT&CK TTPs

T1059 Command and Scripting Interpreter	**T1588** Obtain Capabilities	**T1071.001** Web Protocols	**T1071** Application Layer Protocol	**T1082** System Information Discovery
T1566 Phishing	**T1562** Impair Defenses	**T1588.005** Exploits	**T1027** Obfuscated Files or Information	**T1562.001** Disable or Modify Tools
T1588.006 Vulnerabilities	**T1059.001** PowerShell	**T1190** Exploit Public-Facing Application	**T1055** Process Injection	**T1005** Data from Local System
T1204 User Execution	**T1547.001** Registry Run Keys / Startup Folder	**T1583.001** Domains	**T1564** Hide Artifacts	**T1053** Scheduled Task/Job

Attacks Executed

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
GOGITTER	GOGITTER is a newly identified, downloader developed in Golang that retrieves malicious payloads from a private GitHub repository controlled by threat actors. Designed as a 64-bit executable, the malware operates quietly on infected systems, first checking for the presence of a VBScript file named windows_api.vbs across specific system locations before proceeding with its operations.	Phishing	-
		IMPACT	AFFECTED PLATFORM
TYPE		Downloads additional payloads	Windows
Downloader			PATCH LINK
ASSOCIATED ACTOR			-
-			
IOC TYPE	VALUE		
URL	hxxps[:]//d2i8rh3pkr4ltc[.]cloudfront[.]net/adobe_installation[.]php?file=Adobe_Acrobat_Reader_Installation_Setup		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
GITSHELLPAD	GITSHELLPAD is a newly discovered backdoor developed in Golang that uses private GitHub repositories as its command-and-control (C2) channel, allowing attackers to blend malicious traffic with legitimate GitHub activity. Once deployed, the malware registers the compromised system with the operator's infrastructure and continuously polls the repository for instructions, enabling remote command execution and ongoing control over the victim machine. To manage infected hosts, the backdoor leverages GitHub's REST API to automatically create uniquely named directories within an attacker-controlled repository, effectively organizing victims and facilitating discreet command exchange through a trusted platform.	Phishing	-
		IMPACT	AFFECTED PLATFORM
TYPE		System Compromise	Windows
Backdoor			PATCH LINK
ASSOCIATED ACTOR			-
-			
IOC TYPE	VALUE		
SHA256	8f495603be80b513820a948d51723b616fac33f0f382fa4a141e39e12fff40cf		

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
GOSHELL	GOSHELL is a Golang-based shellcode loader designed to deploy a Cobalt Strike Beacon on targeted systems whose hostnames are hardcoded within the malware, ensuring execution only on selected machines. The loader retrieves payloads packaged in RAR archives, extracts them using system utilities such as tar, and removes the tools afterward to minimize forensic traces, while the primary deployed component functions as the main backdoor for continued access.	Phishing	-
		IMPACT	AFFECTED PLATFORM
TYPE		Loads additional payloads	Windows
Loader			
ASSOCIATED ACTOR			PATCH LINK
-			-
IOC TYPE	VALUE		
SHA256	a83d833f0c8dc0f7eaad65d93d7f3da2d905d83f9eefd420af8939b2e0e921a3		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
SHEETCREEP	SHEETCREEP is a lightweight C#-based backdoor that abuses Google Sheets as its command-and-control (C2) channel, allowing attackers to discreetly send commands and receive data through a trusted cloud service. The malware is typically delivered in a ZIP archive containing a malicious shortcut (LNK) file and a payload disguised as a PNG image, tricking users into executing the file while concealing its true purpose. Once triggered, the backdoor establishes communication with attacker-controlled resources via Google Sheets, enabling remote command execution and persistent access while blending malicious activity with legitimate network traffic.	Phishing	-
		IMPACT	AFFECTED PLATFORM
TYPE		System Compromise	Windows
Backdoor			
ASSOCIATED ACTOR			PATCH LINK
-			-
IOC TYPE	VALUE		
SHA256	b56062033df06738b66c38b3fa2f82a7e8c558336a4790c83c7faad595172167, 71794df37a107472e8d0829387741953f9e6c7778519b11f061c79ff6fb0f386		

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
FIREPOWER	FIREPOWER is a PowerShell-based backdoor, designed to provide attackers with persistent remote access to compromised systems. Once executed, the malware generates a unique victim identifier using the format ComputerName==Username, allowing operators to track infected hosts, and then establishes communication with a Firebase Realtime Database used as its command-and-control channel. Through this setup, attackers can remotely issue commands, manage infected machines, and maintain ongoing control while blending malicious traffic with legitimate cloud service communications.	Phishing	-
		IMPACT	AFFECTED PLATFORM
TYPE		Execute commands, System compromise	Windows
Backdoor			
ASSOCIATED ACTOR			PATCH LINK
-			-
IOC TYPE	VALUE		
SHA256	889b4b1e13b66aff349282eae3999783f5542f961b433a7d4653c5281e7f4d3e, 20d72c8580b4d5ef4f771c91ce1d1207e5416fa789d8216a73a0abb8e030644f		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
MAILCREEP	MAILCREEP is a Golang-based backdoor that abuses the Microsoft Graph API to establish its command-and-control (C2) channel, allowing attackers to communicate with compromised systems through legitimate Microsoft cloud services.	Phishing	-
		IMPACT	AFFECTED PLATFORM
TYPE		System Compromise	Windows
Backdoor			
ASSOCIATED ACTOR			PATCH LINK
-			-
IOC TYPE	VALUE		
SHA256	a97cc81a2f7c05bfc498b71999176c2aeb6e3ad273e48eb1f5c1c5647419c642		

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
CoolClient	CoolClient is a backdoor commonly delivered with encrypted loader components containing configuration data, shellcode, and in-memory DLL modules executed through DLL sideloading using legitimate signed applications. Once deployed, it collects key system and user information such as host details, operating system version, memory size, network identifiers, user accounts, and loaded driver data to profile the compromised environment. Both older and newer variants support functions including file upload and deletion, keylogging, TCP tunneling, reverse proxy capabilities, and in-memory plugin execution for further payload delivery. The latest version adds clipboard monitoring to capture copied data and introduces the ability to extract HTTP proxy credentials from network traffic, while primarily using TCP for command-and-control communications with optional UDP support for flexibility.		-
		IMPACT	AFFECTED PRODUCTS
TYPE		Steal Data, System Compromise	Microsoft Windows
Backdoor			
ASSOCIATED ACTOR			PATCH LINK
Mustang Panda			-
IOC TYPE	VALUE		
SHA256	FD434AC879122DEDB754BD4835822DBC185ACE3A3E75E5898FFB40C213A7C4BA		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
Tsundere Bot	Tsundere Bot is a newly identified malware family that combines loader and backdoor capabilities, enabling attackers to deploy additional payloads while maintaining remote access to compromised systems. Analysis of its infrastructure revealed control panels labeled “Tsundere Netto” and “Tsundere Reborn,” from which the malware derives its name. The bot requires Node.js to operate on infected machines, with installers generated directly from the command-and-control panel and delivered as MSI packages or PowerShell scripts.	Social Engineering	-
		IMPACT	AFFECTED PLATFORM
TYPE		Steal Data, Execute Script	Windows
Bot			
ASSOCIATED ACTOR			PATCH LINK
TA584			-
IOC TYPE	VALUE		
IPv4	85[.]236[.]25[.]119		

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

<table>
<tr><th>NAME</th><th>OVERVIEW</th><th>DELIVERY METHOD</th><th>TARGETED CVE</th></tr>
<tr><td rowspan="2">XWorm</td><td rowspan="5">XWorm is a remote access trojan (RAT) active since 2022 that provides attackers with extensive remote control over compromised systems while also incorporating limited ransomware capabilities. Sold on underground forums and widely adopted by threat actors with varying skill levels, the malware is frequently used in opportunistic campaigns to steal data and maintain persistent access across infected environments.</td><td>Social Engineering</td><td>-</td></tr>
<tr><td rowspan="2">TYPE</td><td>IMPACT</td><td>AFFECTED PLATFORM</td></tr>
<tr><td rowspan="3">Remote Control</td><td rowspan="2">Windows</td></tr>
<tr><td>RAT</td></tr>
<tr><td>ASSOCIATED ACTOR</td><td>PATCH LINK</td></tr>
<tr><td>TA584</td><td>-</td></tr>
<tr><td>IOC TYPE</td><td colspan="3">VALUE</td></tr>
<tr><td>IPv4</td><td colspan="3">80[.]64[.]19[.]148,
85[.]208[.]84[.]208</td></tr>
<tr><td>SHA256</td><td colspan="3">bbedc389af45853493c95011d9857f47241a36f7f159305b097089866502ac99</td></tr>
</table>

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
CVE-2026-21509		Microsoft Office 2016, Microsoft Office 2019, Microsoft Office LTSC 2021, Microsoft Office LTSC 2024, Microsoft 365 Apps for Enterprise	-
	ZERO-DAY		
		**AFFECTED CPE**	**ASSOCIATED ATTACKS/RANSOMWARE**
NAME	**CISA KEV**	cpe:2.3:a:microsoft:office:*:*:*:*:*:*:*:*	-
Microsoft Office Security Feature Bypass Vulnerability			
	CWE ID	**ASSOCIATED TTPs**	**PATCH LINK**
	CWE-807	T1566: Phishing, T1204: User Execution, T1559: Inter-Process Communication, T1562: Impair Defenses	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-21509

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
CVE-2026-24061	✗ ZERO-DAY	GNU InetUtils telnetd versions 1.9.3 - 2.7	-
	✗	**AFFECTED CPE**	**ASSOCIATED ATTACKS/RANSOMWARE**
NAME	**CISA KEV**	cpe:2.3:a:gnu:inetutils:*:*:*:*:*:*:*:*	-
GNU InetUtils Argument Injection Vulnerability	✓		
	CWE ID	**ASSOCIATED TTPs**	**PATCH LINK**
	CWE-88	T1190: Exploit Public-Facing Application, T1068: Exploitation for Privilege Escalation, T1059: Command and Scripting Interpreter, T1098: Account Manipulation, T1082: System Information Discovery	https://codeberg.org/inetutils/inetutils/commit/fd702c02497b2f398e739e3119bed0b23dd7aa7b , https://codeberg.org/inetutils/inetutils/commit/ccba9f748aa8d50a38d7748e2e60362edd6a32cc , https://cgit.git.savannah.gnu.org/cgit/inetutils.git

<table>
<tr><th>CVE ID</th><th>CELEBRITY VULNERABILITY</th><th>AFFECTED PRODUCT</th><th>ASSOCIATED ACTORS</th></tr>
<tr><td rowspan="3">CVE-2026-24858</td><td>  </td><td rowspan="2">Fortinet FortiOS (Before 7.0.19, 7.2.13, 7.4.11, 7.6.6) Fortinet FortiManager (Before 7.0.16, 7.2.13, 7.4.10, 7.6.6) Fortinet FortiAnalyzer (Before 7.0.16, 7.2.12, 7.4.10, 7.6.6) Fortinet FortiProxy (7.0, 7.2, Before 7.4.13, 7.6.6)</td><td rowspan="2">-</td></tr>
<tr><td>ZERO-DAY</td></tr>
<tr><td>  </td><td>AFFECTED CPE</td><td>ASSOCIATED ATTACKS/RANSOMWARE</td></tr>
<tr><td>NAME</td><td>CISA KEV</td><td rowspan="2">cpe:2.3:o:fortinet:fortios:*:*:*:*:*:*:*:*
cpe:2.3:a:fortinet:fortimanager:*:*:*:*:*:*:*:*:*
cpe:2.3:a:fortinet:fortianalyzer:*:*:*:*:*:*:*:*:*
cpe:2.3:a:fortinet:fortiproxy:*:*:*:*:*:*:*:*:*</td><td rowspan="2">-</td></tr>
<tr><td rowspan="2">Fortinet Multiple Products Authentication Bypass Using an Alternate Path or Channel Vulnerability</td><td>  </td></tr>
<tr><td>CWE ID</td><td>ASSOCIATED TTPs</td><td>PATCH LINK</td></tr>
<tr><td>CWE-288</td><td>T1190: Exploit Public-Facing Application, T1059: Command and Scripting Interpreter, T1136: Create Account, T1005: Data from Local System</td><td>https://fortiguard.fortinet.com/psirt/FG-IR-26-060 , https://docs.fortinet.com/upgrade-tool/fortigate</td></tr>
</table>

<table>
<tr><th>CVE ID</th><th>CELEBRITY VULNERABILITY</th><th>AFFECTED PRODUCT</th><th>ASSOCIATED ACTORS</th></tr>
<tr><td rowspan="3">CVE-2026-1281</td><td>✗</td><td rowspan="2">Ivanti EPMM Versions 12.5.0.0 and prior, 12.6.0.0 and prior, 12.7.0.0 and prior, 12.5.1.0 and prior, 12.6.1.0 and prior</td><td rowspan="2">-</td></tr>
<tr><td>ZERO-DAY</td></tr>
<tr><td>✓</td><td>AFFECTED CPE</td><td>ASSOCIATED ATTACKS/RANSOMWARE</td></tr>
<tr><td>NAME</td><td>CISA KEV</td><td rowspan="2">cpe:2.3:a:ivanti:endpoint_manager_mobile:12.5.0.0:*:*:*:*:*:*:*
cpe:2.3:a:ivanti:endpoint_manager_mobile:12.6.0.0:*:*:*:*:*:*:*
cpe:2.3:a:ivanti:endpoint_manager_mobile:12.7.0.0:*:*:*:*:*:*:*
cpe:2.3:a:ivanti:endpoint_manager_mobile:12.5.1.0:*:*:*:*:*:*:*
cpe:2.3:a:ivanti:endpoint_manager_mobile:12.6.1.0:*:*:*:*:*:*:*</td><td>-</td></tr>
<tr><td>Ivanti Endpoint Manager Mobile (EPMM) Code Injection Vulnerability</td><td>✓</td><td></td></tr>
<tr><td></td><td>CWE ID</td><td>ASSOCIATED TTPs</td><td>PATCH LINK</td></tr>
<tr><td></td><td>CWE-94</td><td>T1190: Exploit Public-Facing Application, T1059: Command and Scripting Interpreter</td><td>https://forums.ivanti.com/s/article/Security-Advisory-Ivanti-Endpoint-Manager-Mobile-EPMM-CVE-2026-1281-CVE-2026-1340?language=en_US</td></tr>
</table>

<table>
<tr><th>CVE ID</th><th>CELEBRITY VULNERABILITY</th><th>AFFECTED PRODUCT</th><th>ASSOCIATED ACTORS</th></tr>
<tr><td rowspan="3">CVE-2026-1340</td><td>✗</td><td rowspan="2">Ivanti EPMM Versions 12.5.0.0 and prior, 12.6.0.0 and prior, 12.7.0.0 and prior, 12.5.1.0 and prior, 12.6.1.0 and prior</td><td rowspan="2">-</td></tr>
<tr><td>ZERO-DAY</td></tr>
<tr><td>✓</td><td>AFFECTED CPE</td><td>ASSOCIATED ATTACKS/RANSOMWARE</td></tr>
<tr><td>NAME</td><td>CISA KEV</td><td rowspan="2">cpe:2.3:a:ivanti:endpoint_manager_mobile:12.5.0.0:*:*:*:*:*:*:*
cpe:2.3:a:ivanti:endpoint_manager_mobile:12.6.0.0:*:*:*:*:*:*:*
cpe:2.3:a:ivanti:endpoint_manager_mobile:12.7.0.0:*:*:*:*:*:*:*
cpe:2.3:a:ivanti:endpoint_manager_mobile:12.5.1.0:*:*:*:*:*:*:*
cpe:2.3:a:ivanti:endpoint_manager_mobile:12.6.1.0:*:*:*:*:*:*:*</td><td rowspan="2">-</td></tr>
<tr><td rowspan="2">Ivanti Endpoint Manager Mobile (EPMM) Code Injection Vulnerability</td><td>✗</td></tr>
<tr><td>CWE ID</td><td>ASSOCIATED TTPs</td><td>PATCH LINK</td></tr>
<tr><td>CWE-94</td><td>T1190: Exploit Public-Facing Application, T1059: Command and Scripting Interpreter</td><td>https://forums.ivanti.com/s/article/Security-Advisory-Ivanti-Endpoint-Manager-Mobile-EPMM-CVE-2026-1281-CVE-2026-1340?language=en_US</td></tr>
</table>

Adversaries in Action

<table>
<tr><th>NAME</th><th>ORIGIN</th><th>TARGETED INDUSTRIES</th><th>TARGETED REGIONS</th></tr>
<tr><td rowspan="4"> 

Mustang Panda (aka HoneyMyte, Bronze President, TEMP.Hex, Red Lich, Earth Preta, Camaro Dragon, PKPLUG, Stately Taurus, Twill Typhoon, Hive0154)</td><td>China</td><td rowspan="2">Government</td><td rowspan="2">Myanmar, Mongolia, Malaysia, Russia, Pakistan</td></tr>
<tr><td>MOTIVE</td></tr>
<tr><td>Information theft and espionage</td><td>ASSOCIATED ATTACKS/RANSOM WARE</td><td>AFFECTED PRODUCT</td></tr>
<tr><td>TARGETED CVE</td><td>-</td><td>CoolClient</td><td>Microsoft Windows</td></tr>
<tr><td colspan="4">TTPs</td></tr>
<tr><td colspan="4">TA0002: Execution; TA0003: Persistence; TA0004: Privilege Escalation; TA0005: Defense Evasion; TA0006: Credential Access; TA0007: Discovery; TA0009: Collection; TA0010: Exfiltration; TA0011: Command and Control; TA0040: Impact; T1059: Command and Scripting Interpreter; T1059.001: PowerShell; T1059.003: Windows Command Shell; T1547: Boot or Logon Autostart Execution; T1547.001: Registry Run Keys / Startup Folder; T1053: Scheduled Task/Job; T1053.005: Scheduled Task; T1543: Create or Modify System Process; T1543.003: Windows Service; T1548: Abuse Elevation Control Mechanism; T1548.002: Bypass User Account Control; T1574: Hijack Execution Flow; T1574.001: DLL; T1055: Process Injection; T1140: Deobfuscate/Decode Files or Information; T1555: Credentials from Password Stores; T1555.003: Credentials from Web Browsers; T1056: Input Capture; T1056.001: Keylogging; T1082: System Information Discovery; T1016: System Network Configuration Discovery; T1083: File and Directory Discovery; T1115: Clipboard Data; T1005: Data from Local System; T1560: Archive Collected Data; T1071: Application Layer Protocol; T1071.001: Web Protocols; T1041: Exfiltration Over C2 Channel; T1567: Exfiltration Over Web Service; T1090: Proxy; T1070: Indicator Removal; T1070.004: File Deletion; T1027: Obfuscated Files or Information; T1569: System Services; T1489: Service Stop</td></tr>
</table>

<table>
<tr><th>NAME</th><th>ORIGIN</th><th>TARGETED INDUSTRIES</th><th>TARGETED REGIONS</th></tr>
<tr><td rowspan="4"> 
TA584</td><td>-</td><td rowspan="3">Healthcare, Government, Financial Services, Education, Business Services, Hospitals, Technology, Retail, Insurance, Construction, Automotive</td><td rowspan="3">Antigua and Barbuda, Bahamas, Barbados, Belize, Canada, Costa Rica, Cuba, Dominica, Dominican Republic, El Salvador, Grenada, Guatemala, Haiti, Honduras, Jamaica, Mexico, Nicaragua, Panama, Saint Kitts and Nevis, Saint Lucia, Saint Vincent and the Grenadines, Trinidad and Tobago, United States, United Kingdom, Ireland, Germany, Australia</td></tr>
<tr><th>MOTIVE</th></tr>
<tr><td>Information theft and espionage</td></tr>
<tr><th>TARGETED CVE</th><th>ASSOCIATED ATTACKS/RANSOMWARE</th><th>AFFECTED PRODUCT</th></tr>
<tr><td>-</td><td>Tsundere Bot, XWorm</td><td>Windows</td></tr>
<tr><th colspan="4">TTPs</th></tr>
<tr><td colspan="4">TA0001: Initial Access; TA0002: Execution; TA0003: Persistence; TA0005: Defense Evasion; TA0007: Discovery; TA0011: Command and Control; TA0042: Resource Development; T1566: Phishing; T1566.002: Spearphishing Link; T1078: Valid Accounts; T1078.004: Cloud Accounts; T1059: Command and Scripting Interpreter; T1059.001: PowerShell; T1204: User Execution; T1204.001: Malicious Link; T1547: Boot or Logon Autostart Execution; T1547.001: Registry Run Keys / Startup Folder; T1027: Obfuscated Files or Information; T1027.010: Command Obfuscation; T1055: Process Injection; T1055.012: Process Hollowing; T1562: Impair Defenses; T1562.001: Disable or Modify Tools; T1564: Hide Artifacts; T1564.001: Hidden Files and Directories Discovery; T1082: System Information Discovery; T1071: Application Layer Protocol; T1071.001: Web Protocols; T1102: Web Service; T1102.002: Bidirectional Communication; T1583: Acquire Infrastructure; T1583.001: Domains; T1584: Compromise Infrastructure; T1584.003: Virtual Private Server</td></tr>
</table>

Recommendations

Security Teams

This digest can be utilized as a drive to force security teams to prioritize the **five exploitable vulnerabilities** and block the indicators related to the threat actor **Mustang Panda, TA584,** and malware **GOGITTER, GITSHELLPAD, GOSHELL, SHEETCREEP, FIREPOWER, MAILCREEP, CoolClient, Tsundere Bot,** and **Xworm.**

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 **five exploitable vulnerabilities.**
- Testing the efficacy of their security controls by simulating the attacks related to the threat actors **Mustang Panda, TA584,** and malware **SHEETCREEP, MAILCREEP, CoolClient,** and **XWorm** in Breach and Attack Simulation(BAS).

Threat Advisories

CVE-2026-21509: Microsoft Office Zero-Day Under Active Exploitation

January 2026 Linux Patch Roundup

Instant Root Access via CVE-2026-24061: A Decade-Old Bug Comes Alive

Gopher Strike and Sheet Attack Campaigns Targeting Indian Government

CVE-2026-24858: Critical FortiCloud SSO Zero-day Under Active Exploitation

Mustang Panda Enhances CoolClient for Stealth and Surveillance

TA584 and the Business of Breach: Selling Access at Scale

Ivanti Patches Actively Exploited EPMM Flaws

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
GOGITTER	URLs	hxxps[:]//d2i8rh3pkr4ltc[.]cloudfront[.]net/adobe_installation[.]php?file=Adobe_Acrobat_Reader_Installation_Setup, hxxps[:]//adobereader-upgrade[.]in/adobe_update[.]php?file=Adobe_Acrobat_Reader_Installation, hxxps[:]//adobecloud[.]site/adobe_installer[.]php?file=Adobe_Acrobat_Installer, hxxps[:]//adobe-acrobat[.]in/adobe_reader_setup[.]php?file=Adobe_Acrobat_Reader_Installation_Setup
GITSHELLPAD	MD5	0d86b8039cffc384856e17912f308616, f454e2724a63cbbfda26daff1d8bb610, 10a7725f807056cb0383a1cae38d49b4, e26b3fece2fe296654406ef8045ffda1, f4813d65cd7246f716fcbd8f7fd3e63d, f2284f62625f117c57384b1c5b8b8f58
	SHA1	6a11c0e5f1d1e22e89b4921c7a371dbf9cf54709, 6036098059fa1311866ce6ad2723c4d0d1f00138, 54bfe1ffba8bff3571093ade5038dc98ef5f46ce, 6d1dbd92f7ed7381c7bfca681c3139daeab692f1, 3d48ab9567c6080471459b34dfc12c89418be8a2, 3c17dbf975af8eb7a67e6908f522c93c2c0662e5

Attack Name	TYPE	VALUE
GITSHELLPAD	SHA256	8f495603be80b513820a948d51723b616fac33f0f382fa4a141e39e12fff40cf, 6c60e5b28e352375d101eb0954fa98d229de3b94f22d5815af8948ebed1f44dd, af01c12019a3a3aa64e8a99d7231e0f2af6084298733bba3d7d41db13091cbac, 5d9b2e61ed45b6407b778a18ff87792265fa068d7c4580ae54fbf88af435679f, 95a2fb8b6c7b74a7f598819810ddb0a505f3d5cf392b857ff8e75c5a1401110e, fff79ce90b1af67e0b6d16a850e85861c948f988eda39ef46457241bbe3df170
GOSHELL	SHA256	a83d833f0c8dc0f7eaad65d93d7f3da2d905d83f9eefd420af8939b2e0e921a3
SHEETCREEP	MD5	87c7d69c6131406afdd0a08e89329d0a, 0729db72ab4ad9b2ac7a82918c744388, f9a2da8f12179414663a230f11edca20, 556a567a2c5c27a6aa5660e2e6bcce7b
	SHA1	a55c18a82203cf1efafac6f3c47642ab60c74ffc, daeeb031a9617e6f1b7bf4d85de9c75f62021c82, cdecfe8e1cacd1af204a5da52f6c02eb16fdea8b, e9d9d8c0c818ba9208e61eaf49af4c1b37f4eb59
	SHA256	b56062033df06738b66c38b3fa2f82a7e8c558336a4790c83c7faad595172167, 71794df37a107472e8d0829387741953f9e6c7778519b11f061c79ff6fb0f386, 9eebbf8899a1cf4156a872e9b8cde2a8f6ab364b8089550510938405c622cc58, bb11bea463ab1b976c3716591f93eccc71c1a2d1c389a371416b140cd8faa6f0
FIREPOWER	MD5	12669c29e00057abf20c73a434eb3dd2, cd5aab2b0f8d2b42e7a6537303d6345d, 0f7730a78490c61964b3bfc05eb59ea7, 119b836b4e1e7be8c3be8fe921f72bfb, 41a3752e6ea83d25731f22e1c17f59e2, 12669c29e00057abf20c73a434eb3dd2, e48f1000c86b93cf428a13a0b7384e0d
	SHA1	a38eab1ac01201b651b2efdebc78e994402976f1, e9eeda092500d7c7f278672d35f733e0e26f0e2c, ac06003a774af5a8e4be349fc6f0e65cea116370, e333ae0948ede0cf1368deec53a1eda18210e75e, aa9b4410004d43e4e5cc1fc2cda1956bc5663b03, a38eab1ac01201b651b2efdebc78e994402976f1, 8f9843607ff0ed83ca58e21612b41d6e744beb81

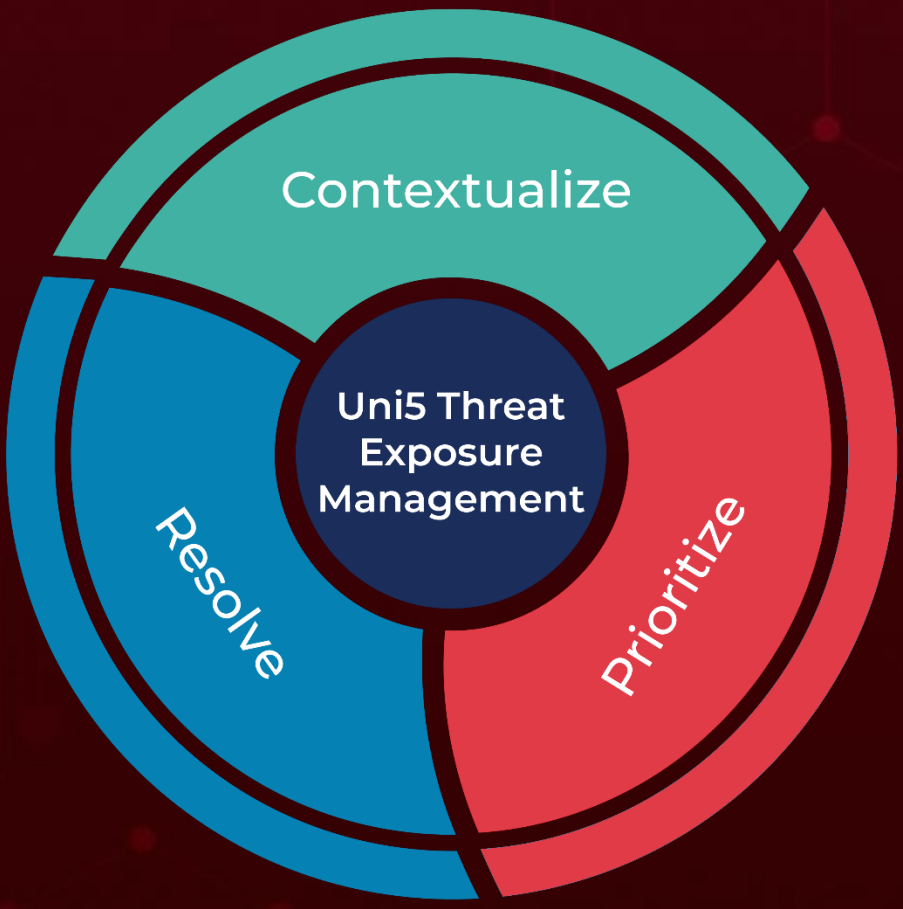
Attack Name	TYPE	VALUE
FIREPOWER	SHA256	889b4b1e13b66aff349282eae3999783f5542f961b433a7d4653c5281e7f4d3e, 20d72c8580b4d5ef4f771c91ce1d1207e5416fa789d8216a73a0abb8e030644f, de14ca6d93dadbc1ec216700d76ad2d0e7b9ebceb95de68c631d0a1c01c915c4, 644dda0ea5db1eb5f07ccfccddb909c6ee57235c4465adbfc342da6867cdb71a, 309a39ba10cd7c7075837b63d247fa45764f5496fdae215e95a3f4b65ab6dfc3, 889b4b1e13b66aff349282eae3999783f5542f961b433a7d4653c5281e7f4d3e, 989ad43bb9e328d786664247c3af4c17be28932760113708a9c6de977d69652c
	URLs	hxxps[:]//webdevurl-cc389-default-rtdb[.]firebaseio[.]com, hxxps[:]//govs-services-in-default-rtdb[.]firebaseio[.]com, hxxps[:]//gov-service-in-default-rtdb[.]firebaseio[.]com
MAILCREEP	MD5	ed4dd29c57a38f2bb1934acbaeadeeba
	SHA1	7bc5d288ec260765a146136194d815ff3c697df8
	SHA256	a97cc81a2f7c05bfc498b71999176c2aeb6e3ad273e48eb1f5c1c5647419c642
CoolClient	MD5	F518D8E5FE70D9090F6280C68A95998F, 1A61564841BBBB8E7774CBBEB3C68D5D, AEB25C9A286EE4C25CA55B72A42EFA2C, 6B7300A8B3F4AAC40EEECFD7BC47EE7C
	SHA256	FD434AC879122DEDB754BD4835822DBC185ACE3A3E75E5898FFB40C213A7C4BA, 941993f885957176d75f24ef3f8935ecb589bb9b445bb0d71fb18b65e61b6ee4
	Domains	account[.]hamsterxnxx[.]com, popnike-share[.]com, japan[.]Lenovoappstore[.]com
Tsundere Bot	IPv4	85[.]236[.]25[.]119
XWorm	SHA256	bbedc389af45853493c95011d9857f47241a36f7f159305b097089866502ac99, 441c49b6338ba25519fc2cf1f5cb31ba51b0ab919c463671ab5c7f34c5ce2d30
	IPv4	80[.]64[.]19[.]148, 85[.]208[.]84[.]208, 178[.]16[.]52[.]242, 94[.]159[.]113[.]64

A comprehensive list of IOCs (Indicators of Compromise) associated with the executed attacks is available on the Uni5Xposure platform.

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

February 2, 2026 • 8:00 AM

More at www.hivepro.com