loginsoft

Monthly Report

Threat & Vulnerabilities Report – June 2026

Executive Summary

As June 2026 unfolded, the cybersecurity landscape faced an unprecedented convergence of vulnerability disclosures, active exploitation campaigns, and ransomware operations. The month emerged as one of the most consequential in recent threat history, marked by relentless attacks across every sector and platform. June 2026 delivered a relentless barrage of vulnerabilities and active exploitation.

CISA's Known Exploited Vulnerabilities catalog swelled with 23 critical entries, showcasing a diversified attack surface spanning Ubiquiti and Cisco (3 each), Oracle (2), plus critical exposures from Google, SimpleHelp, Android, Linux, Check Point, SolarWinds, and Ivanti. This wasn't a concentrated problem- it was systemic.

What made the month particularly dangerous was the velocity of active exploitation: attackers weaponized vulnerabilities within hours. WordPress plugins, Langflow, Fortinet security appliances, Microsoft systems, Oracle infrastructure, and network edge devices from AVTECH and D-Link all faced active exploitation campaigns simultaneously, demonstrating adversaries operating at industrial scale.

The ransomware ecosystem revealed a clear hierarchy of destruction. Qilin and TheGentlemen emerged as co-leaders, each claiming 76 affected organizations in June - a striking parity suggesting systematic, industrialized attacks. LockBit5 followed with 43 compromised organizations, maintaining its position despite law enforcement pressure, while Akira and IncRansom rounded out the top five with 28 and 27 organizations respectively. These weren't isolated incidents; they represented proven business models executed with mechanical precision across enterprises worldwide.

Vulnerabilities added to the CISA KEV catalog in June 2026

CVE-ID	Vendor	Product	Description	Exploited as zero-day	Abused by Malware	OSS
CVE-2026-7473	Arista	Extensible Operating System	Incomplete Comparison with Missing Factors vulnerability in Arista Extensible Operating System when the switch incorrectly decapsulate and forwards other unexpected tunneled packet with a destination IP matching its configured decapsulation IP.	No	No	False
CVE-2026-10520	Ivanti	Sentry	OS Command Injection vulnerability in Ivanti Sentry which could allow a remote unauthenticated user to	No	No	False

CVE-ID	Vendor	Product	Description	Exploited as zero-day	Abused by Malware	OSS
			achieve root-level remote code execution.			
CVE-2026-11645	Google	Chromium V8	Out-of-Bounds Read and Write vulnerability in Google Chromium that could allow a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page.	Yes	No	False
CVE-2026-12569	PTC	Windchill and FlexPLM	Improper Input Validation vulnerability in PTC Windchill and FlexPLM allowing an unauthenticated, remote attacker to execute arbitrary code by sending a malicious request to the network.	No	No	False
CVE-2026-20230	Cisco	Unified Communications Manager	Server-Side Request Forgery (SSRF) Vulnerability in Cisco Unified Communications Manager (Unified CM) and Cisco Unified Communications Manager Session Management Edition (Unified CM SME) that could allow an unauthenticated, remote attacker to write files to the underlying operating system that could be used later to elevate to root.	No	No	False
CVE-2026-20245	Cisco	Catalyst SD-WAN Manager	Improper Encoding or Escaping of Output vulnerability in Cisco Catalyst SD-WAN Manager that could allow an authenticated, local attacker to execute arbitrary commands as root by supplying a crafted file to the affected system.	Yes	No	False
CVE-2026-20253	Splunk	Enterprise	Missing Authentication for Critical Function vulnerability in Splunk Enterprise which could allow an unauthenticated user to create or truncate arbitrary files through a PostgreSQL sidecar service endpoint.	No	No	False
CVE-2026-20262	Cisco	Catalyst SD-WAN Manager	Directory or Path Traversal vulnerability in Cisco	Yes	No	False

CVE-ID	Vendor	Product	Description	Exploited as zero-day	Abused by Malware	OSS
			Catalyst SD-WAN Manager that could allow an authenticated, remote attacker to create a file or overwrite any file on the filesystem of an affected system.			
CVE-2026-28318	SolarWinds	Serv-U	Uncontrolled Resource Consumption vulnerability in SolarWinds Serv-U that allows specially crafted POST requests using the Content-Encoding: deflate header to crash the Serv-U service without authentication.	No	No	False
CVE-2026-34908	Ubiquiti	UniFi OS	An Improper Access Control vulnerability in Ubiquiti UniFi that could allow a malicious actor with access to the network to make unauthorized changes to the system.	No	Yes	False
CVE-2026-34909	Ubiquiti	UniFi OS	Path Traversal vulnerability in Ubiquiti UniFi that could allow a malicious actor with access to the network access files on the underlying system that could be manipulated to access an underlying account.	No	Yes	False
CVE-2026-34910	Ubiquiti	UniFi OS	Improper Input Validation vulnerability in Ubiquiti UniFi OS that could allow a malicious actor with access to the network to conduct command injection.	No	Yes	False
CVE-2026-35273	Oracle	PeopleSoft Enterprise PeopleTools	Missing Authentication for Critical Function vulnerability in Oracle PeopleSoft Enterprise PeopleTools which could allow an unauthenticated attacker to obtain takeover of PeopleSoft Enterprise PeopleTools.	Yes	Yes	False
CVE-2026-42271	BerriAi	LiteLLM	Command Injection Vulnerability in BerriAi LiteLLM that could allow any authenticated user, including holders of low-	No	No	True

CVE-ID	Vendor	Product	Description	Exploited as zero-day	Abused by Malware	OSS
			privilege internal-user keys, to run arbitrary commands on the host.			
CVE-2026-45247	Mirasvit	Mirasvit Full Page Cache Warmer	Deserialization of Untrusted Data vulnerability in Mirasvit Full Page Cache Warmer that could allow unauthenticated attackers to achieve remote code execution by supplying a crafted serialized PHP object in the CacheWarmer cookie.	No	No	False
CVE-2026-48558	SimpleHelp	SimpleHelp	Authentication Bypass vulnerability in SimpleHelp in the OIDC authentication flow that allows a remote unauthenticated attacker to submit a forged token containing arbitrary identity claims to obtain a fully authenticated technician session.	No	Yes	False
CVE-2026-48907	Widget Factory	Joomla Content Editor	Improper Access Control vulnerability in Widget Factory Joomla Content Editor which could allow for upload and execution of PHP code via the creation of new editor profiles for unauthenticated users.	No	No	False
CVE-2026-50751	Check Point	Security Gateway	Improper Authentication vulnerability in Check Point Security Gateway in IKEv1 key exchange that could allow an unauthenticated remote attacker to bypass user authentication and establish a remote access VPN connection without a valid user password.	Yes	Yes	False
CVE-2026-54420	LiteSpeed	cPanel Plugin	UNIX Symbolic Link (Symlink) Following vulnerability in LiteSpeed cPanel Plugin that could allow a user with FTP or web shell access on a shared hosting server running CloudLinux/CageFS.	Yes	No	False
CVE-2025-48595	Android	Framework	Integer Overflow vulnerability in Android Framework that allows for	Yes	No	True

CVE-ID	Vendor	Product	Description	Exploited as zero-day	Abused by Malware	OSS
			code execution that could allow for local privilege escalation.			
CVE-2025-67038	Lantronix	EDS5000	Code Injection vulnerability in Lantronix EDS5000 that could allow attackers to inject arbitrary OS commands into the username parameter.	No	No	False
CVE-2024-21182	Oracle	WebLogic Server	Improper Access Control vulnerability in Oracle WebLogic Server that could allow an unauthenticated attacker with network access via T3, IIOP to compromise Oracle WebLogic Server.	No	No	False
CVE-2022-0492	Linux	Kernel	Improper Authentication vulnerability in Linux Kernel which could allow for privilege escalation via the cgroups v1 ***release_agent*** feature.	No	No	True

Actively Exploited Vulnerabilities in June 2026

CVE-ID	Vendor	Product	Description	Exploited as Zero-day	Abused by Malware	OSS
CVE-2026-3300	WPEverest	Everest Forms Pro WordPress plugin	Remote Code Execution vulnerability in Everest Forms Pro WordPress plugin that can be leveraged by unauthenticated attackers to execute arbitrary PHP code on the server, leading to complete site compromise.	No	No	False
CVE-2026-4020	RocketGenius	Gravity SMTP WordPress plugin	Sensitive Information Disclosure vulnerability in Gravity SMTP WordPress plugin that exposes sensitive system data to unauthenticated attackers	No	No	False
CVE-2026-5027	Langflow	Langflow	A Path Traversal vulnerability in Langflow where the POST ***/api/v2/files*** endpoint	No	No	False

CVE-ID	Vendor	Product	Description	Exploited as Zero-day	Abused by Malware	OSS
			does not sanitize the filename parameter from the multipart form data, allowing an attacker to write files to arbitrary locations on the filesystem, potentially leading to remote code execution.			
CVE-2026-8206	Themeum	Kirki - Freeform Page Builder, Website Builder & Customizer plugin for WordPress	Unauthenticated Privilege Escalation vulnerability in Kirki WordPress plugin that makes it possible for unauthenticated attackers to send a password reset link for any user registered on the site to their own email address.	No	No	False
CVE-2026-10795	Team Updraft	UpdraftPlus: WP Backup & Migration Plugin	An Authentication Bypass vulnerability in the UpdraftPlus: WP Backup & Migration Plugin for WordPress arising from insufficient validation of the remote communications message format, where signature verification can be bypassed, allowing unauthenticated attackers to forge arbitrary RPC commands and ultimately achieve remote code execution.	No	No	False
CVE-2026-28496	FOSSBilling	FOSSBilling	Server-Side Template Injection vulnerability in FOSSBilling that enables attackers to inject arbitrary expressions that gain full access to the Twig environment, application API globals, and the underlying dependency injection (DI) container.	No	No	False
CVE-2026-35616	Fortinet	FortiClient EMS	Improper Access Control vulnerability in Fortinet FortiClient EMS that allows an unauthenticated attacker to execute unauthorized code or commands via crafted requests.	Yes	Yes	False

CVE-ID	Vendor	Product	Description	Exploited as Zero-day	Abused by Malware	OSS
CVE-2026-41089	Microsoft	Windows	Stack-Based Buffer Overflow vulnerability in Microsoft Windows Netlogon that allows an unauthorized attacker to execute code over a network.	No	No	False
CVE-2026-46817	Oracle	E-Business Suite	Missing Authentication for Critical Function vulnerability in Oracle E-Business Suite that could be abused to take over susceptible instances.	No	No	False
CVE-2026-48908	JoomShaper	SP Page Builder extension for Joomla	Unauthenticated Arbitrary File Upload vulnerability in SP Page Builder for Joomla that ultimately results in the upload and execution of PHP code.	No	No	False
CVE-2026-53435	Jenkins	Jenkins	Deserialization vulnerability in Jenkins core that allows attackers to have Jenkins deserialize arbitrary types from an attacker-controlled config.xml submission, enabling user impersonation, arbitrary file reads and remote code execution.	No	No	False
CVE-2025-1055	K7 Computing	K7 Security Anti-Malware	Missing Authorization vulnerability in K7RKScan.sys driver, part of the K7 Security Anti-Malware suite, allows a local low-privilege user to send crafted IOCTL requests to terminate a wide range of processes running with administrative or system-level privileges.	No	Yes	False
CVE-2025-8088	RARLAB	WinRAR	Path Traversal vulnerability in RARLAB WinRAR that could allow an attacker to execute arbitrary code by crafting malicious archive files.	No	Yes	False
CVE-2025-11371	Gladinet	CentreStack and Triofox	Files or Directories Accessible to External Parties vulnerability in Gladinet CentreStack and	No	Yes	False

CVE-ID	Vendor	Product	Description	Exploited as Zero-day	Abused by Malware	OSS
			Triofox that allows unintended disclosure of system files.			
CVE-2025-34054	AVTECH	DVR Devices	Unauthenticated Command Injection vulnerability in AVTECH DVR devices via Search.cgi?action=cgi_query, that allows attackers to inject shell commands through the username or queryb64str parameters, executing commands as root.	No	Yes	False
CVE-2025-61155	Hotta Studio	GameDriverX64.sys	An Access Control vulnerability in GameDriverX64.sys kernel-mode anti-cheat driver that resides in the IOCTL handler, allows a user-mode process to obtain a handle to the driver device and submit specially crafted IOCTL requests.	No	Yes	False
CVE-2023-52271	Topaz Evolution	Topaz Antifraud	Improper Access Control vulnerability in Kernel-Mode driver in Topaz Antifraud, which enables arbitrary process termination.	No	Yes	False
CVE-2022-35914	Teclib	GLPI	Remote Code Injection vulnerability in Teclib GLPI	No	Yes	False
CVE-2021-27137	DD-WRT Project	DD-WRT	Buffer Overflow vulnerability in DD-WRT	No	Yes	False
CVE-2016-15047	AVTECH	DVR Devices	Authenticated OS Command Injection vulnerability in AVTECH devices	No	Yes	False
CVE-2015-2051	D-Link	DIR-645 Router	Remote Code Execution vulnerability in D-Link DIR-645 Routers allows remote attackers to execute arbitrary commands via a ***GetDeviceSettings*** action to the HNAP interface.	No	Yes	False

Ransomware Insights for June 2026

The Ransomware insights were captured from various data leak sites of respective ransomware. This insight helps us to understand which industries and countries were targeted the most.

Ransomware	Description	No of affected organizations in June 2026	Targeted Industries	Vulnerabilities abused most
Qilin	The Qilin ransomware has been in existence since August 2022, also recognized as Agenda, has posed a substantial threat. Employing Rust and Go programming languages, this ransomware group executes intricate and elusive attack strategies. It's developed in Rust and identified as *Ransom.Win32.AGENDA.THIAFBB*, was discovered. Remarkably, this ransomware initially scripted in Go language was notorious for its focus on healthcare and education sectors, particularly in nations such as Thailand and Indonesia.	76	• Manufacturing • Business Services • Technology • Healthcare • Construction	• CVE-2023-4966 • CVE-2023-20269 • CVE-2023-27350 • CVE-2023-27351 • CVE-2023-40044 • CVE-2022-36537 • CVE-2022-41082
TheGentlemen	The Gentlemen ransomware campaign, which surfaced in the summer of 2025, exemplifies the rapid evolution of modern cyber threats. It combines advanced techniques with persistent, targeted operations, leveraging custom defense-evasion tools, adapting to existing security controls, and exploiting both legitimate and vulnerable components to effectively bypass layered defenses. The Gentlemen operators aggressively target and terminate critical services related to backup, database, and security operations, maximizing operational disruption and impact.	76	• Manufacturing • Construction • Healthcare • Insurance • Consumer Services	• CVE-2025-7771 • CVE-2025-32433 • CVE-2025-33073 • CVE-2025-55182 • CVE-2024-55591
Lockbit5	LockBit 5.0, internally codenamed ChuongDong, was announced on the RAMP dark web forum in September 2025 to mark the group's six-year anniversary, resuming operations after the February 2024 Operation Cronos law enforcement takedown. LockBit 5.0 payloads are built with a leaked version of the LockBit 3.0 builder and subsequently packed and 'branded' as a new variant of LockBit. LockBit 5.0 ransom notes instruct the	43	• Business Services • Manufacturing • Technology • Healthcare • Construction	Unknown

Ransomware	Description	No of affected organizations in June 2026	Targeted Industries	Vulnerabilities abused most
	victim to communicate with the attacker via TOX messenger.			
Akira	Akira is a ransomware-as-a-service (RaaS) operation distinguished by its early and aggressive focus on virtualized infrastructure. Beyond standard double-extortion tactics, Akira rapidly introduced a Linux encryptor specifically designed for VMware ESXi, enabling attackers to halt and encrypt large numbers of virtual machines from a single hypervisor using VM-aware options like vmonly and stopvm. Post-compromise activity prioritizes identity systems, backup platforms, and hypervisors, allowing fast, high-impact disruption of entire environments. This hypervisor-centric design, combined with data exfiltration via tools like rclone and SCP, makes Akira particularly effective against modern, virtualization-heavy networks.	28	• Manufacturing • Business Services • Technology • Construction • Agriculture	• CVE-2024-37085 • CVE-2024-40711 • CVE-2024-40766 • CVE-2023-20269 • CVE-2023-27532 • CVE-2023-28252 • CVE-2020-3259 • CVE-2020-3580
IncRansom	INC is a ransomware-as-a-service (RaaS) operation that emerged in mid-to-late 2023, operating through an affiliate-driven model in which core operators supply the malware and infrastructure while affiliates conduct intrusions and share profits. The group relies on a double-extortion strategy, coercing victims by threatening data leaks under the pretext of "protecting their reputation." INC maintains two dedicated leak sites a private, credential-protected portal used for victim communication and negotiation, and a public site used to release stolen data. First detected in July 2023 and tracked by Trend Micro as Water Anito, the ransomware encrypts files using AES algorithm, reinforcing its position as a structured and professionally run extortion operation.	27	• Education • Healthcare • Government • Manufacturing • Information	• CVE-2023-3519 • CVE-2023-4966 • CVE-2023-48788
Dragonforce	DragonForce is a ransomware group originating from Malaysia. Initially, known as a hacktivist group, DragonForce has transitioned into a	25	• Manufacturing • Business Services • Technology	• CVE-2024-21412 • CVE-2024-21893 • CVE-2024-21887 • CVE-2024-57727

Ransomware	Description	No of affected organizations in June 2026	Targeted Industries	Vulnerabilities abused most
	ransomware operation, threatening victims with data encryption and extortion demands. They have targeted various industries and organizations globally, including government entities, businesses, and critical infrastructure sectors. The group gained attention for their attacks on American companies, with details about data compromise and motives undisclosed. DragonForce has also threatened to release stolen information on dark web leak sites to pressure victims into paying ransoms.		• Healthcare • Construction	• CVE-2024-57728 • CVE-2024-57726 • CVE-2023-46805 • CVE-2021-44228
Safepay	SafePay ransomware is an emerging and previously undocumented threat, first observed in October 2024, that relies heavily on valid credentials likely sourced from dark web marketplaces and VPN access to infiltrate target environments. The group employs a multi-stage intrusion chain, commonly initiating attacks via Remote Desktop Protocol (RDP) and exploiting known VPN vulnerabilities while disabling defenses such as Windows Defender using LOLbins. SafePay features a modular and sophisticated design, enabling privilege escalation, UAC bypass, and network propagation, demonstrating a high degree of operational maturity. The ransomware encrypts files with a ***.safepay*** extension and drops a ***readme_safepay.txt*** ransom note, signaling the rise of a globally active ransomware operation targeting diverse industries across multiple countries.	19	• Manufacturing • Technology • Education • Healthcare • Business Services	• CVE-2025-8088 • CVE-2025-31324 • CVE-2025-53770 • CVE-2025-53771 • CVE-2025-61882
KRYBIT	KRYBIT is a sophisticated ransomware operation first observed in 2026 that encrypts files on compromised systems and appends the .KRYBIT extension, while dropping a ransom note named RECOVER-README.txt to initiate extortion procedures. The malware targeted documents, databases, archives, images, and enterprise-critical files, while simultaneously operating a double-extortion model that	19	• Business Services • Consumer Servies • Manufacturing • Technology • Public Sector	Unknown

Ransomware	Description	No of affected organizations in June 2026	Targeted Industries	Vulnerabilities abused most
	combined file encryption with theft of sensitive data including employee records, credentials, financial information, and technical design files. Victims were instructed to access multiple Tor-based onion communication portals hosted on Apache with PHP 8.0.30 using unique victim identifiers to negotiate recovery procedures and ransom payments. Observed operations affected at least 20 organizations across consumer services, business services, education, technology, and manufacturing sectors, with incidents identified in Germany, Mexico, Türkiye, Japan, and Austria.			
Payload	The Payload Ransomware is a lightweight C++ based ransomware (~385 KB) that operates without obfuscation, indicating prior attacker access and possible pre-disabling of AV/EDR defenses. The malware encrypts files using the ".payload" extension and drops a ransom note named RECOVER_payload.txt, leveraging a double-extortion model involving data exfiltration and Tor-based negotiation. It performs extensive pre-encryption actions, including deletion of shadow copies, clearing event logs, disabling security controls, and terminating backup and productivity services to maximize impact. The ransomware supports lateral movement via network share enumeration, uses multi-threaded execution, and employs ChaCha20 encryption with Curve25519 key exchange for efficiency and security. To evade detection and reduce forensic artifacts, it relaunches in hidden mode, leverages NTFS alternate data streams for self-deletion, and avoids encrypting critical system files to maintain operational stability.	13	• Manufacturing • Business Services • Hospitality • Healthcare • Financial Services	Unknown
NightSpire	NightSpire, quickly positioned itself as a high-impact ransomware actor by pairing double-extortion operations with exploitation of	12	• Manufacturing • Business Services • Healthcare	CVE-2024-55591

Ransomware	Description	No of affected organizations in June 2026	Targeted Industries	Vulnerabilities abused most
	advanced vulnerabilities. The group maintains a dark-web leak portal with countdown-based coercion and employs stealth techniques LOLBins, MEGACmd, WinSCP to exfiltrate data while remaining undetected inside victim networks. Its campaigns span the U.S., Japan, Taiwan, Egypt, and the U.K., with a notable concentration on manufacturing, reflecting a globally distributed yet technically disciplined threat posture.		• Technology • Construction	

Conclusion

The events of June 2026 underscore a fundamental reality: speed defines survival in modern cybersecurity. Organizations that delayed patch deployment, lacked real-time visibility into exploited vulnerabilities, or failed to correlate threat intelligence with infrastructure faced catastrophic breaches. To navigate this evolving threat landscape, security teams must adopt intelligent vulnerability intelligence platforms that provide real-time exploit data and threat prioritization. Loginsoft's Vulnerability Intelligence solution delivers exactly this - actionable threat insights correlated with live exploit activity, enabling organizations to patch what matters before adversaries strike. In a month like June, the difference between informed and uninformed defense is measured in compromised organizations.

loginsoft

Connect with us

linkedin.com/loginsoft

x.com/loginsoft_inc

www.loginsoft.com