CyberSagacity

Zero-Day Attacks
The problem with AppSec.

There are threats you can prepare for — and then there are the ones you can't see coming. Zero-day attacks exploit vulnerabilities unknown to the vendor, with no available patch. These “unknown unknowns” are among the most significant and fastest-growing dangers organizations face today.

PUBLISHED
2026

AUDIENCE
CISO · AppSec · Security Operations

FORMAT
Threat Brief

THE INVISIBLE THREAT

There are threats you prepare for.
And then there are the ones you can't see.

Zero-day attacks exploit vulnerabilities that are unknown to the software vendor and, therefore, have no available patch.

These “unknown unknowns” represent one of the most significant and growing dangers to organizations today. By the time a zero-day surfaces, the damage is already in motion — and the tools most teams rely on were never designed to recognize it.

THE NEW NORMAL · A SURGE IN ZERO-DAY EXPLOITS

Zero-day exploitation has stabilized at a new, alarmingly high baseline.

The prevalence of zero-day attacks is no longer an anomaly; it has become a constant and elevated threat. The number of zero-day exploits has stabilized at a new, alarmingly high baseline — and the trend is unambiguous.

75

Zero-days were actively exploited in 2024 — nearly double the number from 2020.

SOURCE · GOOGLE PROJECT ZERO, "2024 ZERO-DAYS: THE YEAR IN REVIEW"

~2×

The increase in actively exploited zero-days since 2020 — dozens weaponized every year.

SOURCE · GOOGLE PROJECT ZERO, 2024

A clear, sustained trajectory: attackers keep getting better at finding and leveraging these flaws.

FIVE-YEAR EXPLOITATION TREND

> **This is the "new normal" — attackers consistently discover and weaponize dozens of these critical flaws each year.**

THE EVOLVING LANDSCAPE OF ATTACKS

Attackers have turned enterprise defenses into entry points.

Today's cybercriminals and state-sponsored groups are not just targeting consumer-facing products. They are increasingly focused on the critical infrastructure of enterprise networks.

- In 2024, over **44%** of zero-day exploits targeted enterprise technologies — a notable increase from the year before.
- Within that category, a **majority** targeted security and networking products like VPNs and firewalls.

THE UNCOMFORTABLE REALITY

Attackers are effectively using a company's own defenses against them.

WHY ZERO-DAYS ARE SO DANGEROUS

What makes these attacks uniquely effective and devastating.

No patch, no defense

By definition, a zero-day strikes before a vendor can issue a patch — leaving traditional signature-based security tools powerless, with no way to recognize the malicious activity.

Speed is critical

The window from public disclosure to active exploitation has shrunk to days. In some cases attackers deploy exploits in as little as **five days** — far faster than most patching cycles.

High value, high incentive

The black market for zero-days is a multi-million-dollar industry. That value incentivizes sophisticated groups to invest heavily in discovering and weaponizing them — ensuring a steady stream of new threats.

> **Signature-based tools can only catch what they've already seen. A zero-day is, by definition, something they never have.**

2025 · A CONTINUING AND INTENSIFYING THREAT

2025 is on pace to surpass every prior year.

+46% Zero-day exploitation in the first half of 2025 is up **46%** compared with previous periods.

30+ Zero-days already added to CISA's list of **actively exploited vulnerabilities** — pointing to a record year.

CVE-2024-21887 · CVE-2023-46805

Ivanti Connect Secure & Policy Secure

Massively exploited in early 2025 across 2,000+ VPN devices. The chain let attackers bypass authentication and execute remote code, establishing a foothold in targeted networks.

CHINESE STATE-SPONSORED ACTORS

CVE-2025-21297

Microsoft Office RTF Remote Code Execution

Code execution triggered simply by opening a malicious Rich Text Format file. Delivered via phishing, it required no user interaction beyond opening the document — making it highly effective.

CVE-2025-53690

Sitecore ViewState Deserialization

Exploited to gain initial access to internet-facing Sitecore servers via a publicly exposed sample machine key — enabling remote code execution, recon tooling, and lateral movement.

RISK OF INSECURE DEFAULTS

References: Help Net Security (Aug 6, 2025), “Ransomware is up, zero-days are booming…” · Todyl (Jan 17, 2025), “Dissecting the Recent Rise in 2025 Zero Days.”

2024 · A NEW, ELEVATED BASELINE

75 zero-days exploited — and the target shifted to the enterprise.

75 Zero-day vulnerabilities actively exploited in 2024, per Google's Threat Analysis Group and Mandiant — solidifying the upward trend since 2022.

44% Of these zero-days targeted **enterprise technologies**, particularly security and networking products.

CVE-2024-21887

Ivanti Connect Secure

One of the most widely exploited vulnerabilities of 2024 and early 2025, compromising thousands of devices globally. Used by state-backed espionage groups for surveillance and data exfiltration.

STATE-BACKED ESPIONAGE

Google Chrome · Multiple CVEs

Google Chrome Exploit Chain

Multiple Chrome zero-days were found and patched throughout 2024 — some used in an exploit chain that targeted individuals through malvertising and social engineering.

NORTH KOREAN STATE-SPONSORED ACTORS

CVE-2024-38112

Microsoft Windows MSHTML

A remote code execution flaw exploited via malicious internet shortcut files to deliver information-stealing malware while bypassing standard defenses.

"VOID BANSHEE"

References: Google Cloud Blog (Apr 29, 2025), "Hello 0-Days, My Old Friend: A 2024 Zero-Day Exploitation Analysis" · Google Threat Analysis Group & Mandiant.

2023 · THE PEAK YEAR FOR ZERO-DAYS

A record-breaking 97 zero-days exploited in the wild.

97 Zero-day vulnerabilities observed being exploited in the wild in 2023 — the highest ever reported by Google and Mandiant at the time.

+56% Year-over-year increase, led by state-sponsored actors — particularly those attributed to China.

CVE-2023-34362

Progress MOVEit Transfer

A critical SQL injection flaw — one of the most impactful zero-days of the year. It drove a global data-theft campaign affecting hundreds of organizations and millions of individuals.

"CLOP" RANSOMWARE GANG

CVE-2023-2868

Barracuda Email Security Gateway

Exploited for months before disclosure. A suspected Chinese espionage group installed custom malware to maintain persistence and exfiltrate data from targeted organizations.

SUSPECTED CHINESE ESPIONAGE

CVE-2023-20867

VMware ESXi

Exploited to take over VMware's virtualization platform — remaining undetected while moving laterally across virtual machines and servers, underscoring attackers' growing sophistication.

UNC3886

References: Google Cloud Blog (Mar 27, 2024), "A review of zero-day in-the-wild exploits in 2023."

PROACTIVE DEFENSE

You can't patch what you can't see. But you can prepare for it.

Don't wait until a zero-day attack compromises your organization. Proactive defense requires a modern, comprehensive security strategy that goes **beyond traditional patching**.

Signature-based tools recognize only what they have seen before. Defending against the unseen means shifting from chasing individual findings to understanding where real exposure lives — validating telemetry, prioritizing by true risk, and concentrating defense where an exploit would do the most damage.

Traditional Patching	Intelligence-Led Defense
○ Blind to vulnerabilities with no signature or patch.	• Validated telemetry over raw, unverified scanner output.
○ Reacts only after disclosure — often days too late.	• Risk prioritized by exploitability and business impact.
○ Treats every finding as equal; real exposure hides in noise.	• Defense concentrated where exposure is greatest.
○ No view of which assets an exploit would actually reach.	• Decision-grade insight that leaders can act on with confidence.

CYBERSAGACITY

To learn how our advanced security solutions can help you detect and mitigate the unseen threats of zero-day attacks, contact us today for a consultation.

Learn more at www.cybersagacity.com →