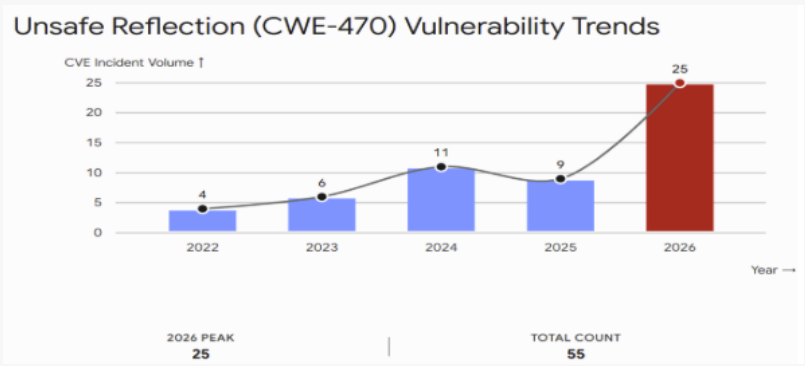
Waratek Launches Reflection Protection, a Zero-Configuration Defense Against Known & Zero-Day Reflection Attacks

The new Reflection Protection rule protects apps and dependencies against reflection attacks from known vulnerabilities to AI-discovered zero-days.

Waratek logo



Trends in Unsafe Reflection Vulnerability: 177.8% year over year increase in disclosed UR vulnerabilities.

DUBLIN, IRELAND, August 18, 2026 /EINPresswire.com/ -- Waratek, the leader in runtime application security, today announced the release of its new Reflection Protection rule, a dedicated runtime security feature designed to block exploitation of unsafe reflection and dynamic class-loading vulnerabilities, for both known CVEs and zero-days, without requiring any code changes, application downtime, or complex configuration.

"Every week brings a new CVE, and the gap between disclosure and exploitation keeps shrinking," said Doug Ennis, CEO of Waratek. "Attackers know that security teams can't realistically patch every application the moment a vulnerability is announced."

“What teams need are automated detection and remediation tools that work at the runtime layer, closing off entire classes of attack before anyone has to identify the next CVE, write a patch, or schedule a maintenance window. That's exactly what the Waratek RASP Reflection Protection delivers: active protection that just works the moment you turn it on."

Unsafe reflection vulnerabilities have exploded in 2026 with a 177.8% year-over-year increase from 2025 so far this year, one of the most significant vulnerability disclosure trends. That puts unsafe reflection vulnerabilities disclosures on pace for more CVEs in this category than the previous three years combined. This surge is likely correlated with the rapid rise of AI-assisted coding and AI-assisted vulnerability discovery tools, which are simultaneously accelerating the introduction of vulnerable code patterns and the speed at which researchers are uncovering coding flaws. As organizations race to adopt AI-driven development pipelines, this data highlights a widening gap between how fast vulnerable code is released and how prepared runtime

defenses are to catch it.

> “Teams need automated detection & remediation tools that work at runtime, closing off entire classes of attack before anyone identifies a CVE, writes a patch, or schedules a maintenance window.”
>
> *Doug Ennis, Waratek CEO*

Unsafe reflection is one of the most persistent and dangerous vulnerability classes in applications and one of the most common vulnerability patterns in AI-generated code. It allows attacker-controlled input to abuse the reflection API and load arbitrary classes at runtime, often via Class.forName() and similar APIs. Because of the vulnerability’s complexity, it shows up again and again, most commonly and most dangerously, in JSP loading paths and in expression language evaluators which remain a favorite target for attackers seeking remote code execution resulting in complete compromise of the system.

Two recent, real-world examples illustrate the risk:

CVE-2026-63317 / CVE-2026-42027 — Three separate code paths load a class by its fully-qualified name via Class.forName() and invoke its no-argument constructor without validating the class name or type first. An attacker who can tamper with a model archive or format name can force the application to instantiate an arbitrary class.

CVE-2026-40008 — The pipe processor reads a fully qualified class name and instantiates it using Class.forName().newInstance() with no validation or allowlisting, giving an attacker who controls that input the ability to load and execute arbitrary code.

Both vulnerabilities share the same underlying weakness: unsafe reflection with no guardrails at the point where the class is loaded. Waratek's new Reflection Protection rule prevents attacks that exploit unsafe reflection vulnerabilities by tracking untrusted data and by hooking into the Reflection API. This addresses the weakness directly, at the runtime layer, regardless of which library, framework, or application introduces it — which means it actively protects against not just these two CVEs, but the broader class of unsafe reflection vulnerabilities yet to be disclosed.

Traditional, reactive, remediation, requires identifying a specific vulnerability, waiting for a vendor patch, and then testing and deploying that patch across every affected application. Reflection Protection is an active security rule. It closes off unsafe reflection vectors broadly, so any attacks that abuse the root cause of this vulnerability are stopped whether or not the specific vulnerability has been identified, disclosed, or patched yet.

That simplicity is central to the release. Security and engineering teams can enable Reflection Protection directly from the Waratek Portal's rule wizard, with zero configuration, zero source code modifications, no re-deployment, and no application downtime required. The protection

rule is applied at the JVM layer, so it goes into effect immediately across all protected applications.

"Unsafe reflection vulnerabilities have grown by 525% between 2022 and 2026 and we are still in the middle of 2026." Apostolos Giannakidis, CTO of Waratek added. "We can no longer run our apps on runtime platforms that are not secure by default."

"The expectation for runtime platforms now has to be preemptive protection by default against the attack vectors that matter most; those that can hand an attacker complete control of the platform. Unsafe reflection vulnerabilities sit at the very top of this list. If your runtime layer isn't stopping that by default, it is not keeping pace with the AI-speed zero-day detection."

Availability

The Reflection Protection rule is available now to Waratek RASP customers and can be enabled in minutes without any configuration.

To see the Reflection Protection rule in action and learn how Waratek's runtime protection platform defends against known and zero-day vulnerabilities without code changes or downtime, visit Waratek.com to schedule a demonstration.

###

About Waratek
With headquarters in Dublin and Chicago, Waratek provides award-winning runtime application security that protects enterprise software from exploits at the point of execution — including vulnerabilities introduced by AI-generated code. Waratek's platform applies security controls directly inside the application runtime, eliminating entire classes of exploits without code changes, signatures, or intrusive agents. The world's most security-conscious organizations rely on Waratek to defend mission-critical applications and meet evolving compliance requirements. Learn more at www.waratek.com.

Doug Ennis, CEO
Waratek
email us here
Visit us on social media:
LinkedIn

in today's world. Please see our Editorial Guidelines for more information.