MITRE ATT&CK TOP 25

Deterministic Protection with Virsec

The world runs on software, yet, until now, there was never a way to achieve 100% protection of that software while it is running, wherever it is running. The only way to fully protect software is by fully mapping and understanding what it is supposed to do and immediately stopping what it is not. Virsec's Deterministic Protection Platform (DPP) eradicates software threats in real-time before they can cause any harm, making security response obsolete.

What is MITRE ATT&CK?

MITRE ATT&CK® stands for MITRE Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK). The MITRE ATT&CK Framework is a curated knowledge base that tracks cyber adversary tactics and techniques used by threat actors across the entire attack lifecycle. The framework is more than a collection of data: it is intended to guide organizations on strengthening their security posture.

Every year, MITRE also publishes the Top 25 Most Dangerous Software Weaknesses based on the most common and impactful issues experienced over the previous two calendar years. These weaknesses are dangerous because they are often easy to find, exploit, and allow adversaries to completely take over a system, steal data, or prevent an application from working. This list is a valuable community asset for developers, testers, and security operations teams, helping them with vulnerability management and security controls selection and prioritization.

MITRE Top 25 Most Dangerous Software Weaknesses

MITRE Top 25 is populated by publicly available threat intelligence and incident reporting and research on new techniques contributed by cyber security analysts and threat hunters. Those same professionals use it to understand better the different ways bad actors might operate such that threat behavior can be detected and stopped.

The 2021 MITRE Top 25 list highlights some common security vulnerabilities that have been around for quite some time. These attacks are still occurring, but traditional security solutions cannot protect the most dangerous and prevalent ones. The below refers to some of the most dangerous attacks mentioned in the current MITRE Top 25 list.

Cross-Site Scripting (XSS): Attackers can use web-based features to plant and insert bits of code that are malicious scripts. Specifically, in XSS situations, attackers can upload these scripts into unprotected client-side web pages to be executed when others open that page. Writing secure code against XSS attacks involves prohibiting web applications from taking unauthorized action or communication. Virsec's Deterministic Protection Platform (DPP) applies a precise approach coupled with strict control integrity controls to stop any unauthorized action in-flow with the application execution.

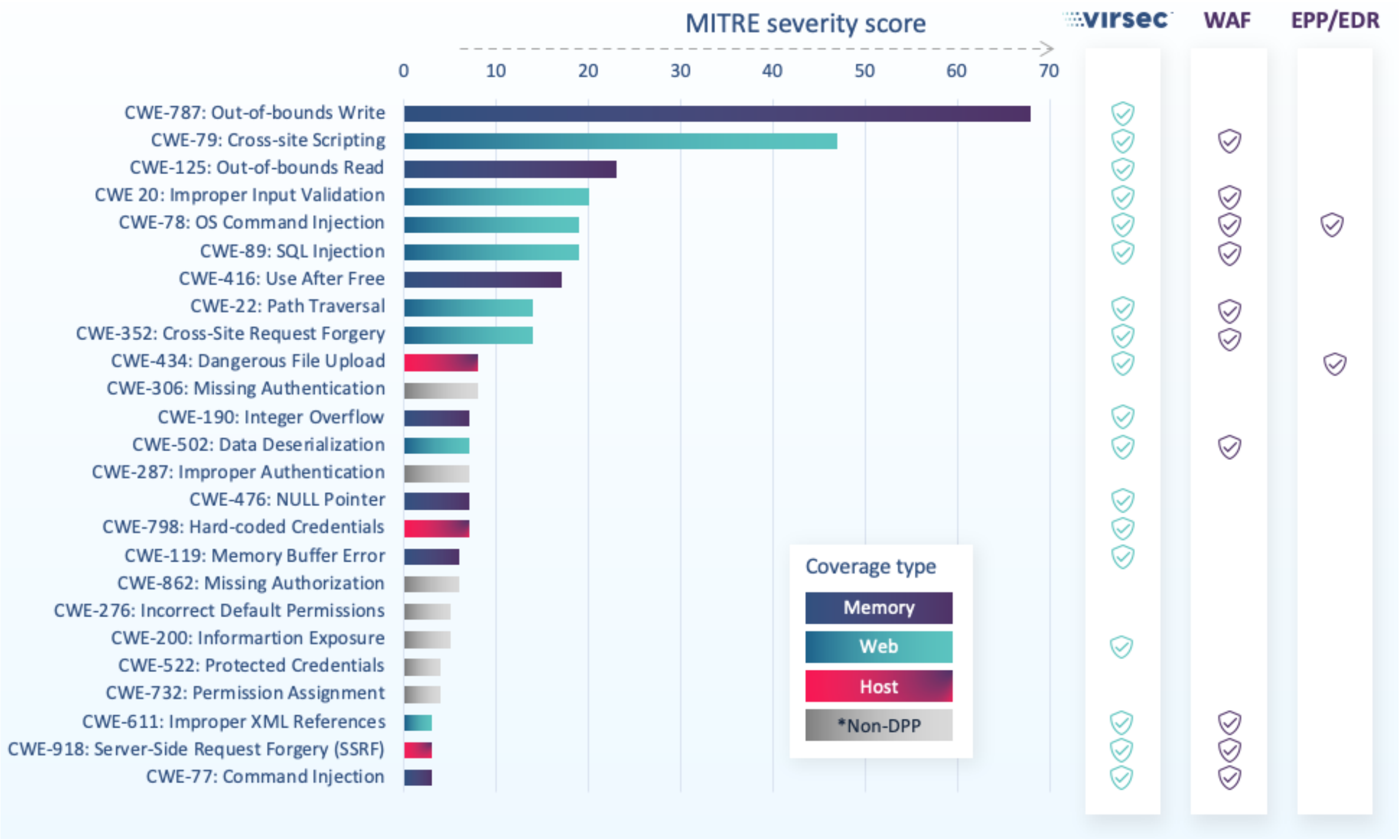
Memory Overruns: Manipulating memory remains one of the most catastrophic ways of attacking a vulnerable system. Suppose an attacker has possession of a specific memory address within an executable application. In that case, they can use it to enter values or commands that exceed the size of that memory space. The attacker can then insert their own executable software, making it possible to take over the trusted application execution or elevate permission levels. With DPP, organizations gain the most advanced level of memory protection for hosted software applications. Our patented approach ensures efficient control flow integrity by uniquely mapping and securing memory at the core without conflicts, kernel dependencies, or access to source code.

SQL/Command Injection: DPP prevents attackers from changing the intended behavior of SQL queries and process control flows to exploit server software components. With the deep instrumentation of the application, DPP constantly monitors input data and blocks any attempts of turning data into interpreted or executable code. With this in-depth approach, DPP stops any opportunity for an attacker to exfiltrate data from an application or gain execution control on a given system.

Virsec Coverage of the MITRE ATT&CK TOP 25

The Deterministic Protection Platform by Virsec offers the most extensive and effective controls for mitigating the top 25 issues identified by MITRE. Virsec's platform offers three layers of protection at the Host, Web, and Memory levels. The graphic below depicts how Virsec DPP protects against each of the top 25 threats.

Web and memory errors dominate the top 10 found to be the most severe and difficult to analyze, and Virsec provides the broadest protection for these. Most of the weaknesses not addressed by Virsec are covered by implementing an Identity and Access Management or Software Configuration Management solution.



About Virsec

Virsec is on a mission to make security response obsolete. Taking a First Principles approach to protection, the Virsec Deterministic Protection Platform (DPP) automatically and consistently maps precisely what your software is supposed to do and stops, in milliseconds, any deviations -- preventing attackers from leveraging vulnerabilities to execute control and run malicious code. DPP is a proven technology that enables leading government and commercial organizations worldwide to protect their server workloads, at runtime, against ransomware and other known and unknown threats, reduce operating costs and meet key compliance requirements. Virsec is headquartered in San Jose, California, with offices all over the world. For more information, please visit https://www.virsec.com.