STERNUM

MITRE ATT&CK TOP 25 FOR IOT DEVICES

Self-Protection to Actively Mitigate Threats From The MITRE ATT&CK Top 25

ABOUT THE MITRE ATTACK TOP 25

The MITRE ATT&CK Framework catalogs the adversarial tactics and techniques used by threat actors across the attack lifecycle. This helps organizations strengthen their security posture. Every year, MITRE publishes the Top 25 Most Dangerous Software Weaknesses (CWE Top 25), a list of the most common and impactful issues of the previous two calendar years. These weaknesses are relatively easy to find and exploit; they allow adversaries to take over systems, steal data, and prevent devices from working. As part of its process, the CWE Team leverages Common Vulnerabilities and Exposures (CVE®) data from the National Institute of Standards and Technology (NIST) National Vulnerability Database (NVD), as well as the Common Vulnerability Scoring System (CVSS) associated with each CVE record. A formula is applied to the data to score each weakness based on prevalence and severity.

WHAT MAKES IOT DEVICES DIFFERENT

The CWE Top 25 list covers all IT infrastructure, PCs, servers, and network and other devices without differentiating between them. However, IoT devices, including all IIoT and IoMT devices, have unique characteristics. Unlike PCs and servers, they are unprotected by EPP and EDR, leaving them vulnerable to exploitation. Deployments thus include hundreds or thousands of mission-critical smart devices with no on-device protection. This makes them easier to attack and since an attack can precipitate a life-and-death event, or propagate to thousands of devices, the magnitude of the impact can be consequential. Because of their unique risk profile, IoT devices require a different approach to the CWE Top 25.

The following characteristics are unique to IoT devices:

Low Resources: IoT devices have limited resources, making it harder to secure them or apply monitoring and protection. EPP and EDR agents, and other endpoint technologies, while suited for IT products, are too computationally intensive for the low power, battery, and memory capacities of IoT devices.

Limited updating and patching. Unlike PCs and servers that constantly push security updates and patches, IoT devices are updated infrequently. Releasing a patch is organizationally expensive and by definition fails to address the risk of zero-days. Even when released, many devices remain unpatched, leaving them vulnerable to 1-day attacks.

Third-party components: IoT devices rely heavily on third-party libraries and diverse components. These 'black boxes' are difficult to scan for vulnerabilities, patch, and control in the field. Often they are overlooked. Vulnerabilities that are no longer a threat in the broader IT world are still dangerous in the IoT world.

Diverse OSs: IoT devices have many types of hardware and operating systems, from different flavors of Linux to real-time operating systems. Together they create a large attack surface with a wide range of different vulnerabilities that is difficult to secure. Because they are not OS-agnostic, tools like agents rely on the underlying OS and would have to be changed for every variant of OS. These protections are structurally maladaptive for heterogeneous environments and architectures.

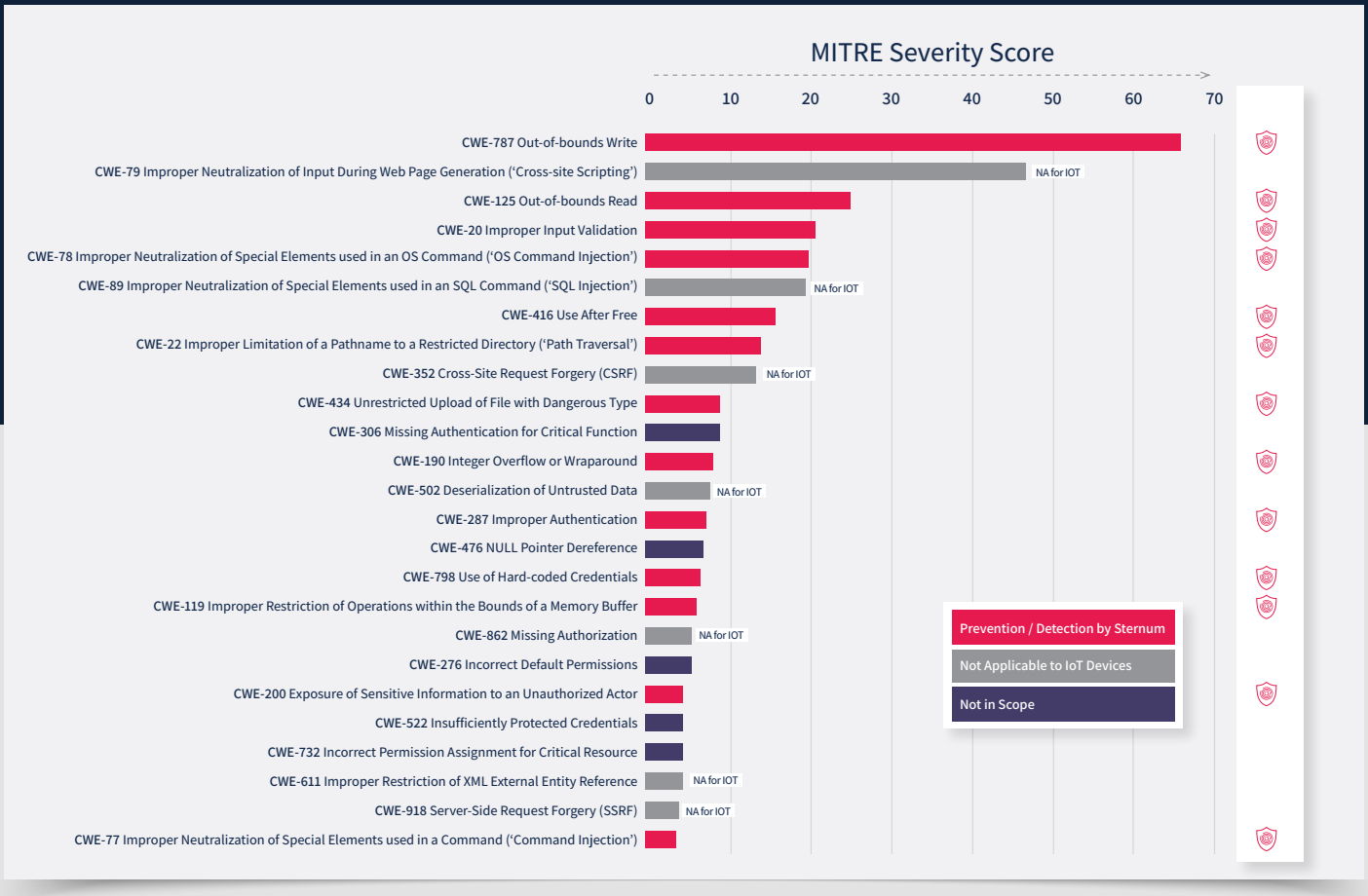
Scale of Attack Surface: According to IoT Analytics, there are over 12.3 billion connected devices globally. A single IoT deployment may involve hundreds or thousands of devices and innumerable lines of code. Attackers rely on this expanding composite attack surface, perforated with 10 vulnerabilities per 1000 lines of code, for their gateway to exploitation and breach.

STERNUM

STERNUM COVERAGE OF MITRE ATTACK TOP 25

To overcome the limitations mentioned above and secure IoT devices against the Top 25 Most Dangerous Software Weaknesses (CWE Top 25) list, Sternum uses an approach known as Embedded Integrity Verification (EIV) to implement deterministic runtime protection. Sternum's single-click security solution gives any edge device the ability to protect itself from attempts to exploit vulnerabilities in real-time. EIV expresses the steps an attacker takes to exploit vulnerabilities as a unique Fingerprint of Exploitation™. During the operation of a device, Sternum uses its agentless on-device presence to verify the integrity of memory and the execution flow of programs, preventing attacks when the unique Fingerprint of Exploitation™ triggers the prevention mechanism. This protects the firmware and all software and services on a device from entire families of exploits, such as command injection and buffer overflow, safeguarding the device in real time from zero-day and one-day attacks. It embodies a proactive IoT security paradigm that neutralizes the risk of vulnerabilities and nullifies the urgency of patching them: a vulnerability which cannot be exploited ceases to be a threat. Sternum's solution enables devices to actively defend themselves from new malware before security researchers identify it.

The diagram below shows Sternum's coverage of the 2021 MITRE ATTACK top 25 list. The vulnerabilities marked in red represent the chief risk on an IoT device. All are prevented deterministically by Sternum. The vulnerabilities marked in gray relate to PCs and servers and are not characteristic of IoT devices. The vulnerabilities marked in blue are out of scope for attacks on the firmware and software of devices. They fall into the category of flaws that should be protected by basic design or administrative controls. In many cases though, Sternum would detect behavioral anomalies and alert on attacks that used these vulnerabilities.



ABOUT STERNUM

Sternum, the provider of the only universal IoT platform for security and observability, offers runtime protection and visibility for all IoT devices. It was founded in 2018 by veterans of the Israeli Defense Forces' elite cyber team, Unit 8200. Trained to design exploits that could bypass any defense, they invented a technology that would protect a system from themselves. Sternum's holistic unified platform consists of two modules: Embedded Integrity Verification (EIV) and Analytics and Detection System (ADS). Both answer the unique needs of IoT device-level protection and visibility in medical, industry 4.0, smart city, energy, telecommunication and beyond, future proofing the security of digital transformation.

Email us for more information: sales@sternumiot.com