Traditional Vulnerability Management: The Dog That Won't Hunt

Running a vulnerability management program for Internet of Medical Things (IoMT) devices can be a frustrating or even insurmountable task. The sheer number of vulnerabilities that are disclosed can be overwhelming, and there is no easy way to apply a fix. Traditional vulnerability management approaches designed for endpoints and servers simply don't work for securing medical devices. Asimily Insight offers a better way forward.

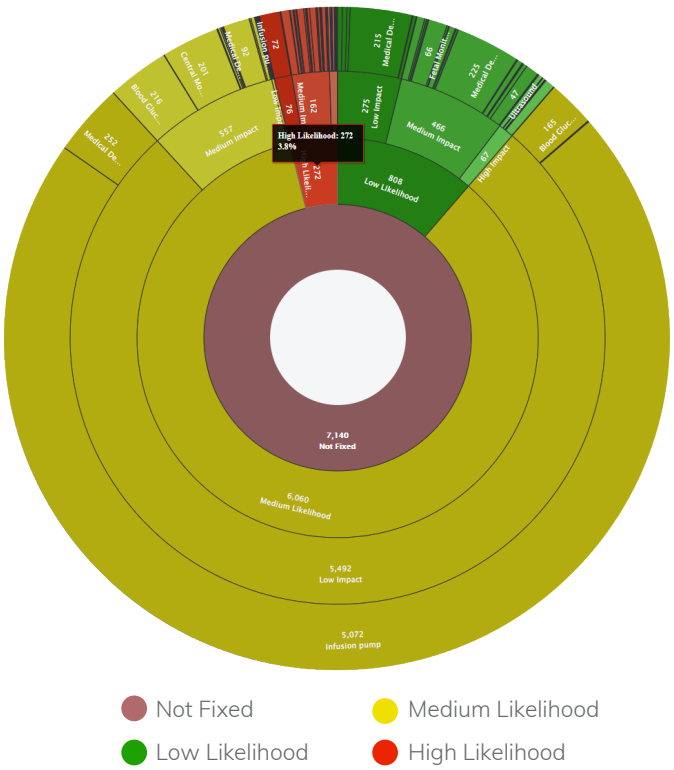
There are several reasons why the standard vulnerability management approach is a poor fit for the unique challenges of IoMT:

01 A typical medical device may contain many components, any of which could have potential vulnerabilities, but that does not mean that every vulnerability poses an actual threat. Medical devices have a much more constrained set of behaviors, based on how they are configured for clinical use. It is very common for a particular component installed on a device to never be used during typical operation. By using the traditional approach, you can spend large numbers of man-hours fixing vulnerabilities that never posed a real risk.

02 Common VM solutions also do not consider the impact that a breach of specific devices could cause in the medical setting. For example: Some devices, such as those that store or transmit protected health information (PHI), pose a much greater risk if they are compromised than others. Vulnerability scoring systems such as CVSS do not take these factors into account. Without this context, you risk leaving vulnerabilities on crucial devices open.

03 Traditional vulnerability management has a strong focus on patching vulnerable devices as the primary form of remediation. While this largely works for endpoints and servers, it is often unrealistic for IoMT devices. Vendors often do not release patches for newly-discovered vulnerabilities, and if a third-party patch is available, it may void the device's warranty to apply it. Segmentation is another possibility, but the process is time-consuming and error-prone, and even when successful only serves to reduce the "blast radius" of an attack. Without better options, remediation will be difficult and time-consuming.

Distribution of devices that have at least one known vulnerability



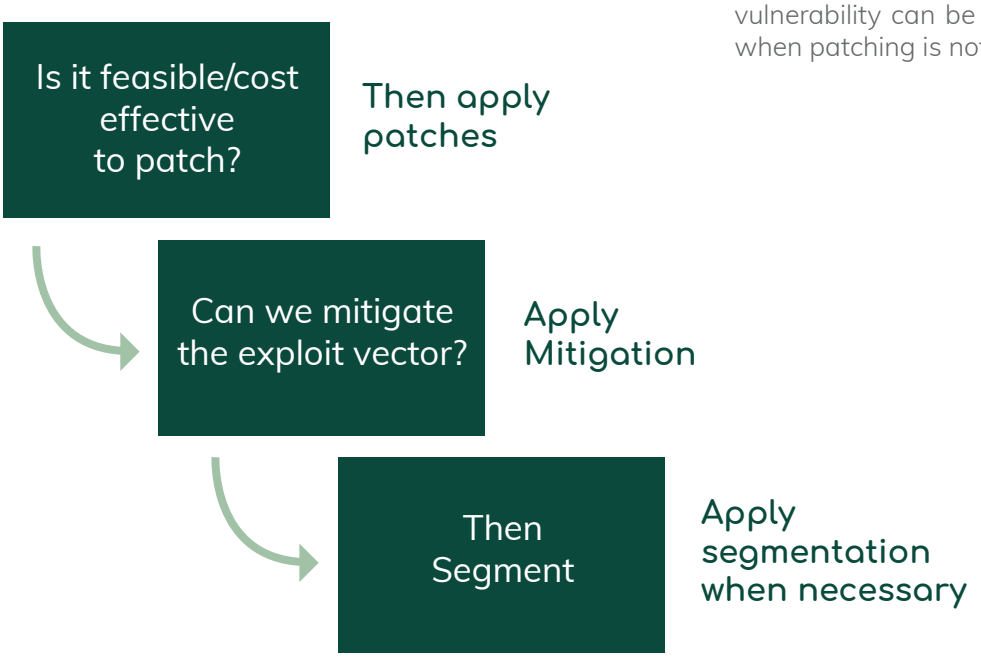
A Better Way to Do VM

Asimily Insight offers a new approach to vulnerability management, specifically designed for IoMT devices and the challenges that HDOs face:

01 Insight shows which devices have the highest likelihood of exploitation. We proactively predict potential paths for an attacker to compromise a device and we leverage Manufacturer Disclosure Statements for Medical Device Security (MDS2s) and Software Bills of Material (SBOMs) to understand what is "under the hood." In some cases, mitigations already exist on the device. Using Insight, you can avoid spending time fixing vulnerabilities that exist "in name only."

02 Insight also shows the impact a breach would have through Asimily's proprietary risk modeling. This takes the context of the device into account, such as its function and capabilities, the types of data it handles, and any connections to other systems, enabling you to prioritize fixes for the highest impact devices first.

03 Insight provides device-specific workaround recommendations that have been tested in real-world scenarios and proven to be clinically viable. Using these recommendations, the risk of a vulnerability can be reduced or eliminated, even when patching is not feasible.



Tech

- Exploit analysis using the MITRE ATT&CK framework for every vulnerability discovered since 1995
- Largest repository of MDS2 manufacturer capability information, covering over 1000 unique device models
- Workaround recommendations, customized based on the specific vulnerability and device

Outcomes

- Reduce time to remediate issues by prioritizing high likelihood, high impact issues first
- Reduce manual VM analyst effort by 90%+ by streamlining remediation efforts and avoiding fixing "in name only" vulnerabilities that pose no real threat
- Reduce risk for devices that cannot be patched or easily segmented through battle-tested workarounds