HVSS v1.0 Documentation

General Idea

Create a calculator which would provide a simple way to accurately evaluate cybersecurity risk on medical software products – pre and post mitigations.

High Level Summary

HVSS (Healthcare Vulnerability Scoring System) calculator is built to resolve the following existing issues:

- Accuracy of cybersecurity risk evaluation on medical software products
- Lack of ability to efficiently collaborate as an industry arriving to the common denominator on what the risk scoring system should be.

HVSS (Healthcare Vulnerability Scoring System) calculator is built to resolve those issue through introduction of following:

- A new way to calculate **Exploitability** through re-defining **Attack Complexity,** and as such – allowing to factor into the calculation how difficult for attacker would be complete the attack successfully.
- A new, AI driven evaluation methodology behind the calculator allowing to arrive to more exact scoring of examined attack scenarios for medical software products.
- New risk profiles: Patient Safety, Sensitive Data, and Hospital Breach. Introduction of those risk profiles is allowing to evaluate greater variety of the risks on medical software products with the necessary amount of precision.
- Full disclosure of all the HVSS materials to the community coupled with neural-network AI\ML model-based approach to the calculations, allowing any organization or individual interested to participate to become a partner and contribute an amendment of the **Exploitability** parameters, **Risk Profiles**, and **Attack Scenarios** (or their proposed scores) that were used to train the AI\ML models, which are driving the HVSS calculator scoring system.

As such – creating a simple, efficient and practical way, while establishing a forum for industry to align on approach and tools for calculating cybersecurity risks on medical software products.

Aside from resolving issues stated above for the medical software industry, the HVSS calculator holds the potential to be adopted by other industries with minimal modifications.

- **Exploitability** calculations would be similar for all the software products.
- As such, adaptation by other industries would require creation of **industry specific impact profiles** (or running of existing **Original CIA impact profile**), which is made very simple by utilization of AI\ML model supervised learning approach – with which the modifications would boil down to editing provided spreadsheet with the list of parameters, attack scenarios and scores proposed for them.

Following materials are shared by HVSS group on GitHub:

- HVSS Calculator service code (back+front ends)
- HVSS Calculator lab for training and evaluating the AI\ML models

Fields Definitions

Exploitability:

Attack Vector (AV):

Network – Attack can be carried out over the network; attacker can connect from any node. Examples:

- The attacker carries out an attack over the medical device network interface exposed to the network external to the hospital.

Adjacent Network – Attack can be carried out over the restricted set of subnets. Examples:

- Attacker carries out attack via network interface exposed to the hospital intranet only.
- The attacker carries out an attack over the Bluetooth interface exposed inside the hospital and providing ability to connect from another room or hallway.

Local – Attack can be carried out over interfaces of the product available as part normal operation (touchscreen, keyboard, mouse, externally exposed ports, etc.) and requiring operator to be physically present near the targeted product. Examples:

- The attacker carries out an attack by loading malicious software from flash drive using USB port.
- The attacker carries out an attack by escaping KIOSK and modifying device settings using keyboard and mouse.

Physical – Attack can be carried out either over hardware interfaces typically not available as part of the normal operations or require manipulations at hardware level . Examples:

- The attack is carried out over JTAG port, available on one of the boards inside the physical encasement.
- The attack is carried out through channel created by directly soldering wires to the board

Extended Attack Complexity (EAC):

Negligible – The unauthorized change of state in product can be achieved through application interface. Example:

- Overprivileged users are getting access to admin capabilities.

Low - The unauthorized change of state in product can be achieved without a need to install malicious code on the product. Examples:

- Code injection
- Man in the Middle Attack

Medium - The unauthorized change of state in product can be achieved through installation of malicious scripts and subsequently altering data in persistent storage. Examples:

- Malicious software update
- Installation of malicious scripts, which will modify treatment data stored on disk.

High – The unauthorized change of state in product can be achieved through installation of malicious scripts and subsequently altering data in memory. Example:

- Installation of malicious scripts, which will modify treatment data in memory.

Critical – The unauthorized change of state in product can be achieved through installation of custom exploits, built for specific hardware configuration or to exploit zero day, discovered as part of dedicated vulnerability research. Examples:

- Installation of malicious driver for network card
- Re-flashing the microcontroller with malicious code
- Exploiting discovered zero, consisting of unique per network software library set of vulnerabilities (Urgent11 as an good example)

Extreme – The unauthorized change of state in product can be achieved through successful compromise of one of the commonly utilized security solutions not residing on target product. Example:

- Compromise of the PKI as a Service and stealing code signing key
- Compromise of a Cloud HSM solution

Privileges Required (PR)

None – no privileges are required to carry out an attack. Example:

- Attacker can bypass the authentication control in web application by closing out authentication pop-up and get full access to application content.

Low – to obtain privileges required for the attack, the attacker has to bypass low quality authentication controls, such as password or PIN. Example:

- To obtain user privileges and establish live session, the attacker has to brute force 8-characters password.

High – to obtain privileges required for the attack, the attacker has to bypass high quality authentication controls, such as Multifactor Authentication or x509 digital certificate. Example:

- To obtain admin privileges and establish live session, attacker has to successfully overcome multifactor authentication barrier (i.e., obtain password of high complexity, phone and approval for strong second factor such as push notifications)

User Interactions (UI)

None – For the attack to succeed, the attacker doesn't have to interact with the target application at the moment of the attack. Examples:

Brute force attack on application password, which is not protected against this type of the attack.
Required – For the attack to succeed, attacker must interact with the target application at the moment of the attack. Examples:

- Cross-site request forgery (CSRF) attack
- Insertion of USB drive that contains a malware

Impact Type (XIT):

Original CIA (XCIA):

The definitions for Confidentiality (None, Low, High), Integrity (None, Low, High) and Availability (None, Low, High) fully match those from CVSS 3.1. This impact profile was left in place as-is to enable risk calculations for:

- Re-scoring post-market risks identified by pen testing or vulnerability scans, taking context of the system into consideration.
- Ability to calculate risk using more familiar ways for expressing impact and allow using this calculator for non-healthcare organizations as well to assess cybersecurity risk associated with a non-medical software product.

Patient Safety (XPS):

The definition of patient safety impact (Negligible, Limited, Moderate, Major, Critical) should be matching organizational ones to enable calculation of patient safety cybersecurity risk following schema

introduced by **FDA in 2016 Cybersecurity Postmarket Guidance** (**Exploitability * Severity of Harm**). Following definitions are introduced as a potential equalizer:

Negligible – No illness or injury to patient or user. Inconvenience to use. Labeling issues not impacting expiration date, product size. No effect on product performance, but product may be exchanged prior to use (e.g., cosmetic issues).

Limited – May cause transient, self-limiting illness or injury to patient or user (e.g., delay in procedure)

Moderate – May cause recoverable injury to patient or user (e.g., unintended treatment).

Major – May cause permanent or significant disability or severe illness in a patient or user that requires treatment but is not likely to result in death (e.g., myocardial infarction, stroke)

Critical –Potential for death, failure of the device or procedure likely to lead to patient or user death. (e.g., perforation of aorta)

Sensitive Data (XSD):

The sensitive data impact profile is in place to evaluate the impact in risk of potentially losing sensitive data on the system. Key definitions introduced:

Secondary Personal Identifiers **–** personal identifiers, which are listed as such under HIPAA, but can't be by itself utilized to definitively identify the person, without having access to additional information such as hospital database. Examples:

- Age
- Data of the procedure

Primary Personal Identifiers - personal identifiers, which are listed as such under HIPAA, and can be by itself utilized to definitively identify the person, without having access to hospital database, but having access to online search tools. Examples:

- First and Last name

None – none of the personal identifiers were lost.

Less than 10,000 (SL) – Less than 10,000 of secondary personal identifiers were lost.

More than 10,000 (SG) – More than 10,000 of secondary personal identifiers were lost.

Less than 10,000 (PL) – Less than 10,000 of primary personal identifiers were lost.

More than 10,000 (PG) – More than 10,000 of primary personal identifiers were lost.

Hospital Breach (XHB):

The hospital breach impact profile is in place to evaluate the risk and potential impact of an attacker exploiting a vulnerable medical device (the "channel") as a pivot point to launch a cybersecurity attack on a hospital.

None – the risk of hospital breach is not elevated by presence in hospital of the evaluated software medical product.

Device Availability (DA) – potential attack can make evaluated medical software product not available for use. Example:

- Device can be successfully DoS'ed

Network Access (NA) – attacker can obtain access to hospital network using device as a pivot point. Example:

- Attacker obtains sufficient privileges on the compromised device to connect to hospital network and attempt to DoS/MITM existing connections or mount an attack on other connected nodes on the affected subnet.

User Impersonation (UI) – attacker can compromise and start impersonating legitimate hospital user, utilizing evaluated software product as a pivot point. Example:

As the evaluated medical software product is installed on a hospital corporate PC, an attacker was able to obtain enough privileges to record hospital user credentials and start an attack on hospital network, moving laterally (through Office365, mounted SMB shares, etc.)