2023 IEEE International Students' Conference on Electrical, Electronics and Computer Science

A Threat modeling approach to analyze and mitigate WhatsApp attacks: A Review

1st Pawan Kumar Patidar
Dept. of Computer Science Engineering
Maulana Azad National Institute of Technology
Bhopal, INDIA
212112214@stu.manit.ac.in

2nd Dr. Deepak Singh Tomar
Dept. of Computer Science Engineering
Maulana Azad National Institute of Technology
Bhopal, INDIA
deepaktomar@manit.ac.in

3rd Dr. R.K. Pateriya
Dept. of Computer Science Engineering
Maulana Azad National Institute of Technology
Bhopal, INDIA
pateriyark@manit.ac.in

4th Mr. Yogesh Kumar Sharma
Dept. of Computer Science Engineering
Maulana Azad National Institute of Technology
Bhopal, INDIA
yogesh.cse1984@gmail.com

2023 IEEE International Students' Conference on Electrical, Electronics and Computer Science (SCEECS) | 979-8-3503-9874-8/23/$31.00 ©2023 IEEE | DOI: 10.1109/SCEECS57921.2023.10062984

***Abstract*—One of the most popularly used features on smartphones is WhatsApp. It is a free messaging app available for Android, IOS, and all other smartphones.A WhatsApp vulnerability is a hole or a weakness in the app, which can be a design flaw or an implementation bug. Through bug, an attacker can enter into the app and cause harm to the database of an application. A database contains private information like backup files, chatting information, contacts, etc. The most dangerous vulnerability in WhatsApp are Authentication, Account Hijacking, and Message Manipulation. In these vulnerabilities, an attacker can manipulate the message but not hijack the entire account. There are some basic requirements for a secure and privacy-preserving chat service, database backup, encrypted database, etc. The awareness about the vulnerability of WhatsApp and its security settings in new versions of WhatsApp. Use WhatsApp security features and secure the services of the application.This paper aims to be aware of the risks and vulnerabilities of WhatsApp and use the Threat modeling method to mitigate its vulnerability. It used threat Modelling steps to help organizations to quantify risks and vulnerabilities, ensuring those that need the most attention and resources do so to minimize their attack surface in a purposeful way.**

***Index Terms*—WhatsApp, Vulnerabilities, Security Threat Modelling, Database Security, Backup, Cryptography.**

I. Introduction

Communication is a process of connecting people to exchange facts, impressions, feelings, or ideas. A communication system requires three things sender, receiver, and medium. In today's world, several mediums are present to conduct effective communication [2]. Due to technology, a new communication medium is known as wireless communications. Mobile phones are used for wireless communication to send and receive audio, video, or text messages across the world using wireless connections of service providers [1].

WhatsApp is a cross-platform instant messaging application available for Symbian, Asha, Windows Mobile, Android, iOS, and Blackberry operating systems. WhatsApp was developed in 2009 by Brian Acton and Jan Koum and was acquired by Facebook in 2014. WhatsApp can auto-sync to the phone address book allowing unlimited messages to the contacts using the WhatsApp application. Messages also include attachments to share multimedia like audios, videos, locations, images, etc. WhatsApp has started calling features to the contacts using the WhatsApp application [8].

The three main aspects of security are Confidentiality, Integrity, and Availability. A new version of WhatsApp contain various security settings which mitigate the vulnerability of Confidentiality, Integrity and Availability. Apply Threat modeling on WhatsApp application to mitigate the threat as well as validate that threat has been mitigated.

II. Versions of WhatsApp

There are various new versions of Whatsapp which are not safe like GB WhatsApp, YOWhatsApp, etc. also called Modded apps. These WhatsApp applications are dilated on the internet and they provide some new features which are generally not present in official WhatsApp. These versions are WhatsApp are not safe to use even though they promise to provide great features time to time. WhatsApp warned people of the risk of temporarily getting banned for using such versions. Most used WhatsApp versions that are not secure.

A. YOWhatsApp

It is just a modified version of WhatsApp, which was developed by Yousef al-Basha after it was handed over for development work to Fouad Mokdad. It has various new features and modifications which are missing from the official version, like hidden status, reading the message, ICONS, privacy modules, etc.

B. FMWhatsApp

FM WhatsApp latest version brings many new features and improvements and supports a lot of Android devices.The following are the breakdown of the top FM WhatsApp features:

979-8-3503-9874-8/23/$31.00 ©2023 IEEE

- Theme can be changed with many options.
- Can modify Universal page, Home page and Chat page.
- There is a floating action button function.
- Send high-resolution images up to 50MB. So that the quality of the photo is not reduced.
- Send photos from gallery as 90 images at once.
- Send video files up to 700MB, etc.

C. OGWhatsApp

OGWhatsApp used some features of OGWhatsApp Pro, which make this application more enjoyable, personal, and interesting. Following are the various features of OGWhatsApp.

- Use more than one WhatsApp account on single device.
- Change the color and background of the unread message counter in the chat window.
- Customize contacts by setting specific text colors for status, unread messages and names.
- Organize photos in and out of conversations.

D. GBWhatsApp MiNi

GB WhatsApp, also called as GBWA, is the clone of original WhatsApp, which provides more functions.It also have some extra features of GB WhatsApp that are not available in the official version.

- Manage multiple accounts.
- Customizable themes for totally free.
- Privacy options: Users can decide on whether to hide these privacy settings or not.
- Undo multiple messages.
- Videos over 50mb can be sent.

III. Vulnerabilities of WhatsApp

A WhatsApp vulnerability is a hole or a weakness in the app, which can be a design flaw or an implementation bug. Through bug, an attacker can enter into the app and cause harm to the database of an application. A database contains private information like backup files, chatting information, contacts, etc. Mainly attacker used four main vulnerabilities for the attack [15].

A. WhatsApp Web Malware

The most obvious target of cybercriminals on WhatsApp is the WhatsApp web. Now WhatsApp has allowed user's to open a website, or download a desktop application, by scanning the code with the app on the phone and using WhatsApp on browser. Hackers, criminals, and scammers have taken advantage of this. They used to pass off malicious software such as WhatsApp desktop applications. If user unfortunate enough to have downloaded one of these, it can distribute malware or otherwise compromise the computer.

Another approach is to create phishing websites and try to handle personal information, like masquerade as WhatsApp Web, asking for to enter phone number and connect to the service. However, they used that number to bombard us with spam and correlate it with other leaked or hacked data on the internet.

B. Unencrypted Backups

WhatsApp used an end-to-end encrypted technique, this means only the sender and receiver have decoded data. This feature prevents user's messages by an attacker or other persons. The backup file which is stored in Google Drive or iCloud is not necessarily encrypted. Nowadays WhatsApp's new version used an security feature to encrypt backup data of WhatsApp.

C. Exporting WhatsApp Chats

This attack requires physical access to user smartphone, only for a few seconds. This gives enough time to export messages to the other location, which is later accessed. The location could be anything i.e. an email account, cloud storage, or even a messaging app.

D. Media File Jacking

In this attack, an attacker tries to fetch the details of WhatsApp application from the database. If files will be saved in internal storage then only the app has permission to access the data but if data is stored in external memory then it is accessible by all the applications of mobile. This feature is used by attackers to send malware by link, other applications, etc. It used the database of WhatsApp, and try to manipulate the data like images, payments, etc.

Recent attack on WhatsApp: Timing of 2019 WhatsApp-NSO Hack in India Validates Leaked Database Accessed by Pegasus Project:

- About Pegasus : Pegasus is a Spyware which is developed by an Israeli cyber-arm company, which is ruined by NSO group that can be installed on mobile phones, mostly on IOS and Android versions. It is capable of reading text messages, tracking calls, location tracking, collecting passwords, accessing the device's camera and microphone, and harvesting information from apps.it calls as a Pegasus based on a Trojan horse virus that can be sent "flying through the air" to infect cell phones. It have an permission to after install the virus it just delete all the files from documents or download.
  For example:
  import os
  write malicious code here
  os.remove('filename.py')
- Working of Pegasus :An earlier version of the virus was installed on the smartphone by clicking a suspicious link or opening a document that secretly install the infected software.
  1) In 2019, Pegasus users install the software on smartphones with missed voice call feature of WhatsApp.
  2) It can able to delete the record of a missed call, It can theoretically harvest the data from the user device and simply send it back to the attacker without any users notification.
  3) It can steal recordings, location records, videos, audio, photos, call logs, and social media posts.

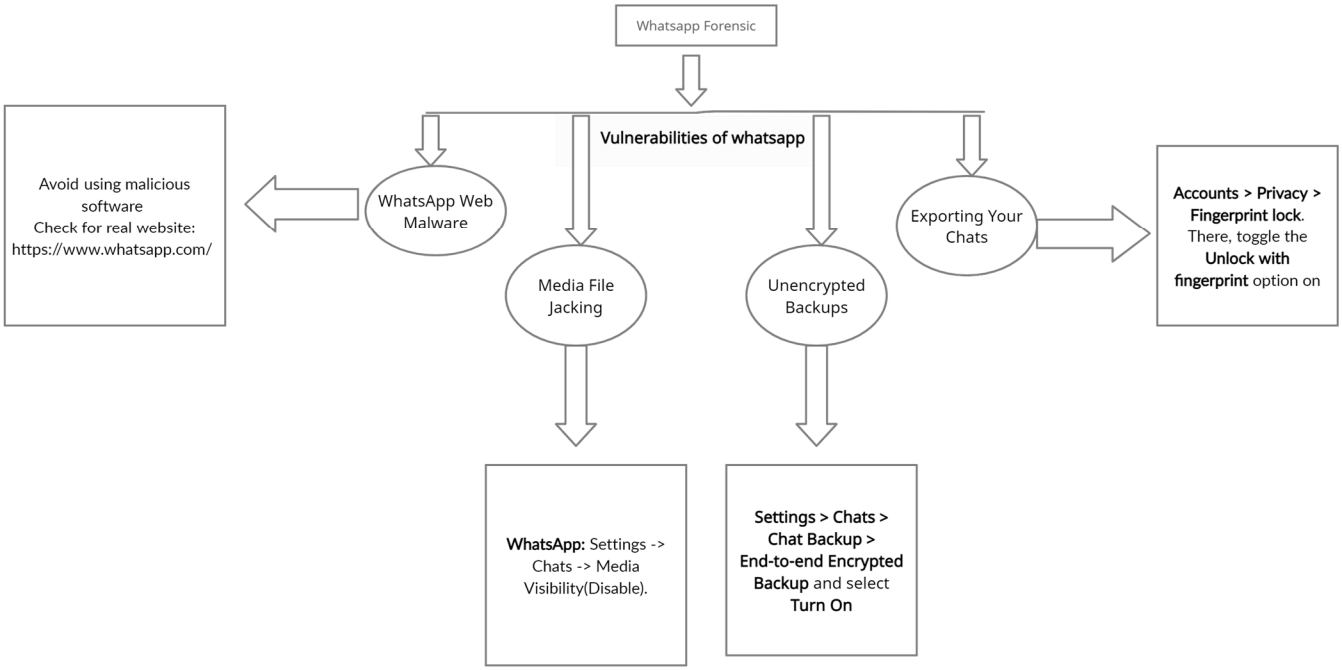

Fig. 1. Vulnerabilities and its secure solutions

4) It has permission to use a microphone and cameras for real-time surveillance without the permission or knowledge of the user.

IV. Possible solutions for vulnerabilities in WhatsApp

Various vulnerability management solutions for WhatsApp are considered i.e., to identify the security level of WhatsApp and maintain it. During WhatsApp settings, it used security settings of encrypted chat, end-to-end encryption, backup facility, etc. The most common settings which are given by WhatsApp are identified and shown in figure -1

A. Defining security requirements

- Privacy and Security : Due to which an WhatsApp build end-to-end encryption into the app. Which encrypt messages, photos, videos, voice messages, documents, calls and status updates are secured from falling into the wrong hands [12].
- Personal Messaging: WhatsApp used end-to-end encryption when chatting with another person. It ensures that only the sender and receiver can read or listen to what to send, and nobody in between, not even WhatsApp. Through end-to-end encryption, messages are secured with a lock, only the recipient has a special key to unlock and read them. This process happens automatically, no need to do additional settings on WhatsApp.
- Business Messaging: WhatsApp used the Bussiness app to manage and store customer messages themselves to be end-to-end encrypted. Once the message is received, it is subject to the business's privacy practices. In business prospective Meta(Facebook) is the parents company of WhatsApp. Over billions of people use Facebook to connect and share their images, document, videos etc.
- Payments: WhatsApp introducing a new and safe payment method through UPI. It is very simple to use payment method, just open the chat action sheet, placing a dedicated button on the chat bar.

B. Creating an application diagram

An application diagram contain an profile information, profile services(API), chat server, mapping database, group service, last seen service, message storage server and store temp message DB, media type messages etc. These are some applications of WhatsApp which are used by old versions of WhatsApp. A new versions of WhatsApp contain new application features like payment through UPI, status and its database. More applications of new version of WhatsApp are identified and shown in figure -**??**

C. Identifying threats

It contains various threats through which an attacker possesses the android and IOS devices.Following are the common threats like:

- WhatsApp Web Malware
- Unencrypted Backups
- Facebook Data Sharing
- Hoaxes and Fake News
- WhatsApp Status
- Exporting Your Chats
- Media File Jacking

D. Mitigating threats

Some of the most common vulnerabilities which are mitigated by the settings of WhatsApp and through awareness about the WhatsApp. Basic security solutions which are used to mitigate the threat listed in given points are:

- Use the latest updated versions of WhatsApp.
- Avoid using other WhatsApp versions which are not certified.
- Avoid installing harmful applications.
- Use all security settings of WhatsApp.

E. Validating that threats have been mitigated

Most security controls are used to prevent the infection point of WhatsApp. Despite all the preventative controls, malware find a way to infect the system. Some protections are built to place limits on malware that gets on the application.

Mitigation of threat is a process to reduce the extent of a problem or an attack by containing a threat until the problem can be correct. It contain ten points to mitigate the threats which is shown in figure- 2

- Auditing and Logging: Whatsapp is connected to a phone number. Typically installed on phone. It verify the user's number. That phone belongs to just one person. Hence the app also belongs to just one person.
- Authentication: The authentication feature of WhatsApp is a process of determining whether someone is authorized to access the application or not. Authentication technology provides access control for an app by matching the input credentials to the database of an authorized user or in the data authentication server. Authentication assures secure data, chats, audio, video, status, etc. WhatsApp used two feature to authenticate the user i.e.
  1) Enable two-step verification: Open WhatsApp settings, tap to account and verify it by two step verification process. It contain an six digit PIN of user's choice and confirm it,additionally it require an email address which helps safeguard your account.
  2) Add an email address: Open WhatsApp settings, tap to account, two-step verification, and add email address which will be used to recover the PIN or safeguard the account.
- Authorization: Authorization is the process to permit another user to access the resource. WhatsApp authorization is related to identity. Users have their mobile numbers and email IDs to identify the person. There are various identity options which are listed below:
  1) Registration: To confirm the phone number, enter 6-digit registration code send on registered SMS or phone call. Registration code is verified by phone number, it is only way to activate the account by receive the code on phone.
  2) 2-step Verification: After successful register email and phone number on WhatsApp. Two step verification is an process by which an PIN will be generated which is required to access the account.
- Communication Security: Modern technology of WhatsApp provides various options for communicating in the application. It include voice call, video call, status, group messaging etc.This guidance contains a set of principles that can help an application to make secure decisions when selecting any fetures that provide secure communication. For secure communication WhatsApp use various technique which are listed below:
  1) WhatsApp uses end-to-end encryption
  2) WhatsApp does not store messages on their servers
  3) WhatsApp does not keep call detail records
  4) WhatsApp has strict rules for businesses that want to use their services
  5) The WhatsApp Business API offers the same level of security as the app
- Configuration Management: It used some common features to manage the configuration such as:
  1) WhatsApp uses end-to-end encryption to configuration management.
  2) It used a safe path to store the database i.e. Internal Storage → *Android* → *Media* → *com.whatsapp* → *WhatsApp* → *Databases*
- Cryptography: Every WhatsApp message is protected by the encryption protocol that secure messages before they leave your device. It used an cryptographic techinque to encrypt and decrypt the message [3], to secure data by third person. For this it used AES message encryption and decryption method [10].
- Exception Management: WhatsApp used various exceptions, which is managed by the awarness of WhatsApp. It contain some security options to manage the exception which are listed below:
  1) WhatsApp might have deleted your account.
  2) Make sure you have a solid wireless connection.
  3) Restart WhatsApp.
  4) Check to see if WhatsApp is down.
  5) Restart your phone
  6) Make sure WhatsApp is up to date.
  7) Clear your cache.
- Input Validation: To insure that the input credential is validate or not. It used phone number in database belongs to a valid account, it ensure that the status is valid before send the message. It used various features to validate the input credentials which are listed below:
  1) WhatsApp uses end-to-end encryption.
  2) Database Security: Go to Settings → *Chats* → *ChatBackup* → *End − to − endEncryptedBackup*
- Sensitive Data: Data send on WhatsApp are sensitive data or personal data, if any integrity is performed between the communication then data leakage problem is there. To avoid the data leakage problem and make sensitive data secure WhatsApp use an data encryption technique which are listed below:

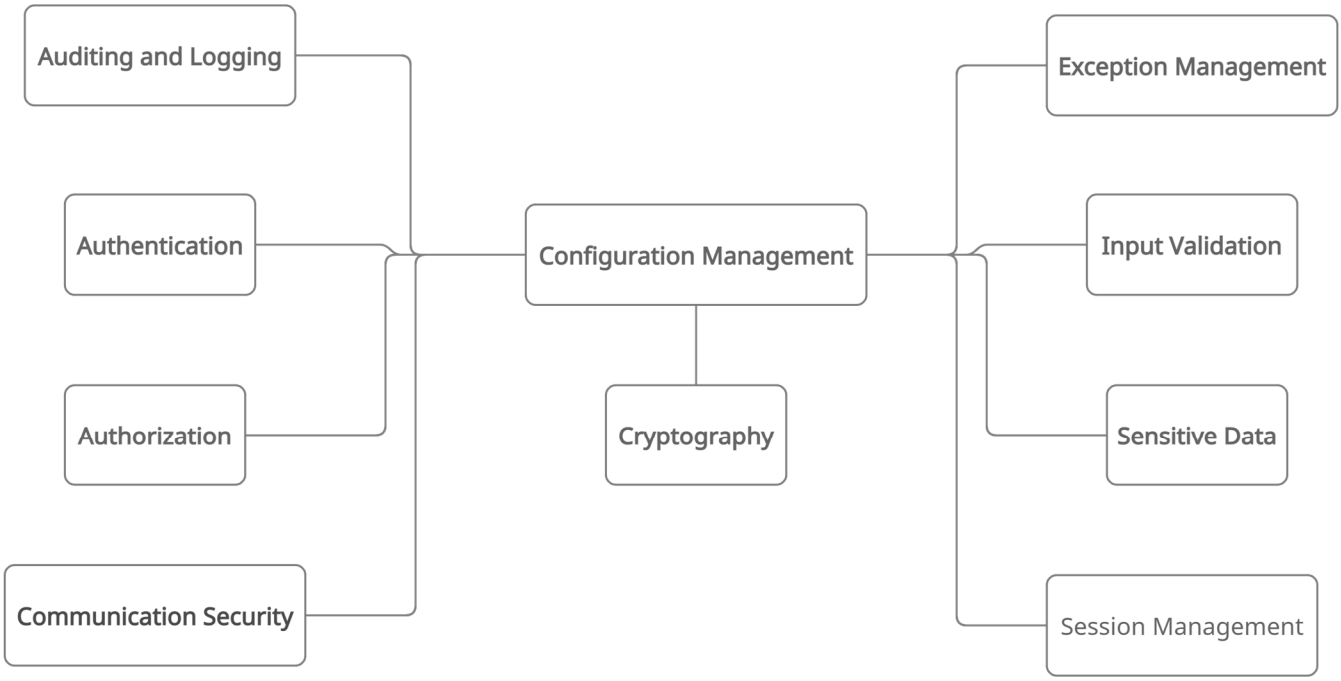

Fig. 2. Validating that threats have been mitigated

1) WhatsApp currently uses AES256 in CBC mode for encryption and HMAC-SHA256 for authentication [10].
2) Uses Curve25519 for key exchange and AES256 in CBC mode for message encryption and uses HMAC-SHA256 for message authenticity and integrity [10].

- Session Management: Session is just like an website in which an variable is store while building a chatbot on WhatsApp. It used to manage an session as the user continually interacts with the chatbot. Session managment techniques of WhatsApp are:
  1) Use database to sort of simulate a session management for chatbots.
  2) For WhatsApp, use the phone number as the 'session-id' then map this 'session-id' to a 'data' field that's contain everything that want to store for the particular user.

CONCLUSION

In this paper, various types of WhatsApp versions and their security patches are discussed. It is all about the awareness of WhatsApp and using the threat modeling method to validate that threat has been mitigated. A recent attack on WhatsApp and its security option which are updated by WhatsApp are also presented. A WhatsApp contains various vulnerabilities for which security solutions are provided in the setting of WhatsApp.A threat modeling method is developed that helps to identify the security requirements of a system or process. It is a structured process that aims to identify threats and their vulnerabilities to reduce the risk to IT resources.Using Threat modeling in WhatsApp reduce the attack surface on application, It used to identifies and eliminates single points of failure. In future, our aim to identify more techniques to mitigate the WhatsApp attacks, Threat Modelling is one of the technique which is generally used to mitigate the attacks but we try to find the technique which prove the threat will be mitigated with more accuracy.

REFERENCES

[1] "REVEALED: Top uses of our smartphones - and calling doesn't even make the list," 2017. [Online]. Available: revealed: Top uses of our smartphones - and calling doesn't even make the list[Accessed: 10-Nov-2017]
[2] T. Sutikno, L. Handayani, D. Stiawan, M. A. Riyadi, and I. M. I. Subroto, "WhatsApp, viber and telegram: Which is the best for instant messaging?," Int. J. Electr. Comput. Eng., vol. 6, no. 3, pp. 909–914, 2016.
[3] J. Koum and B. Acton, "End-to-end encryption," 2016. [Online]. Available: https://blog.whatsapp.com/10000618/end-to-end-encryption. [Accessed: 10-Nov-2017].
[4] D. Goodin. (2014, February) Crypto Weaknesses in WhatsApp "The Kind of Student the NSA would Love'. Online. ARS Technica.
[5] Everyday dwelling with WhatsApp. In Proceedings of the 17th ACM conference on Computer supported cooperative work social computing (pp. 1131-1143). (Accessed on 2nd April, 2018).
[6] Katriel Cohn-Gordon, Cas Cremers, Luke Garratt, Jon Millican, Kevin Milner, "On Ends-to-Ends Encryption", Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security, pp.1802, 2018.

[7] Exploring User's Perception of Storage Management Features in Instant Messaging Applications: A Case on WhatsApp Messenger Mashael M. Alsulami;Arwa Y. Al-Aama 2019 2nd International Conference on Computer Applications Information Security (ICCAIS)
[8] The Security Analysis of Popular Instant Messaging Applications Lijun Zhang;Qingbing Ji;Fei Yu 2017 International Conference on Computer Systems, Electronics and Control (ICCSEC)
[9] FaceLock Homes: A Contactless Smart Home Security System to Prevent COVID Transmission Krish Sethi;Simrit Kaul;Ishan Patel;Sujatha R. 2021 Sixth International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET)
[10] Design and Implementation of AES and SHA-256 Cryptography for Securing Multimedia File over Android Chat Application Noveline Aziz Fauziah;Eko Hari Rachmawanto;De Rosal Ignatius Moses Setiadi;Christy Atika Sari 2018 International Seminar on Research of Information Technology and Intelligent Systems (ISRITI)
[11] Understanding User Tradeoffs for Search in Encrypted Communication Wei Bai;Ciara Lynton;Charalampos Papamanthou;Michelle L. Mazurek 2018 IEEE European Symposium on Security and Privacy (EuroSP)
[12] Is WhatsApp Plus Malicious? A Review Using Static Analysis Rizaldi Wahaz;Rakha Nadhifa Harmana;Amiruddin Amiruddin;Ardya Suryadinata 2021 6th International Workshop on Big Data and Information Security (IWBIS)
[13] A threat risk estimation model for computer network security Razieh Rezaee;Abbas Ghaemi Bafghi;Masoud Khosravi-Farmad 2016 6th International Conference on Computer and Knowledge Engineering (ICCKE)
[14] Efficient and effective security model for database specially designed to avoid internal threats Aditya A. Shastri;P.N. Chatur 2015 International Conference on Smart Technologies and Management for Computing, Communication, Controls, Energy and Materials (ICSTM)
[15] IEEE/ISO International Standard-Health informatics–Device interoperability–Part 40101: Foundational–Cybersecurity–Processes for vulnerability assessment ISO/IEEE 11073-40101:2022(E)