The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

TLP: WHITE
www.cisa.gov/tlp
Information may be distributed without restriction, subject to standard copyright rules.

DATE(S) ISSUED:
03/15/2022

SUBJECT:
Multiple Vulnerabilities in Apple Products Could Allow for Arbitrary Code Execution

OVERVIEW:
Multiple vulnerabilities have been discovered in Apple Products, the most severe of which could allow for arbitrary code execution.

- GarageBand is an audio tool
- iOS is a mobile operating system for mobile devices, including the iPhone, iPad, and iPod touch.
- iPadOS is the successor to iOS 12 and is a mobile operating system for iPads.
- Logic Pro X is a digital audio workstation
- macOS Monterey is the 18th and current major release of macOS.
- macOS Big Sur is the 17th release of macOS.
- macOS Catalina is the 16th major release of macOS
- watchOS is the mobile operating system for Apple Watch and is based on the iOS operating system.
- tvOS is an operating system for fourth-generation Apple TV digital media player.
- Xcode is Apple's integrated development environment for macOS

Successful exploitation of the most severe of these vulnerabilities could result in arbitrary code execution within the context of the application, an attacker gaining the same privileges as the logged-on user, or the bypassing of security restrictions. Depending on the permission associated with the application running the exploit, an attacker could then install programs; view, change, or delete data

THREAT INTELLIGENCE:
There are currently no reports of these vulnerabilities being exploited in the wild.

SYSTEMS AFFECTED:
- GarageBand prior 10.4.6
- iOS and iPadOS prior to 15.3

- Logic Pro X prior to 10.7.3
- macOS Monterey prior to 12.2
- macOS Big Sur prior to 11.6.3
- macOS Catalina prior to security update 2022-001
- watchOS prior to 8.4
- tvOS prior to 15.3
- Xcode prior to 13.3

RISK:

Government:

- Large and medium government entities: **High**
- Small government entities: **Medium**

Businesses:

- Large and medium business entities: **High**
- Small business entities: **Medium**

Home users: Low

TECHNICAL SUMMARY:
Multiple vulnerabilities have been discovered in Apple Products, the most severe of which could allow for arbitrary code execution in the context of the affected user. Details of these vulnerabilities are as follows:

GarageBand 10.4.6

- Opening a maliciously crafted file may lead to unexpected application termination or arbitrary code execution (CVE-2022-22657, CVE-2022-22664)

iOS and iPadOS 15.4

- Opening a maliciously crafted PDF file may lead to an unexpected application termination or arbitrary code execution (CVE-2022-22633)
- Processing a maliciously crafted image may lead to heap corruption (CVE-2022-22666)
- A malicious application may be able to execute arbitrary code with kernel privileges (CVE-2022-22634)
- An application may be able to gain elevated privileges (CVE-2022-22635)
- An application may be able to execute arbitrary code with kernel privileges (CVE-2022-22636)
- A person with physical access may be able to view and modify the carrier account information and settings from the lock screen (CVE-2022-22652)
- An app may be able to learn information about the current camera view before being granted camera access (CVE-2022-22598)
- A user may be able to bypass the Emergency SOS passcode prompt (CVE-2022-22642)

- A user may send audio and video in a FaceTime call without knowing that they have done so (CVE-2022-22643)
- An application may be able to execute arbitrary code with kernel privileges (CVE-2022-22667)
- Processing a maliciously crafted image may lead to arbitrary code execution (CVE-2022-22611)
- Processing a maliciously crafted image may lead to heap corruption (CVE-2022-22612)
- An application may be able to gain elevated privileges (CVE-2022-22641)
- A malicious website may be able to access information about the user and their devices (CVE-2022-22653)
- An application may be able to execute arbitrary code with kernel privileges (CVE-2022-22596, CVE-2022-22640)
- An application may be able to execute arbitrary code with kernel privileges (CVE-2022-22613)
- An application may be able to execute arbitrary code with kernel privileges (CVE-2022-22614, CVE-2022-22615)
- A malicious application may be able to elevate privileges (CVE-2022-22632)
- An attacker in a privileged position may be able to perform a denial of service attack (CVE-2022-22638)
- Multiple issues in libarchive (CVE-2022-22622)
- A malicious application may be able to identify what other applications a user has installed (CVE-2022-22670)
- An attacker in a privileged network position may be able to leak sensitive user information (CVE-2022-22659)
- A user may be able to bypass the Emergency SOS passcode prompt (CVE-2022-22618)
- A malicious application may be able to read other applications' settings (CVE-2022-22609)
- A malicious application may be able to bypass certain Privacy preferences (CVE-2022-22600)
- A person with physical access to a device may be able to use Siri to obtain some location information from the lock screen (CVE-2022-22599)
- An application may be able to gain elevated privileges (CVE-2022-22639)
- A person with physical access to an iOS device may be able to see sensitive information via keyboard suggestions (CVE-2022-22621)
- A person with physical access to an iOS device may be able to access photos from the lock screen (CVE-2022-22671)
- Processing maliciously crafted web content may disclose sensitive user information (CVE-2022-22662)
- Processing maliciously crafted web content may lead to code execution (CVE-2022-22610)
- Processing maliciously crafted web content may lead to arbitrary code execution (CVE-2022-22624, CVE-2022-22628, CVE-2022-22629)
- A malicious website may cause unexpected cross-origin behavior (CVE-2022-22637)
- A malicious application may be able to leak sensitive user information (CVE-2022-22668)

Logic Pro X 10.7.3

- Opening a maliciously crafted file may lead to unexpected application termination or arbitrary code execution (CVE-2022-22657, CVE-2022-22664)

MacOS Monterey 12.3

- Opening a maliciously crafted PDF file may lead to an unexpected application termination or arbitrary code execution (CVE-2022-22633)
- An application may be able to execute arbitrary code with kernel privileges (CVE-2022-22669)
- A malicious application may be able to gain root privileges (CVE-2022-22665)
- An application may be able to gain elevated privileges (CVE-2022-22631)
- Processing a maliciously crafted AppleScript binary may result in unexpected application termination or disclosure of process memory (CVE-2022-22625)
- An application may be able to read restricted memory (CVE-2022-22648)
- Processing a maliciously crafted AppleScript binary may result in unexpected application termination or disclosure of process memory.(CVE-2022-22626, CVE-2022-22627)
- Processing a maliciously crafted file may lead to arbitrary code execution (CVE-2022-22597)
- A maliciously crafted ZIP archive may bypass Gatekeeper checks (CVE-2022-22616)
- Multiple issues in curl (CVE-2021-22946, CVE-2021-22947, CVE-2021-22945, CVE-2022-22623)
- A user may send audio and video in a FaceTime call without knowing that they have done so (CVE-2022-22643)
- Processing a maliciously crafted image may lead to arbitrary code execution (CVE-2022-22611)
- Processing a maliciously crafted image may lead to heap corruption (CVE-2022-22612)
- An application may be able to execute arbitrary code with kernel privileges (CVE-2022-22661)
- An application may be able to gain elevated privileges (CVE-2022-22641)
- An application may be able to execute arbitrary code with kernel privileges (CVE-2022-22613)
- An application may be able to execute arbitrary code with kernel privileges (CVE-2022-22614, CVE-2022-22615)
- A malicious application may be able to elevate privileges (CVE-2022-22632)
- An attacker in a privileged position may be able to perform a denial of service attack (CVE-2022-22638)
- An application may be able to execute arbitrary code with kernel privileges (CVE-2022-22640)
- Multiple issues in libarchive (CVE-2021-36976)
- A person with access to a Mac may be able to bypass Login Window (CVE-2022-22647)
- A local attacker may be able to view the previous logged in user’s desktop from the fast user switching screen (CVE-2022-22656)
- Opening a maliciously crafted file may lead to unexpected application termination or arbitrary code execution (2022-22657)

- Opening a maliciously crafted file may lead to unexpected application termination or arbitrary code execution (CVE-2022-22664)
- A malicious application may be able to access information about a user's contacts (CVE-2022-22644)
- An application may be able to gain elevated privileges (CVE-2022-22617)
- A malicious application may be able to read other applications' settings (CVE-2022-22609)
- A plug-in may be able to inherit the application's permissions and access user data (CVE-2022-22650)
- A maliciously crafted ZIP archive may bypass Gatekeeper checks (CVE-2022-22616)
- A malicious application may be able to bypass certain Privacy preferences (CVE-2022-22600)
- A person with physical access to a device may be able to use Siri to obtain some location information from the lock screen (CVE-2022-22599)
- A remote attacker may be able to cause unexpected system termination or corrupt kernel memory (CVE-2022-22651)
- An application may be able to gain elevated privileges (CVE-2022-22639)
- An app may be able to spoof system notifications and UI (CVE-2022-22660)
- A person with physical access to an iOS device may be able to see sensitive information via keyboard suggestions (CVE-2022-22621)
- Multiple issues in Vim (CVE-2021-4136, CVE-2021-4166, CVE-2021-4173, CVE-2021-4187, CVE-2021-4192, CVE-2021-4193, CVE-2021-46059, CVE-2022-0128, CVE-2022-0156, CVE-2022-0158)
- A user may be able to view restricted content from the lock screen (CVE-2021-30918)
- Processing maliciously crafted web content may disclose sensitive user information (CVE-2022-22662)
- Processing maliciously crafted web content may lead to code execution (CVE-2022-22610)
- Processing maliciously crafted web content may lead to arbitrary code execution (CVE-2022-22624, CVE-2022-22628, CVE-2022-22629)
- A malicious website may cause unexpected cross-origin behavior (CVE-2022-22637)
- A malicious application may be able to leak sensitive user information (CVE-2022-22668)
- A local user may be able to write arbitrary files (CVE-2022-22582)

MacOS Big Sur 11.6.5

- Opening a maliciously crafted PDF file may lead to an unexpected application termination or arbitrary code execution (CVE-2022-22633)
- An application may be able to gain elevated privileges (CVE-2022-22631)
- An application may be able to read restricted memory (CVE-2022-22648)
- Processing a maliciously crafted AppleScript binary may result in unexpected application termination or disclosure of process memory.(CVE-2022-22626, CVE-2022-22627)
- Processing a maliciously crafted AppleScript binary may result in unexpected application termination or disclosure of process memory. (CVE-2022-22625)

- Processing a maliciously crafted file may lead to arbitrary code execution (CVE-2022-22597)
- A maliciously crafted ZIP archive may bypass Gatekeeper checks (CVE-2022-22616)
- An application may be able to execute arbitrary code with kernel privileges (CVE-2022-22661)
- An application may be able to execute arbitrary code with kernel privileges (CVE-2022-22613)
- An application may be able to execute arbitrary code with kernel privileges (CVE-2022-22614, CVE-2022-22615)
- An attacker in a privileged position may be able to perform a denial of service attack (CVE-2022-22638)
- A malicious application may be able to elevate privileges (CVE-2022-22632)
- A person with access to a Mac may be able to bypass Login Window (CVE-2022-22647)
- A local attacker may be able to view the previous logged in user’s desktop from the fast user switching screen (CVE-2022-22656)
- An application may be able to gain elevated privileges (CVE-2022-22617)
- A plug-in may be able to inherit the application's permissions and access user data (CVE-2022-22650)
- A person with physical access to a device may be able to use Siri to obtain some location information from the lock screen (CVE-2022-22599)
- Processing maliciously crafted web content may disclose sensitive user information (CVE-2022-22662)
- A local user may be able to write arbitrary files (CVE-2022-22582)

MacOS Catalina Security Update 2022-003

- An application may be able to gain elevated privileges (CVE-2022-22631)
- An application may be able to read restricted memory (CVE-2022-22648)
- Processing a maliciously crafted AppleScript binary may result in unexpected application termination or disclosure of process memory.(CVE-2022-22626, CVE-2022-22627)
- Processing a maliciously crafted AppleScript binary may result in unexpected application termination or disclosure of process memory. (CVE-2022-22625)
- Processing a maliciously crafted file may lead to arbitrary code execution (CVE-2022-22597)
- A maliciously crafted ZIP archive may bypass Gatekeeper checks (CVE-2022-22616)
- An application may be able to execute arbitrary code with kernel privileges (CVE-2022-22661)
- An application may be able to execute arbitrary code with kernel privileges (CVE-2022-22613)
- An application may be able to execute arbitrary code with kernel privileges (CVE-2022-22614, CVE-2022-22615)
- An attacker in a privileged position may be able to perform a denial of service attack (CVE-2022-22638)
- A person with access to a Mac may be able to bypass Login Window (CVE-2022-22647)
- A local attacker may be able to view the previous logged in user’s desktop from the fast user switching screen (CVE-2022-22656)

- An application may be able to gain elevated privileges (CVE-2022-22617)
- A plug-in may be able to inherit the application's permissions and access user data (CVE-2022-22650)
- Processing maliciously crafted web content may disclose sensitive user information (CVE-2022-22662)
- A local user may be able to write arbitrary files (CVE-2022-22582)

WatchOS 8.5

- Opening a maliciously crafted PDF file may lead to an unexpected application termination or arbitrary code execution (CVE-2022-22633)
- Processing a maliciously crafted image may lead to heap corruption (CVE-2022-22666)
- Processing a maliciously crafted image may lead to arbitrary code execution (CVE-2022-22611)
- Processing a maliciously crafted image may lead to heap corruption (CVE-2022-22612)
- An application may be able to execute arbitrary code with kernel privileges (CVE-2022-22596, CVE-2022-22640)
- An application may be able to execute arbitrary code with kernel privileges (CVE-2022-22613)
- An application may be able to execute arbitrary code with kernel privileges (CVE-2022-22614, CVE-2022-22615)
- A malicious application may be able to elevate privileges (CVE-2022-22632)
- An attacker in a privileged position may be able to perform a denial of service attack (CVE-2022-22638)
- Multiple issues in libarchive (CVE-2021-36976)
- A malicious application may be able to identify what other applications a user has installed (CVE-2022-22670)
- A user may be able to bypass the Emergency SOS passcode prompt (CVE-2022-22618)
- A malicious application may be able to read other applications' settings (CVE-2022-22609)
- Visiting a malicious website may lead to address bar spoofing (CVE-2022-22654)
- A malicious application may be able to bypass certain Privacy preferences (CVE-2022-22600)
- A person with physical access to a device may be able to use Siri to obtain some location information from the lock screen (CVE-2022-22599)
- A person with physical access to an iOS device may be able to see sensitive information via keyboard suggestions (CVE-2022-22621)
- Processing maliciously crafted web content may disclose sensitive user information (CVE-2022-22662)
- Processing maliciously crafted web content may lead to code execution (CVE-2022-22610)
- Processing maliciously crafted web content may lead to arbitrary code execution (CVE-2022-22624, CVE-2022-22628, CVE-2022-22629)
- A malicious website may cause unexpected cross-origin behavior (CVE-2022-22637)

tvOS 15.4

- Processing a maliciously crafted image may lead to heap corruption (CVE-2022-22666)
- A malicious application may be able to execute arbitrary code with kernel privileges (CVE-2022-22634)
- An application may be able to gain elevated privileges (CVE-2022-22635)
- An application may be able to execute arbitrary code with kernel privileges (CVE-2022-22636)
- Processing a maliciously crafted image may lead to arbitrary code execution (CVE-2022-22611)
- Processing a maliciously crafted image may lead to heap corruption (CVE-2022-22612)
- An application may be able to gain elevated privileges (CVE-2022-22641)
- An application may be able to execute arbitrary code with kernel privileges (CVE-2022-22613)
- An application may be able to execute arbitrary code with kernel privileges (CVE-2022-22614, CVE-2022-22615)
- A malicious application may be able to elevate privileges (CVE-2022-22632)
- An attacker in a privileged position may be able to perform a denial of service attack (CVE-2022-22638)
- An application may be able to execute arbitrary code with kernel privileges (CVE-2022-22640)
- A malicious application may be able to identify what other applications a user has installed (CVE-2022-22670)
- A malicious application may be able to read other applications' settings (CVE-2022-22609)
- A malicious application may be able to bypass certain Privacy preferences (CVE-2022-22600)
- A person with physical access to an iOS device may be able to see sensitive information via keyboard suggestions (CVE-2022-22621)
- Processing maliciously crafted web content may disclose sensitive user information (CVE-2022-22662)
- Processing maliciously crafted web content may lead to code execution (CVE-2022-22610)
- Processing maliciously crafted web content may lead to arbitrary code execution (CVE-2022-22624, CVE-2022-22628, CVE-2022-22629)
- A malicious website may cause unexpected cross-origin behavior (CVE-2022-22637)

Xcode 13.3

- Multiple issues in iTMSTransporter (CVE-2019-14379, CVE-2021-44228)
- Opening a maliciously crafted file may lead to unexpected application termination or arbitrary code execution (CVE-2022-22601, CVE-2022-22602, CVE-2022-22603, CVE-2022-22604, CVE-2022-22605, CVE-2022-22606, CVE-2022-22607, CVE-2022-22608)

Successful exploitation of the most severe of these vulnerabilities could result in arbitrary code execution within the context of the application, an attacker gaining the same privileges as the logged-on user, or the bypassing of security restrictions. Depending on the permission

associated with the application running the exploit, an attacker could then install programs; view, change, or delete data.

RECOMMENDATIONS:
We recommend the following actions be taken:

- Apply appropriate patches provided by Apple to vulnerable systems immediately after appropriate testing.
- Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.
- Remind users not to download, accept or execute files from untrusted and unknown sources.
- Remind users not to visit untrusted websites or follow links provided by untrusted or unknown sources.
- Evaluate read, write, and execute permissions on all newly installed software.
- Apply the Principle of Least Privilege to all systems and services.

REFERENCES:

Apple:

https://support.apple.com/en-us/HT213191
https://support.apple.com/en-us/HT213182
https://support.apple.com/en-us/HT213190
https://support.apple.com/en-us/HT213183
https://support.apple.com/en-us/HT213184
https://support.apple.com/en-us/HT213185
https://support.apple.com/en-us/HT213186
https://support.apple.com/en-us/HT213193
https://support.apple.com/en-us/HT213189

CVE:

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-4136
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-4166
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-4173
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-4187
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-4192
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-4193
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-36976
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-30918
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-46059
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-0128
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-0156
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-0158
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-22582
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-22596

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-22597
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-22598
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-22599
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-22600
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-22609
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-22610
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-22611
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-22612
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-22613
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-22614
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-22615
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-22616
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-22617
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-22618
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-22621
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-22622
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-22623
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-22624
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-22625
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-22626
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-22627
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-22628
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-22629
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-22631
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-22632
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-22633
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-22634
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-22635
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-22636
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-22637
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-22638
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-22639
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-22640
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-22641
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-22642
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-22643
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-22644
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-22645
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-22646
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-22647
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-22648

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-22650
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-22651
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-22652
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-22653
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-22654
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-22656
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-22657
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-22659
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-22660
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-22661
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-22662
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-22664
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-22665
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-22666
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-22667
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-22668
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-22669
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-22670
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-22671