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
https://www.cisa.gov/tlp
Sources may use TLP:WHITE when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.

DATE(S) ISSUED:
12/14/2021

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.

- 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.
- 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.

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 no reports of these vulnerabilities being exploited in the wild.

SYSTEMS AFFECTED:
- iOS and iPadOS prior to 15.2
- macOS Monterey prior to 12.1
- macOS Big Sur prior to 11.6.2
- macOS Catalina prior to security update 2021-008
- watchOS prior to 8.3
- tvOS prior to 15.2

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:

- **iOS 15.2 and iPadOS 15.2**
  - Audio
    - Parsing a maliciously crafted audio file may lead to disclosure of user information. A buffer overflow issue was addressed with improved memory handling. (CVE-2021-30960)
  - CFNetwork Profiles
    - User traffic might unexpectedly be leaked to a proxy server despite PAC configurations. A logic issue was addressed with improved state management. (CVE-2021-30966)
  - ColorSync
    - Processing a maliciously crafted image may lead to arbitrary code execution. A memory corruption issue in the processing of ICC profiles was addressed with improved input validation. (CVE-2021-30926, CVE-2021-30942)
  - CoreAudio
    - Processing a maliciously crafted audio file may lead to arbitrary code execution. A buffer overflow issue was addressed with improved memory handling. (CVE-2021-30957)
    - Playing a malicious audio file may lead to arbitrary code execution. An out-of-bounds read was addressed with improved input validation. (CVE-2021-30958)
  - Crash Reporter
    - A local attacker may be able to elevate their privileges. This issue was addressed with improved checks. (CVE-2021-30945)
  - FaceTime
    - A user in a FaceTime call may unexpectedly leak sensitive user information through Live Photos metadata. This issue was addressed with improved handling of file metadata. (CVE-2021-30992)
  - ImageIO
    - Processing a maliciously crafted image may lead to arbitrary code execution. An out-of-bounds read was addressed with improved bounds checking. (CVE-2021-30939)
  - IOMobileFrameBuffer
    - A malicious application may be able to execute arbitrary code with kernel privileges.
      i. A race condition was addressed with improved state handling. (CVE-2021-30996)
      ii. A buffer overflow issue was addressed with improved memory handling. (CVE-2021-30983)

iii. An out-of-bounds write issue was addressed with improved bounds checking. (CVE-2021-30985)
iv. An out-of-bounds read was addressed with improved bounds checking. (CVE-2021-30991)

- Kernel
  - A malicious application may be able to execute arbitrary code with kernel privileges.
    i. A use after free issue was addressed with improved memory management. (CVE-2021-30937)
    ii. A memory corruption issue was addressed with improved state management. (CVE-2021-30949)
    iii. A race condition was addressed with improved state handling. (CVE-2021-30955)
  - An application may be able to execute arbitrary code with kernel privileges. A use after free issue was addressed with improved memory management. (CVE-2021-30927, CVE-2021-30980)
  - An attacker in a privileged network position may be able to execute arbitrary code. A buffer overflow issue was addressed with improved memory handling. (CVE-2021-30993)
- Model I/O
  - Processing a maliciously crafted USD file may lead to unexpected application termination or arbitrary code execution.
    i. An out-of-bounds write issue was addressed with improved bounds checking. (CVE-2021-30971)
    ii. A buffer overflow issue was addressed with improved memory handling. (CVE-2021-30979)
  - Processing a maliciously crafted file may disclose user information. An out-of-bounds read was addressed with improved input validation. (CVE-2021-30973)
  - Processing a maliciously crafted USD file may disclose memory contents.
    i. An out-of-bounds write issue was addressed with improved bounds checking. (CVE-2021-30929)
    ii. A buffer overflow issue was addressed with improved memory handling. (CVE-2021-30940, CVE-2021-30941)
- NetworkExtension
  - A local attacker may be able to read sensitive information. A permissions issue was addressed with improved validation. (CVE-2021-30967)
  - A malicious application may be able to identify what other applications a user has installed. A permissions issue was addressed with improved validation. (CVE-2021-30988)
- Notes
  - A person with physical access to an iOS device may be able to access contacts from the lock screen. The issue was addressed with improved permissions logic. (CVE-2021-30932)
- Password Manager
  - A person with physical access to an iOS device may be able to access stored passwords without authentication. An inconsistent user interface issue was addressed with improved state management. (CVE-2021-30948)
- Preferences

        - A malicious application may be able to elevate privileges. A race condition was addressed with improved state handling. (CVE-2021-30995)
    - Sandbox
        - A malicious application may be able to bypass certain Privacy preferences.
            i. A validation issue related to hard link behavior was addressed with improved sandbox restrictions. (CVE-2021-30968)
            ii. A logic issue was addressed with improved restrictions. (CVE-2021-30946)
        - An application may be able to access a user's files. An access issue was addressed with additional sandbox restrictions. (CVE-2021-30947)
    - TCC
        - A local user may be able to modify protected parts of the file system. A logic issue was addressed with improved state management. (CVE-2021-30767)
        - A malicious application may be able to bypass Privacy preferences. An inherited permissions issue was addressed with additional restrictions. (CVE-2021-30964)
    - WebKit
        - Processing maliciously crafted web content may lead to arbitrary code execution.
            i. A buffer overflow issue was addressed with improved memory handling. (CVE-2021-30934)
            ii. A use after free issue was addressed with improved memory management. (CVE-2021-30936, CVE-2021-30951)
            iii. An integer overflow was addressed with improved input validation. (CVE-2021-30952)
            iv. A race condition was addressed with improved state handling. (CVE-2021-30984)
            v. An out-of-bounds read was addressed with improved bounds checking. (CVE-2021-30953)
            vi. A type confusion issue was addressed with improved memory handling. (CVE-2021-30954)

- **macOS Monterey 12.1**
    - Airport
        - A device may be passively tracked via BSSIDs. An access issue was addressed with improved access restrictions. (CVE-2021-30987)
    - Archive Utility
        - A malicious application may bypass Gatekeeper checks. A logic issue was addressed with improved state management. (CVE-2021-30950)
    - Audio
        - Parsing a maliciously crafted audio file may lead to disclosure of user information. A buffer overflow issue was addressed with improved memory handling. (CVE-2021-30960)
    - Bluetooth
        - A device may be passively tracked by its Bluetooth MAC address. A device configuration issue was addressed with an updated configuration. (CVE-2021-30986)
    - CFNetwork Proxies

        - User traffic might unexpectedly be leaked to a proxy server despite PAC configurations. A logic issue was addressed with improved state management. (CVE-2021-30966)
    - ColorSync
        - Processing a maliciously crafted image may lead to arbitrary code execution. A memory corruption issue in the processing of ICC profiles was addressed with improved input validation. (CVE-2021-30926, CVE-2021-30942)
    - CoreAudio
        - Processing a maliciously crafted audio file may lead to arbitrary code execution. A buffer overflow issue was addressed with improved memory handling. (CVE-2021-30957)
        - Playing a malicious audio file may lead to arbitrary code execution. An out-of-bounds read was addressed with improved input validation. (CVE-2021-30958)
    - Crash Reporter
        - A local attacker may be able to elevate their privileges. This issue was addressed with improved checks. (CVE-2021-30945)
    - Graphics Divers
        - A malicious application may be able to execute arbitrary code with kernel privileges. A buffer overflow was addressed with improved bounds checking. (CVE-2021-30977)
    - ImageIO
        - Processing a maliciously crafted image may lead to arbitrary code execution. An out-of-bounds read was addressed with improved bounds checking. (CVE-2021-30939)
    - Intel Graphics Driver
        - An application may be able to execute arbitrary code with kernel privileges. A buffer overflow was addressed with improved bounds checking. (CVE-2021-30981)
    - IOMobileFrameBuffer
        - A malicious application may be able to execute arbitrary code with kernel privileges. A race condition was addressed with improved state handling. (CVE-2021-30996)
    - IOUSBHostFamily
        - A remote attacker may be able to cause unexpected application termination or heap corruption. A race condition was addressed with improved locking. (CVE-2021-30982)
    - Kernel
        - A malicious application may be able to execute arbitrary code with kernel privileges.
            i. A memory corruption vulnerability was addressed with improved locking. (CVE-2021-30937)
            ii. A memory corruption issue was addressed with improved state management. (CVE-2021-30949)
            iii. A race condition was addressed with improved state handling. (CVE-2021-30955)
        - An application may be able to execute arbitrary code with kernel privileges. A use after free issue was addressed with improved memory management. (CVE-2021-30927, CVE-2021-30980)

        - An attacker in a privileged network position may be able to execute arbitrary code. A buffer overflow issue was addressed with improved memory handling. (CVE-2021-30993)
    - LaunchServices
        - A malicious application may bypass Gatekeeper checks.
            i. A logic issue was addressed with improved state management. (CVE-2021-30976)
            ii. A logic issue was addressed with improved validation. (CVE-2021-30990)
    - Model I/O
        - Processing a maliciously crafted USD file may lead to unexpected application termination or arbitrary code execution.
            i. An out-of-bounds write issue was addressed with improved bounds checking. (CVE-2021-30971)
            ii. A buffer overflow issue was addressed with improved memory handling. (CVE-2021-30979)
        - Processing a maliciously crafted file may disclose user information. An out-of-bounds read was addressed with improved input validation. (CVE-2021-30973)
        - Processing a maliciously crafted USD file may disclose memory contents.
            i. An out-of-bounds write issue was addressed with improved bounds checking. (CVE-2021-30929)
            ii. A buffer overflow issue was addressed with improved memory handling. (CVE-2021-30940, CVE-2021-30941)
    - Preferences
        - A malicious application may be able to elevate privileges. A race condition was addressed with improved state handling. (CVE-2021-30995)
    - Sandbox
        - A malicious application may be able to bypass certain Privacy preferences.
            i. A validation issue related to hard link behavior was addressed with improved sandbox restrictions. (CVE-2021-30968)
            ii. A logic issue was addressed with improved restrictions. (CVE-2021-30946)
        - An application may be able to access a user's files. An access issue was addressed with additional sandbox restrictions. (CVE-2021-30947)
    - Script Editor
        - A malicious OSAX scripting addition may bypass Gatekeeper checks and circumvent sandbox restrictions. This issue was addressed by disabling execution of JavaScript when viewing a scripting dictionary. (CVE-2021-30975)
    - TCC
        - A local user may be able to modify protected parts of the file system. A logic issue was addressed with improved state management. (CVE-2021-30767)
        - A malicious application may be able to bypass Privacy preferences.
            i. An inherited permissions issue was addressed with additional restrictions. (CVE-2021-30964)
            ii. A logic issue was addressed with improved state management. (CVE-2021-30970)

        - A malicious application may be able to cause a denial of service to Endpoint Security clients. A logic issue was addressed with improved state management. (CVE-2021-30965)
    - WebKit
        - Processing maliciously crafted web content may lead to arbitrary code execution.
            i. A buffer overflow issue was addressed with improved memory handling. (CVE-2021-30934)
            ii. A use after free issue was addressed with improved memory management. (CVE-2021-30936, CVE-2021-30951)
            iii. An integer overflow was addressed with improved input validation. (CVE-2021-30952)
            iv. A race condition was addressed with improved state handling. (CVE-2021-30984)
            v. An out-of-bounds read was addressed with improved bounds checking. (CVE-2021-30953)
            vi. A type confusion issue was addressed with improved memory handling. (CVE-2021-30954)
    - Wi-Fi
        - A local user may be able to cause unexpected system termination or read kernel memory. This issue was addressed with improved checks. (CVE-2021-30938)

- **macOS Big Sur 11.6.2 and 2021-008 Catalina**
    - Archive Utility
        - A malicious application may bypass Gatekeeper checks. A logic issue was addressed with improved state management. (CVE-2021-30950)
    - Bluetooth
        - A malicious application may be able to disclose kernel memory. A logic issue was addressed with improved validation. (CVE-2021-30931)
        - An application may be able to execute arbitrary code with kernel privileges. A logic issue was addressed with improved validation. (CVE-2021-30935)
    - ColorSync
        - Processing a maliciously crafted image may lead to arbitrary code execution. A memory corruption issue in the processing of ICC profiles was addressed with improved input validation. (CVE-2021-30942)
    - CoreAudio
        - Playing a malicious audio file may lead to arbitrary code execution. An out-of-bounds read was addressed with improved input validation. (CVE-2021-30958)
        - Parsing a maliciously crafted audio file may lead to disclosure of user information. A buffer overflow issue was addressed with improved memory handling. (CVE-2021-30959, CVE-2021-30961, CVE-2021-30963)
    - Crash Reporter
        - A local attacker may be able to elevate their privileges. This issue was addressed with improved checks. (CVE-2021-30945)
    - Graphics Drivers

        - A malicious application may be able to execute arbitrary code with kernel privileges. A buffer overflow was addressed with improved bounds checking. (CVE-2021-30977)
- Help Viewer
    - Processing a maliciously crafted URL may cause unexpected JavaScript execution from a file on disk. A path handling issue was addressed with improved validation. (CVE-2021-30969)
- ImageIO
    - Processing a maliciously crafted image may lead to arbitrary code execution. An out-of-bounds read was addressed with improved bounds checking. (CVE-2021-30939)
- Intel Graphics Driver
    - An application may be able to execute arbitrary code with kernel privileges. A buffer overflow was addressed with improved bounds checking. (CVE-2021-30981)
- IOUSBHostFamily
    - A remote attacker may be able to cause unexpected application termination or heap corruption. A race condition was addressed with improved locking. (CVE-2021-30982)
- Kernel
    - An application may be able to execute arbitrary code with kernel privileges. A use after free issue was addressed with improved memory management. (CVE-2021-30927, CVE-2021-30980)
    - A malicious application may be able to execute arbitrary code with kernel privileges.
        i. A memory corruption vulnerability was addressed with improved locking. (CVE-2021-30937)
        ii. A memory corruption issue was addressed with improved state management. (CVE-2021-30949)
- Launch Services
    - A malicious application may bypass Gatekeeper checks.
        i. A logic issue was addressed with improved validation. (CVE-2021-30990)
        ii. A logic issue was addressed with improved state management. (CVE-2021-30976)
- Model I/O
    - Processing a maliciously crafted USD file may disclose memory contents.
        i. An out-of-bounds write issue was addressed with improved bounds checking. (CVE-2021-30929)
        ii. A buffer overflow issue was addressed with improved memory handling. (CVE-2021-30940, CVE-2021-30941)
    - Processing a maliciously crafted USD file may lead to unexpected application termination or arbitrary code execution.
        i. A buffer overflow issue was addressed with improved memory handling. (CVE-2021-30979)
        ii. An out-of-bounds write issue was addressed with improved bounds checking. (CVE-2021-30971)
    - Processing a maliciously crafted file may disclose user information. An out-of-bounds read was addressed with improved input validation. (CVE-2021-30973)
- Preferences

        - A malicious application may be able to elevate privileges. A race condition was addressed with improved state handling. (CVE-2021-30995)
    - Sandbox
        - A malicious application may be able to bypass certain Privacy preferences. A validation issue related to hard link behavior was addressed with improved sandbox restrictions. (CVE-2021-30968)
    - Script Editor
        - A malicious OSAX scripting addition may bypass Gatekeeper checks and circumvent sandbox restrictions. This issue was addressed by disabling execution of JavaScript when viewing a scripting dictionary. (CVE-2021-30975)
    - TCC
        - A local user may be able to modify protected parts of the file system. A logic issue was addressed with improved state management. (CVE-2021-30767)
        - A malicious application may be able to cause a denial of service to Endpoint Security clients. A logic issue was addressed with improved state management. (CVE-2021-30965)
    - Wi-Fi
        - A local user may be able to cause unexpected system termination or read kernel memory. This issue was addressed with improved checks. (CVE-2021-30938)

- **WatchOS 8.3 and tvOS 15.2**
    - Audio
        - Parsing a maliciously crafted audio file may lead to disclosure of user information. A buffer overflow issue was addressed with improved memory handling. (CVE-2021-30960)
    - CFNetwork Proxies
        - User traffic might unexpectedly be leaked to a proxy server despite PAC configurations. A logic issue was addressed with improved state management. (CVE-2021-30966)
    - ColorSync
        - Processing a maliciously crafted image may lead to arbitrary code execution. A memory corruption issue in the processing of ICC profiles was addressed with improved input validation. (CVE-2021-30926, CVE-2021-30942)
    - CoreAudio
        - Processing a maliciously crafted audio file may lead to arbitrary code execution. A buffer overflow issue was addressed with improved memory handling. (CVE-2021-30957)
        - Playing a malicious audio file may lead to arbitrary code execution. An out-of-bounds read was addressed with improved input validation. (CVE-2021-30958)
    - Crash Reporter
        - A local attacker may be able to elevate their privileges.
            i. This issue was addressed with improved checks. (CVE-2021-30945)
    - ImageIO

        - Processing a maliciously crafted image may lead to arbitrary code execution. An out-of-bounds read was addressed with improved bounds checking. (CVE-2021-30939)
    - Kernel
        - A malicious application may be able to execute arbitrary code with kernel privileges.
            i. A memory corruption issue was addressed with improved memory handling. (CVE-2021-30916)
            ii. A memory corruption vulnerability was addressed with improved locking. (CVE-2021-30937)
            iii. A use after free issue was addressed with improved memory management. (CVE-2021-30927, CVE-2021-30980)
            iv. A memory corruption issue was addressed with improved state management. (CVE-2021-30949)
        - An attacker in a privileged network position may be able to execute arbitrary code. A buffer overflow issue was addressed with improved memory handling. (CVE-2021-30993)
        - A malicious application may be able to execute arbitrary code with kernel privileges. A race condition was addressed with improved state handling. (CVE-2021-30955)
    - Preferences
        - A malicious application may be able to elevate privileges. A race condition was addressed with improved state handling. (CVE-2021-30995)
    - Sandbox
        - A malicious application may be able to bypass certain Privacy preferences.
            i. A validation issue related to hard link behavior was addressed with improved sandbox restrictions. (CVE-2021-30968)
            ii. A logic issue was addressed with improved restrictions. (CVE-2021-30946)
        - An application may be able to access a user's files. An access issue was addressed with additional sandbox restrictions. (CVE-2021-30947)
    - TCC
        - A local user may be able to modify protected parts of the file system. A logic issue was addressed with improved state management. (CVE-2021-30767)
        - A malicious application may be able to bypass Privacy preferences. An inherited permissions issue was addressed with additional restrictions. (CVE-2021-30964)
    - WebKit
        - Processing maliciously crafted web content may lead to arbitrary code execution.
            i. A buffer overflow issue was addressed with improved memory handling. (CVE-2021-30934)
            ii. A use after free issue was addressed with improved memory management. (CVE-2021-30936, CVE-2021-30951)
            iii. An integer overflow was addressed with improved input validation. (CVE-2021-30952)
            iv. A race condition was addressed with improved state handling. (CVE-2021-30984)

v. An out-of-bounds read was addressed with improved bounds checking. (CVE-2021-30953)
vi. A type confusion issue was addressed with improved memory handling. (CVE-2021-30954)

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:
The following actions should be taken:

- Apply appropriate patches provided by Apple to vulnerable systems immediately after appropriate testing.
- Run all software as a nonprivileged 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/HT212981
https://support.apple.com/en-us/HT212980
https://support.apple.com/en-us/HT212979
https://support.apple.com/en-us/HT212978
https://support.apple.com/en-us/HT212976
https://support.apple.com/en-us/HT212975

CVE:
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-30996
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-30995
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-30993
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-30992
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-30991
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-30990
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-30988
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-30987
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-30986
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-30985
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-30984
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-30983
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-30982
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-30981
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-30980
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-30979

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-30977
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-30976
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-30975
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-30973
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-30971
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-30970
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-30969
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-30968
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-30967
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-30966
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-30965
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-30964
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-30963
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-30961
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-30960
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-30959
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-30958
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-30957
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-30955
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-30954
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-30953
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-30952
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-30951
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-30950
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-30949
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-30948
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-30947
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-30946
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-30945
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-30942
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-30941
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-30940
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-30939
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-30938
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-30937
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-30936
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-30935
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-30934
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-30932
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-30931
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-30929
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-30927
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-30926
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-30916
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-30767

be distributed without restriction.