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:

04/27/2021

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.

- iCloud for Windows is a cloud storage and cloud computing service.
- Xcode is an integrated development environment (IDE) for macOS.
- Safari is a graphical web browser developed by Apple, based on the WebKit engine.
- macOS Big Sur is the 17th and current major release of macOS.
- macOS Catalina is the 16th major release of macOS.
- macOS Mojave is the 15th major release of macOS.
- 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.
- watchOS is the mobile operating system for the Apple Watch and is based on the iOS operating system.
- tvOS is an operating system for the fourth-generation Apple TV digital media player.
- iTunes for Windows is a media player, media library, Internet radio broadcaster, mobile device management utility, and the client app for the iTunes Store.
- GarageBand is a line of digital audio workstations for macOS, iPadOS, and iOS devices that allows users to create music or podcasts.

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 reports that WebKit Storage issues in iOS, iPadOS, Apple Watch, Apple TV 4K, and Apple TV HD may have been actively exploited. (CVE-2021-30661)

SYSTEMS AFFECTED:

- iCloud for Windows prior to version 12.3

- Xcode prior to version 12.5
- Safari prior to version 14.1
- macOS Big Sur prior to version 11.3
- macOS Catalina prior to security update 2021-002
- macOS Mojave prior to security update 2021-003
- iOS prior to version 14.5
- iPadOS prior to version 14.5
- watchOS prior to version 7.4
- tvOS prior to version 14.5
- iTunes prior to version 12.11.3
- GarageBand prior to version 10.4.3

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. Details of these vulnerabilities are as follows:

iOS 14.5 and iPadOS 14.5

- An issue in code signature validation was addressed with improved checks. (CVE-2021-1835)
- A certificate validation issue was addressed. (CVE-2021-1837)
- An issue in code signature validation was addressed with improved checks. (CVE-2021-1849)
- An out-of-bounds read was addressed with improved input validation. (CVE-2021-1867)
- A logic issue was addressed with improved state management. (CVE-2021-1810)
- A logic issue was addressed with improved restrictions. (CVE-2021-1836)
- A memory corruption issue was addressed with improved validation. (CVE-2021-1808)
- A memory initialization issue was addressed with improved memory handling. (CVE-2021-1857)
- An out-of-bounds read was addressed with improved input validation. (CVE-2021-1846)
- A memory corruption issue was addressed with improved validation. (CVE-2021-1809)
- A validation issue was addressed with improved logic. (CVE-2021-30659)
- A logic issue was addressed with improved state management. (CVE-2021-1811)
- A logic issue was addressed with improved state management. (CVE-2021-1872)
- An out-of-bounds read was addressed with improved input validation. (CVE-2021-1881)
- A memory corruption issue was addressed with improved validation. (CVE-2021-1882)

- A validation issue was addressed with improved logic. (CVE-2021-1813)
- An access issue was addressed with improved memory management. (CVE-2021-30656)
- Heap corruption issue was addressed with improved checks. (CVE-2021-1883)
- A denial of service condition was addressed with improved locking. (CVE-2021-1884)
- Out-of-bounds read issue were addressed with improved bounds checking. (CVE-2021-1885)
- Processing of maliciously crafted image was addressed with improved checks. (CVE-2021-30653, CVE-2021-1843)
- Out-of-bounds write issue were addressed with improved bounds checking. (CVE-2021-1858)
- A use after free issue was addressed with improved memory management. (CVE-2021-1864)
- An out-of-bounds read was addressed with improved input validation. (CVE-2021-1877, CVE-2021-1852, CVE-2021-1830)
- A logic issue was addressed with improved state management. (CVE-2021-1874, CVE-2021-1851)
- A buffer overflow was addressed with improved bounds checking. (CVE-2021-1816)
- File permission issue was addressed with improved permissions logic. (CVE-2021-1832)
- An out-of-bounds read was addressed with improved bounds checking. (CVE-2021-30660)
- Root privilege condition was addressed with additional validation. (CVE-2021-30652)
- A double free issue was addressed with improved memory management. (CVE-2021-1875)
- A logic issue was addressed with improved restrictions. (CVE-2021-1822)
- An issue obscuring passwords in screenshots was addressed with improved logic. (CVE-2021-1865)
- A validation issue was addressed with improved input sanitization. (CVE-2021-1807)
- An application may allow shortcuts issue was addressed with improved permissions logic. (CVE-2021-1831)
- A logic issue was addressed with improved state management. (CVE-2021-1868)
- A call termination issue was addressed with improved logic. (CVE-2021-1854)
- Sensitive information disclosure issue was addressed with improved UI handling. (CVE-2021-1848)
- A cross site scripting vulnerability was addressed with improved input validation. (CVE-2021-1825)
- A memory corruption issue was addressed with improved state management. (CVE-2021-1817)
- A logic issue was addressed with improved restrictions. (CVE-2021-1826)
- A memory initialization issue was addressed with improved memory handling. (CVE-2021-1820)
- Arbitrary code execution issue was addressed with improved memory management. (CVE-2021-30661)
- A use after free issue was addressed with improved memory management. (CVE-2021-7463)

Garage Band 10.4.3

- A local attacker may be able to read sensitive information. (CVE-2021-30654)

iTunes 12.11.3

- A double free issue was addressed with improved memory management. (CVE-2021-1875)
- A logic issue was addressed with improved state management. (CVE-2021-1811)
- An input validation issue was addressed with improved input validation. ((CVE-2021-1825)
- A use after free issue was addressed with improved memory management. (CVE-2021-7463)

Xcode 12.5

- Arbitrary code execution issue was addressed with improved checks. (CVE-2021-21300)

iCloud for Windows 12.3

- A memory initialization issue was addressed with improved memory handling. (CVE-2021-1857)
- A logic issue was addressed with improved state management. (CVE-2021-1811)
- An input validation issue was addressed with improved input validation. ((CVE-2021-1825)
- A use after free issue was addressed with improved memory management. (CVE-2021-7463)

tvOS 14.5

- An issue in code signature validation was addressed with improved checks. (CVE-2021-1849)
- A logic issue was addressed with improved restrictions. (CVE-2021-1836)
- A memory corruption issue was addressed with improved validation. (CVE-2021-1808)
- A memory initialization issue was addressed with improved memory handling. (CVE-2021-1857)
- An out-of-bounds read was addressed with improved input validation. (CVE-2021-1846)
- A memory corruption issue was addressed with improved validation. (CVE-2021-1809)
- A logic issue was addressed with improved state management. (CVE-2021-1811)
- An out-of-bounds read was addressed with improved input validation. (CVE-2021-1881)
- A memory corruption issue was addressed with improved validation. (CVE-2021-1882)
- A validation issue was addressed with improved logic. (CVE-2021-1813)
- Heap corruption issue was addressed with improved checks. (CVE-2021-1883)
- A denial of service condition was addressed with improved locking. (CVE-2021-1884)
- Out-of-bounds read issue were addressed with improved bounds checking. (CVE-2021-1885)
- Processing of maliciously crafted image was addressed with improved checks. (CVE-2021-30653, CVE-2021-1843)

- Out-of-bounds write issue were addressed with improved bounds checking. (CVE-2021-1858)
- A use after free issue was addressed with improved memory management. (CVE-2021-1864)
- A memory initialization issue was addressed with improved memory handling. (CVE-2021-1860)
- A buffer overflow was addressed with improved bounds checking. (CVE-2021-1816)
- A logic issue was addressed with improved state management. (CVE-2021-1851)
- File permission issue was addressed with improved permissions logic. (CVE-2021-1832)
- An out-of-bounds read was addressed with improved bounds checking. (CVE-2021-30660)
- Root privilege condition was addressed with additional validation. (CVE-2021-30652)
- A double free issue was addressed with improved memory management. (CVE-2021-1875)
- A logic issue was addressed with improved restrictions. (CVE-2021-1822)
- A parsing issue in the handling of directory paths was addressed with improved path validation. (CVE-2021-1815, CVE-2021-1739, CVE-2021-1740)
- A logic issue was addressed with improved state management. (CVE-2021-1868)
- A memory corruption issue was addressed with improved validation. (CVE-2021-1844)
- An input validation issue was addressed with improved input validation. ((CVE-2021-1825)
- A memory corruption issue was addressed with improved state management. (CVE-2021-1817)
- A logic issue was addressed with improved restrictions. (CVE-2021-1826)
- A memory initialization issue was addressed with improved memory handling. (CVE-2021-1820)
- Arbitrary code execution issue was addressed with improved memory management. (CVE-2021-30661)

watchOS 7.4

- An issue in code signature validation was addressed with improved checks. (CVE-2021-1849)
- A memory corruption issue was addressed with improved validation. (CVE-2021-1808)
- A memory initialization issue was addressed with improved memory handling. (CVE-2021-1857)
- An out-of-bounds read was addressed with improved input validation. (CVE-2021-1846)
- A memory corruption issue was addressed with improved validation. (CVE-2021-1809)
- A validation issue was addressed with improved logic. (CVE-2021-30659)
- A logic issue was addressed with improved state management. (CVE-2021-1811)
- A logic issue was addressed with improved state management. (CVE-2021-1872)
- An out-of-bounds read was addressed with improved input validation. (CVE-2021-1881)
- A logic issue was addressed with improved restrictions. (CVE-2021-1822)
- A validation issue was addressed with improved logic. (CVE-2021-1813)

- Heap corruption issue was addressed with improved checks. (CVE-2021-1883)
- A denial of service condition was addressed with improved locking. (CVE-2021-1884)
- Processing of maliciously crafted image was addressed with improved checks. (CVE-2021-1880, CVE-2021-1814, CVE-2021-30653, CVE-2021-1843)
- Out-of-bounds read issue were addressed with improved bounds checking. (CVE-2021-1885)
- Out-of-bounds write issue were addressed with improved bounds checking. (CVE-2021-1858)
- A use after free issue was addressed with improved memory management. (CVE-2021-1864)
- A memory initialization issue was addressed with improved memory handling. (CVE-2021-1860)
- A buffer overflow was addressed with improved bounds checking. (CVE-2021-1816)
- A logic issue was addressed with improved state management. (CVE-2021-1851)
- File permission issue was addressed with improved permissions logic. (CVE-2021-1832)
- An out-of-bounds read was addressed with improved bounds checking. (CVE-2021-30660)
- Root privilege condition was addressed with additional validation. (CVE-2021-30652)
- A double free issue was addressed with improved memory management. (CVE-2021-1875)
- A logic issue was addressed with improved restrictions. (CVE-2021-1822)
- A parsing issue in the handling of directory paths was addressed with improved path validation. (CVE-2021-1815, CVE-2021-1739, CVE-2021-1740)
- A validation issue was addressed with improved input sanitization. (CVE-2021-1807)
- Privilege escalation issue was addressed with improved state management. (CVE-2021-1868)
- A cross site scripting vulnerability was addressed with improved input validation. (CVE-2021-1825)
- A memory corruption issue was addressed with improved state management. (CVE-2021-1817)
- A logic issue was addressed with improved restrictions. (CVE-2021-1826)
- A memory initialization issue was addressed with improved memory handling. (CVE-2021-1820)
- Arbitrary code execution issue was addressed with improved memory management. (CVE-2021-30661)

macOS Big Sur 11.3

- Privilege escalation was addressed with improved state management. (CVE-2021-1853)
- An issue in code signature validation was addressed with improved checks. (CVE-2021-1849)
- An out-of-bounds read was addressed with improved input validation. (CVE-2021-1867)
- A logic issue was addressed with improved state management. (CVE-2021-1810)
- A memory corruption issue was addressed with improved validation. (CVE-2021-1808)

- A memory initialization issue was addressed with improved memory handling. (CVE-2021-1857)
- An out-of-bounds read was addressed with improved input validation. (CVE-2021-1846)
- A memory corruption issue was addressed with improved validation. (CVE-2021-1809)
- A validation issue was addressed with improved logic. (CVE-2021-30659)
- Arbitrary code execution or unexpected application termination issue was addressed with improved validation. (CVE-2021-1847)
- Disclosure of process memory issue was addressed with improved state management. (CVE-2021-1811)
- Fraudulent OCSP response issue was addressed with improved checks. (CVE-2021-8286)
- A buffer overflow was addressed with improved input validation. (CVE-2021-8285)
- A permissions issue existed in DiskArbitration. This was addressed with additional ownership checks. (CVE-2021-1784)
- A logic issue was addressed with improved state management. (CVE-2021-1872)
- An out-of-bounds read was addressed with improved input validation. (CVE-2021-1881)
- A memory corruption issue was addressed with improved validation. (CVE-2021-1882)
- A validation issue was addressed with improved logic. (CVE-2021-1813)
- Heap corruption issue was addressed with improved checks. (CVE-2021-1883)
- A denial of service condition was addressed with improved locking. (CVE-2021-1884)
- Processing of maliciously crafted image was addressed with improved checks. (CVE-2021-1880, CVE-2021-1814, CVE-2021-30653, CVE-2021-1843)
- Out-of-bounds read issue were addressed with improved bounds checking. (CVE-2021-1885)
- Out-of-bounds write issue were addressed with improved bounds checking. (CVE-2021-1858)
- An out-of-bounds write issue was addressed with improved bounds checking. (CVE-2021-1841, CVE-2021-1834)
- A memory initialization issue was addressed with improved memory handling. (CVE-2021-1860)
- A memory corruption issue was addressed with improved validation. (CVE-2021-1840)
- A logic issue was addressed with improved state management. (CVE-2021-1851)
- File permission issue was addressed with improved permissions logic. (CVE-2021-1832)
- An out-of-bounds read was addressed with improved bounds checking. (CVE-2021-30660)
- Root privilege condition was addressed with additional validation. (CVE-2021-30652)
- A double free issue was addressed with improved memory management. (CVE-2021-1875)
- Access to privilege information was addressed with improved entitlements. (CVE-2021-1824)
- Unexpected lock issue was addressed with improved state management. (CVE-2021-1859)

- Arbitrary code execution issue was addressed with improved memory management. (CVE-2021-1876)
- A parsing issue in the handling of directory paths was addressed with improved path validation. (CVE-2021-1815, CVE-2021-1739, CVE-2021-1740)
- An issue existed in determining cache occupancy. The issue was addressed through improved logic. (CVE-2021-1861)
- Favicon network connection issue was addressed with improved state management. (CVE-2021-1855)
- Privilege escalation issue was addressed with improved state management. (CVE-2021-1868)
- An integer overflow was addressed with improved input validation. (CVE-2021-1878)
- A logic issue was addressed with improved state management. (CVE-2021-30657)
- A denial of service issue was addressed with improved checks. (CVE-2020-8037)
- Privilege escalation issue was addressed with improved permissions logic. (CVE-2021-1839)
- A cross site scripting vulnerability was addressed with improved input validation. (CVE-2021-1825)
- A memory corruption issue was addressed with improved state management. (CVE-2021-1817)
- A logic issue was addressed with improved restrictions. (CVE-2021-1826)
- A memory initialization issue was addressed with improved memory handling. (CVE-2021-1820)
- Arbitrary code execution issue was addressed with improved memory management. (CVE-2021-30661)
- Corrupt kernel memory or unexpected system termination issue was addressed with improved memory management. (CVE-2020-7463)
- Write kernel memory or unexpected system termination issue was addressed with improved validation. (CVE-2021-1828)
- Arbitrary code execution with kernel privileges issue was addressed with improved state handling. (CVE-2021-1829)
- Arbitrary code with system privileges issue was addressed with improved permissions logic. (CVE-2021-30655)
- An API issue in Accessibility TCC permissions was addressed with improved state management. (CVE-2021-1873)

macOS Catalina:

- The issue was addressed with improved permissions logic. (CVE-2021-1797)
- A logic issue was addressed with improved state management. (CVE-2021-1810)
- A memory corruption issue was addressed with improved validation. (CVE-2021-1808)
- A memory initialization issue was addressed with improved memory handling. (CVE-2021-1857)
- A memory corruption issue was addressed with improved validation. (CVE-2021-1809)
- A memory corruption issue was addressed with improved validation. (CVE-2021-1847)
- A logic issue was addressed with improved state management. (CVE-2021-1811)
- A buffer overflow was addressed with improved input validation. (CVE-2020-8285)
- This issue was addressed with improved checks. (CVE-2020-8286)

- A permissions issue existed in DiskArbitration. This was addressed with additional ownership checks. (CVE-2021-1784)
- An out-of-bounds read was addressed with improved input validation. (CVE-2021-1881)
- A logic issue was addressed with improved state management. (CVE-2020-27942)
- A validation issue was addressed with improved logic. (CVE-2021-1813)
- A memory corruption issue was addressed with improved validation. (CVE-2021-1882)
- This issue was addressed with improved checks. (CVE-2021-1843)
- An out-of-bounds write issue was addressed with improved bounds checking. (CVE-2021-1834)
- A memory initialization issue was addressed with improved memory handling. (CVE-2021-1860)
- A logic issue was addressed with improved state management. (CVE-2021-1851)
- A memory corruption issue was addressed with improved validation. (CVE-2021-1840)
- A race condition was addressed with additional validation. (CVE-2021-30652)
- A double free issue was addressed with improved memory management. (CVE-2021-1875)
- This issue was addressed with improved entitlements. (CVE-2021-1824)
- A use after free issue was addressed with improved memory management. (CVE-2021-1824)
- A parsing issue in the handling of directory paths was addressed with improved path validation. (CVE-2021-1739, CVE-2021-1740)
- An integer overflow was addressed with improved input validation. (CVE-2021-1878)
- A logic issue was addressed with improved state management. (CVE-2021-1868)
- This issue was addressed with improved checks. (CVE-2020-8037)
- The issue was addressed with improved permissions logic. (CVE-2021-1839)
- A memory corruption issue was addressed with improved validation. (CVE-2021-1828)
- The issue was addressed with improved permissions logic. (CVE-2020-3838)
- An API issue in Accessibility TCC permissions was addressed with improved state management. (CVE-2021-1873)

macOS Mojave:

- The issue was addressed with improved permissions logic. (CVE-2021-1797)
- A memory corruption issue was addressed with improved validation. (CVE-2021-1808)
- A memory corruption issue was addressed with improved validation. (CVE-2021-1809)
- A memory corruption issue was addressed with improved validation. (CVE-2021-1847)
- A buffer overflow was addressed with improved input validation. (CVE-2020-8285)
- This issue was addressed with improved checks. (CVE-2020-8256)
- A permissions issue existed in DiskArbitration. This was addressed with additional ownership checks. (CVE-2021-1784)
- An out-of-bounds read was addressed with improved input validation. (CVE-2021-1881)
- A logic issue was addressed with improved state management. (CVE-2020-27942)

- A validation issue was addressed with improved logic. (CVE-2021-1813)
- This issue was addressed with improved checks. (CVE-2021-1843)
- An out-of-bounds write was addressed with improved input validation. (CVE-2021-1805)
- A race condition was addressed with additional validation. (CVE-2021-1806)
- An out-of-bounds write issue was addressed with improved bounds checking. (CVE-2021-1834)
- A memory initialization issue was addressed with improved memory handling. (CVE-2021-1860)
- A logic issue was addressed with improved state management. (CVE-2021-1851)
- A memory corruption issue was addressed with improved validation. (CVE-2021-1840)
- A race condition was addressed with additional validation. (CVE-2021-30652)
- A double free issue was addressed with improved memory management. (CVE-2021-1875)
- A use after free issue was addressed with improved memory management. (CVE-2021-1876)
- A parsing issue in the handling of directory paths was addressed with improved path validation. (CVE-2021-1739)
- An integer overflow was addressed with improved input validation. (CVE-2021-1878)
- A logic issue was addressed with improved state management. (CVE-2021-1868)
- This issue was addressed with improved checks. (CVE-2020-8037)
- The issue was addressed with improved permissions logic. (CVE-2021-1839)
- A memory corruption issue was addressed with improved validation. (CVE-2021-1828)
- The issue was addressed with improved permissions logic. (CVE-2020-3838)
- An API issue in Accessibility TCC permissions was addressed with improved state management. (CVE-2021-1873)

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/HT201222
https://support.apple.com/en-us/HT212299
https://support.apple.com/en-us/HT212317
https://support.apple.com/en-us/HT212318
https://support.apple.com/en-us/HT212319
https://support.apple.com/en-us/HT212320
https://support.apple.com/en-us/HT212321
https://support.apple.com/en-us/HT212323
https://support.apple.com/en-us/HT212324
https://support.apple.com/en-us/HT212325
https://support.apple.com/en-us/HT212326
https://support.apple.com/en-us/HT212327

Bleeping Computer:
https://www.bleepingcomputer.com/news/security/apple-fixes-macos-zero-day-bug-exploited-by-shlayer-malware/

CVE:
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-3838
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-3838
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-8037
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-8285
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-8286
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-27942
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1739
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1740
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1784
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1797
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1805
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1806
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1807
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1808
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1809
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1810
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1811
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1813
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1814
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1815
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1816
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1817
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1820
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1822
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1824
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1825
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1825
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1826
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1828
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1829
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1830
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1831

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1832

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1834

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1835

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1836

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1837

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1839

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1840

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1841

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1843

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1844

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1846

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1847

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1848

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1849

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1851

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1852

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1853

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1854

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1855

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1857

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1858

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1859

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1860

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1861

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1864

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1865

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1867

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1868

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1868

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1872

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1873

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1874

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1875

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1876

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1877

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1878

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1880

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1881

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1882

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1883

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1884

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1885

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-7463

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-8285

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-8286

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-21300

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-30652

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-30653

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-30654

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-30655

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-30656

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-30657
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-30658
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-30659
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-30660
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-30661

TLP: WHITE