

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

Disclosure is not limited. Subject to standard copyright rules, TLP: WHITE information may be distributed without restriction.

<http://www.us-cert.gov/tlp/>

DATE(S) ISSUED:

09/25/2020

SUBJECT:

Multiple Vulnerabilities in Apple Products Could Allow for Arbitrary Code Execution

OVERVIEW:

Multiple vulnerabilities have been discovered in iCloud for Windows and macOS. The most severe of these vulnerabilities could allow for arbitrary code execution.

- macOS is a desktop operating system for Macintosh computers
- iCloud for Windows is a cloud storage service that can be used on Windows computers.

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 privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Users whose accounts are configured to have fewer user rights on the system could be less impacted than those who operate with administrative user rights.

THREAT INTELLIGENCE:

There are no reports of these vulnerabilities being exploited in the wild.

SYSTEMS AFFECTED:

- macOS prior to High Sierra 10.15.7, Security Update 2020-005 High Sierra, Security Update 2020-005 Mojave
- iCloud for Windows prior to 11.4

RISK:

Government:

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

Businesses:

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

Home users: Low

TECHNICAL SUMMARY:

Multiple vulnerabilities have been discovered in iCloud for Windows and macOS. The most severe of these vulnerabilities could allow for arbitrary code execution. Details of these vulnerabilities are as follows:

- An out-of-bounds read vulnerability in ImageIO, which could allow for arbitrary code execution, was addressed with improved input validation. (CVE-2020-9961)
- A vulnerability in Mail, which could allow for a remote attacker to unexpectedly alter application state, was addressed with improved checks. (CVE-2020-9941)
- An out-of-bounds read vulnerability in Model I/O, which could allow for arbitrary code execution or unexpected application termination, was addressed with improved bounds checking. (CVE-2020-9973)
- A vulnerability in Sandbox, which could allow for a malicious application to access restricted files, was addressed with improved restrictions. (CVE-2020-9968)
- A vulnerability in WebKit, which could allow for a cross site scripting attack, was addressed with improved input validation. (CVE-2020-9952)

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 privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Users whose accounts are configured to have fewer user rights on the system could be less impacted than those who operate with administrative user rights.

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 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 un-trusted or unknown sources.
- Remind users not to visit untrusted websites or follow links provided by unknown or un-trusted sources.
- Apply the Principle of Least Privilege to all systems and services.

REFERENCES:

Apple:

<https://support.apple.com/en-us/HT211849>

<https://support.apple.com/en-us/HT211846>

CVE:

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-9961>

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-9941>

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-9973>

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-9968>

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-9952>

TLP: WHITE

Disclosure is not limited. Subject to standard copyright rules, TLP: WHITE information may be distributed without restriction.

<http://www.us-cert.gov/tlp/>