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:
11/12/2021

SUBJECT:
Multiple Vulnerabilities in iCloud for Windows Could Allow for Arbitrary Code Execution.

OVERVIEW:
Multiple vulnerabilities have been discovered in iCloud for Windows Could Allow for Arbitrary Code Execution. iCloud for Windows is a cloud storage and cloud computing service. Successful exploitation 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:
- iCloud for Windows versions prior to 13

RISK:
Government:
- Large and medium government entities: **Medium**
- Small government entities: **Medium**

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

Home users: Low

TECHNICAL SUMMARY:
Multiple Vulnerabilities have been discovered in iCloud for Windows which could allow for arbitrary code execution in the context of the affected user. Details of these vulnerabilities are as follows:

- A type confusion issue was addressed with improved memory handling, which could allow for arbitrary code execution. (CVE-2021-30852)
- A memory corruption issue was addressed with improved input validation, which could allow for arbitrary code execution. (CVE-2021-30814)

- Processing a maliciously crafted image could allow for arbitrary code execution. (CVE-2021-30835, CVE-2021-30847)
- An attacker in a privileged network position may be able to bypass HSTS. (CVE-2021-30823)
- Multiple memory corruption issues, which could allow for arbitrary code execution. (CVE-2021-30849)

Successful exploitation 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/HT212953

CVE:
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-30852
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-30814
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-30835
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-30847
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-30823
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-30849