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.
https://www.us-cert.gov/tlp/

DATE(S) ISSUED:
06/17/2019

SUBJECT:
A Vulnerability in VLCMedia Player Could Allow for Arbitrary Code Execution

OVERVIEW:
A vulnerability has been identified in VLCMedia Player which could allow for arbitrary code execution. VLC is a cross-platform multimedia player and framework. Successful exploitation of this vulnerability could allow for arbitrary code execution in the context of the affected application. Depending on the privileges associated with this application, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. If this application has been configured to have fewer user rights on the system, exploitation of this vulnerability could have less impact than if it was configured with administrative rights. Failed exploitation could result in a denial-of-service condition.

THREAT INTELLIGENCE:
There are currently no reports of this vulnerability being exploited in the wild.

SYSTEMS AFFECTED:
- VLCMedia Player versions prior to 3.0.7

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:
A buffer overflow vulnerability has been identified in VLCMedia Player which could allow for arbitrary code execution. This vulnerability occurs due to the failure to perform adequate boundary checks on user-supplied input in the 'ReadFrame()' function in 'avi.c' source file. Successful exploitation of this vulnerability could allow for arbitrary code execution in the context of the affected application. Depending on the privileges associated with this application, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. If this application has been configured to have fewer user rights on the system, exploitation of this vulnerability could have less impact than if it was configured with administrative rights. Failed exploitation could result in a denial-of-service condition.

RECOMMENDATIONS:
The following actions should be taken:

- Apply appropriate updates provided by VLC 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 visit un-trusted websites or follow links provided by unknown or un-trusted sources.
- Inform and educate users regarding the threats posed by hypertext links contained in emails or attachments especially from un-trusted sources.
- Apply the Principle of Least Privilege to all systems and services.

REFERENCES:
VLC:
http://www.videolan.org/

CVE:
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-5439

TLP: WHITE
Disclosure is not limited. Subject to standard copyright rules, TLP: WHITE information may be distributed without restriction.
https://www.us-cert.gov/tlp/

Chris Watts
Security Operations Analyst
MS Department of Information Technology Services
601-432-8201 | www.its.ms.gov