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:
05/14/2019

SUBJECT:
A Vulnerability in Adobe Flash Could Allow for Arbitrary Code Execution (APSB19-26)

OVERVIEW:
A vulnerability has been discovered in Adobe Flash which could allow for arbitrary code execution. Adobe Flash Player is a widely distributed multimedia and application player used to enhance the user experience when visiting web pages or reading email messages. Successful exploitation this vulnerability could result in an attacker executing arbitrary code 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.

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

SYSTEMS AFFECTED:
- Adobe Flash Player Desktop Runtime for Windows, macOS and Linux versions prior to 32.0.0.171
- Adobe Flash Player for Google Chrome for Windows, macOS, Linux and Chrome OS versions prior to 32.0.0.171
- Adobe Flash Player for Microsoft Edge and Internet Explorer for Windows 10 and 8 versions prior to 32.0.0.171

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: Medium

TECHNICAL SUMMARY:

A use after free vulnerability has been discovered in Adobe Flash which could allow for arbitrary code execution. Successful exploitation of this vulnerability could result in an attacker executing arbitrary code 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.

RECOMMENDATIONS:
The following actions should be taken:
- Install the updates provided by Adobe 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 websites or follow links provided by unknown or untrusted 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:
Adobe:
https://helpx.adobe.com/security/products/flash-player/apsb19-26.html

CVE:
https://cve.mitre.org/cgi-bin/cvename.cgi?name=2019-7837

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

Mississippi Department of
Information Technology Services

3771 Eastwood Drive | Jackson, Mississippi 39211-6381