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:
04/14/2021

SUBJECT:
Multiple Vulnerabilities in Adobe Products Could Allow for Arbitrary Code Execution

OVERVIEW:
Multiple vulnerabilities have been discovered in Adobe Products, the most severe of which could allow for arbitrary code execution.

- Photoshop is Adobe's flagship image editing software.
- Digital Editions is an e-book reader software program.
- Bridge is a free digital asset management app. It is a mandatory component of Adobe Creative Suite, Adobe eLearning Suite, Adobe Technical Communication Suite and Adobe Photoshop CS2 through CS6.
- RoboHelp is a help authoring tool.

Successful exploitation of the most severe of these vulnerabilities could allow for arbitrary code execution. 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 currently no reports of these vulnerabilities being exploited in the wild.

SYSTEMS AFFECTED:
- Adobe Photoshop 2020 versions 21.2.6 and earlier
- Adobe Photoshop 2021 versions 22.3 and earlier
- Adobe Digital Editions versions 4.5.11.187245 and earlier
- Adobe Bridge versions 10.1.1 and earlier
- Adobe Bridge versions 11.0.1 and earlier
- Adobe RoboHelp versions RH2020.0.3 and earlier

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 Adobe Photoshop, Digital Editions, Bridge and RoboHelp, the most severe of which could allow for arbitrary code execution. Details of these vulnerabilities are as follows:

Adobe Photoshop

- Buffer Overflow, which could allow for arbitrary code execution. (CVE-2021-28548, CVE-2021-28549)

Adobe Digital Editions

- Privilege Escalation, which could allow for arbitrary file system write. (CVE-2021-21100)

Adobe Bridge

- Out-of-bounds read, which could allow for information disclosure. (CVE-2021-21091)
- Improper Authorization, which could allow for privilege escalation. (CVE-2021-21096)
- Memory Corruption, which could allow for arbitrary code execution. (CVE-2021-21093, CVE-2021-21092)
- Out-of-bounds write, which could allow for arbitrary code execution. (CVE-2021-21094, CVE-2021-21095)

Adobe RoboHelp

- Uncontrolled search path element, which could allow for privilege escalation. (CVE-2021-21070)

Successful exploitation of the most severe of these vulnerabilities could allow for arbitrary code execution. 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:

- 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.
- Apply the Principle of Least Privilege to all systems and services.

REFERENCES:

Adobe:

- https://helpx.adobe.com/security.html
- https://helpx.adobe.com/security/products/photoshop/apsb21-28.html
- https://helpx.adobe.com/security/products/Digital-Editions/apsb21-26.html
- https://helpx.adobe.com/security/products/bridge/apsb21-23.html
- https://helpx.adobe.com/security/products/robohelp/apsb21-20.html

CVE:

- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-21070
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-21091
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-21092
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-21093
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-21094
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-21095
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-21096
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-21100
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-28548
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-28549

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.