TLP: WHITE
www.cisa.gov/tlp
Information may be distributed without restriction, subject to standard copyright rules.

DATE(S) ISSUED:
01/11/2022
03/23/2022 – **UPDATED**

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.

- Acrobat and Reader is a family of application software and Web services mainly used to create, view, and edit PDF documents.
- Illustrator is a vector graphics editor and design program.
- Bridge is a digital asset management application.
- Adobe InCopy is a professional word processor.
- InDesign is an industry-leading layout and page design software for print and digital media.

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.

March 23 - UPDATED OVERVIEW:
Two additional vulnerabilities have been reported in Adobe Acrobat and Adobe Reader which could allow for remote code execution.

THREAT INTELLIGENCE:
There are currently no reports of these vulnerabilities being exploited in the wild.

SYSTEMS AFFECTED:

- Acrobat DC and Acrobat Reader DC 21.007.20099 and earlier versions for Windows and macOS
- Acrobat 2020 and Acrobat Reader 2020 20.004.30017 and earlier versions for Windows and macOS.
- Acrobat 2017 and Acrobat Reader 2017 17.011.30204 and earlier versions for Windows and macOS.
- Illustrator 2022 26.0.1 and earlier versions for Windows and macOS.
- Illustrator 2021 25.4.2 and earlier versions for Windows and macOS.
- Adobe Bridge 12.0 and earlier versions for Windows and macOS.
- Adobe Bridge 11.1.2 and earlier versions for Windows and macOS.
- Adobe InCopy 16.4 and earlier versions for Windows and macOS.
- Adobe InDesign 16.4 and earlier versions for Windows and macOS.

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 Products, the most severe of which could allow for arbitrary code execution. Details of these vulnerabilities are as follows:

Adobe Acrobat and Reader

- Use After Free, which could allow for Arbitrary code execution. (CVE-2021-44701, CVE-2021-44704, CVE-2021-44706, CVE-2021-44710, CVE-2021-45062, CVE-2021-45064)
- Improper Access Control which could allow for Privilege escalation. (CVE-2021-44702)
- Stack-based Buffer Overflow which could allow for Arbitrary code execution. (CVE-2021-44703)
- Access of Uninitialized Pointer which could allow for Arbitrary code execution. (CVE-2021-44705)
- Out-of-bounds Write which could allow for Arbitrary code execution. (CVE-2021-44707, CVE-2021-45061, CVE-2021-45068)
- Heap-based Buffer Overflow which could allow for Arbitrary code execution. (CVE-2021-44708, CVE-2021-44709)

- Integer Overflow or Wraparound which could allow for Arbitrary code execution. (CVE-2021-44711)
- Improper Input Validation which could allow for Application denial-of-service. (CVE-2021-44712)
- Use After Free which could allow for Application denial-of-service. (CVE-2021-44713)
- Violation of Secure Design Principles which could allow for Security feature bypass. (CVE-2021-44714)
- Out-of-bounds Read which could allow for a Memory Leak. (CVE-2021-44715, CVE-2021-44742)
- Improper Input Validation which could allow for Security feature bypass. (CVE-2021-44739)
- NULL Pointer Dereference which could allow for Application denial-of-service. (CVE-2021-44740, CVE-2021-44741)
- Out-of-bounds Read which could allow for Arbitrary code execution. (CVE-2021-45060)
- Use After Free which could allow for Privilege escalation. (CVE-2021-45063)
- Access of Memory Location After End of Buffer which could allow for a Memory Leak. (CVE-2021-45067)

Adobe Illustrator

- Out-of-bounds Read which could allow for Privilege escalation. (CVE-2021-43752, CVE-2021-44700)

Adobe Bridge

- Out-of-bounds Write which could allow for Arbitrary code execution. (CVE-2021-44743)
- Use After Free which could allow for Privilege escalation. (CVE-2021-45051)
- Out-of-bounds Read which could allow for Privilege escalation. (CVE-2021-45052)
- Out-of-bounds Read which could allow for a Memory leak. (CVE-2021-44187, CVE-2021-44186, CVE-2021-44185)

Adobe InCopy

- Out-of-bounds Write which could allow for Arbitrary code execution. (CVE-2021-45053, CVE-2021-45056)
- Use After Free which could allow for Privilege escalation. (CVE-2021-45054)
- Out-of-bounds Read which could allow for Arbitrary code execution. (CVE-2021-45055)

Adobe InDesign

- Out-of-bounds Write which could allow for Arbitrary code execution. (CVE-2021-45057, CVE-2021-45058)
- Use After Free which could allow for Privilege escalation. (CVE-2021-45059)

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.

March 23 – UPDATED TECHNICAL SUMMARY:
Adobe Acrobat and Reader

- **Out-of-bounds Write which could allow for Arbitrary code execution (CVE-2022-24091, CVE-2022-24092)**

RECOMMENDATIONS:
We recommend the following actions 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 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:

Adobe:
https://helpx.adobe.com/security/security-bulletin.html
https://helpx.adobe.com/security/products/acrobat/apsb22-01.html
https://helpx.adobe.com/security/products/illustrator/apsb22-02.html
https://helpx.adobe.com/security/products/bridge/apsb22-03.html
https://helpx.adobe.com/security/products/incopy/apsb22-04.html
https://helpx.adobe.com/security/products/indesign/apsb22-05.html

CVE:
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-43752

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-44185

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-44186

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-44187

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-44700

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-44701

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-44702

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-44703

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-44704

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-44705
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-44706
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-44707

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-44708

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-44709

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-44710

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-44711

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-44712

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-44713

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-44714

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-44715

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-44739
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-44740
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-44741
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-44742

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-44743

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-45051

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-45052

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-45053
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-45054
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-45055
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-45056
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-45057
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-45058
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-45059
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-45060
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-45061
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-45062

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-45063
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-45064
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-45067

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-45068

March 23 – UPDATED REFERENCES:

CVE:
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-24091
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-24092