EXECUTIVE SUMMARY

May 16, 2019 | MTIS19-023

Since the last McAfee® Labs Security Advisory (May 14), the following noteworthy event has taken place:

- Patches are available for multiple Adobe security vulnerabilities

NEW THREAT OVERVIEW

(APSB19-18) Adobe Acrobat Reader Out-of-Bounds Read Information Disclosure (CVE-2019-7778)

MTIS19-023-A

IMPORTANCE:	Low
COVERED PRODUCTS:	Vulnerability Manager
UNDER ANALYSIS:	DAT | Web Gateway | Firewall Enterprise

Back to top

(APSB19-18) Adobe Acrobat Reader Security bypass Remote Code Execution (CVE-2019-7779)

MTIS19-023-B

IMPORTANCE:	Low
COVERED PRODUCTS:	Vulnerability Manager
UNDER ANALYSIS:	DAT | Web Gateway | Firewall Enterprise

Back to top

(APSB19-18) Adobe Acrobat Reader Out-of-Bounds Read Information Disclosure (CVE-2019-7780)

MTIS19-023-C

IMPORTANCE:	Low
COVERED PRODUCTS:	Vulnerability Manager
UNDER ANALYSIS:	DAT | Web Gateway | Firewall Enterprise

Back to top

(APSB19-18) Adobe Acrobat Reader Use After Free Remote Code Execution (CVE-2019-7781)

MTIS19-023-D

IMPORTANCE:	Low
COVERED PRODUCTS:	Vulnerability Manager
UNDER ANALYSIS:	DAT | Web Gateway | Firewall Enterprise

Back to top

(APSB19-18) Adobe Acrobat Reader Use After Free Remote Code Execution (CVE-2019-7782)

MTIS19-023-E

IMPORTANCE:	Low
COVERED PRODUCTS:	Vulnerability Manager
UNDER ANALYSIS:	DAT | Web Gateway | Firewall Enterprise

Back to top

(APSB19-18) Adobe Acrobat Reader Use After Free Remote Code Execution (CVE-2019-7783)
MTIS19-023-F

IMPORTANCE: Low
COVERED PRODUCTS: Vulnerability Manager
UNDER ANALYSIS: DAT | Web Gateway | Firewall Enterprise

Back to top

(APSB19-18) Adobe Acrobat Reader Double Free Remote Code Execution (CVE-2019-7784)
MTIS19-023-G

IMPORTANCE: Low
COVERED PRODUCTS: Vulnerability Manager
UNDER ANALYSIS: DAT | Web Gateway | Firewall Enterprise

Back to top

(APSB19-18) Adobe Acrobat Reader Use After Free Remote Code Execution (CVE-2019-7785)
MTIS19-023-H

IMPORTANCE: Low
COVERED PRODUCTS: Vulnerability Manager
UNDER ANALYSIS: DAT | Web Gateway | Firewall Enterprise

Back to top

(APSB19-18) Adobe Acrobat Reader Use After Free Remote Code Execution (CVE-2019-7786)
MTIS19-023-I

IMPORTANCE: Low
COVERED PRODUCTS: Vulnerability Manager
UNDER ANALYSIS: DAT | Web Gateway | Firewall Enterprise

Back to top

(APSB19-18) Adobe Acrobat Reader Out-of-Bounds Read Information Disclosure (CVE-2019-7787)
MTIS19-023-J

IMPORTANCE: Low
COVERED PRODUCTS: Vulnerability Manager
UNDER ANALYSIS: DAT | Web Gateway | Firewall Enterprise

Back to top

(APSB19-18) Adobe Acrobat Reader Use After Free Remote Code Execution (CVE-2019-7788)
MTIS19-023-K

IMPORTANCE: Low
COVERED PRODUCTS: Vulnerability Manager
UNDER ANALYSIS: DAT | Web Gateway | Firewall Enterprise

Back to top

(APSB19-18) Adobe Acrobat Reader Out-of-Bounds Read Information Disclosure (CVE-2019-7789)
MTIS19-023-L

IMPORTANCE: Low
COVERED PRODUCTS: Vulnerability Manager
UNDER ANALYSIS: DAT | Web Gateway | Firewall Enterprise

Back to top

(APSB19-18) Adobe Acrobat Reader Out-of-Bounds Read Information Disclosure (CVE-2019-7790)
MTIS19-023-M

IMPORTANCE: Low
COVERED PRODUCTS: Vulnerability Manager
UNDER ANALYSIS: DAT | Web Gateway | Firewall Enterprise

Back to top

(APSB19-18) Adobe Acrobat Reader Use After Free Remote Code Execution (CVE-2019-7791)
MTIS19-023-N

IMPORTANCE: Low
COVERED PRODUCTS: Vulnerability Manager
UNDER ANALYSIS: DAT | Web Gateway | Firewall Enterprise

Back to top

(APSB19-18) Adobe Acrobat Reader Use After Free Remote Code Execution (CVE-2019-7792)
MTIS19-023-O

IMPORTANCE: Low
COVERED PRODUCTS: Vulnerability Manager
UNDER ANALYSIS: DAT | Web Gateway | Firewall Enterprise

Back to top

(APSB19-18) Adobe Acrobat Reader Out-of-Bounds Read Information Disclosure (CVE-2019-7793)
MTIS19-023-P

IMPORTANCE: Low
COVERED PRODUCTS: Vulnerability Manager
UNDER ANALYSIS: DAT | Web Gateway | Firewall Enterprise

Back to top

(APSB19-18) Adobe Acrobat Reader Out-of-Bounds Read Information Disclosure (CVE-2019-7794)
MTIS19-023-Q

IMPORTANCE: Low
COVERED PRODUCTS: Vulnerability Manager
UNDER ANALYSIS: DAT | Web Gateway | Firewall Enterprise

Back to top

(APSB19-18) Adobe Acrobat Reader Out-of-Bounds Read Information Disclosure (CVE-2019-7795)
MTIS19-023-R

IMPORTANCE: Low
COVERED PRODUCTS: Vulnerability Manager
UNDER ANALYSIS: DAT | Web Gateway | Firewall Enterprise

Back to top

(APSB19-18) Adobe Acrobat Reader Use After Free Remote Code Execution (CVE-2019-7796)
MTIS19-023-S

IMPORTANCE: Low
COVERED PRODUCTS: Vulnerability Manager
UNDER ANALYSIS: DAT | Web Gateway | Firewall Enterprise

Back to top

(APSB19-18) Adobe Acrobat Reader Use After Free Remote Code Execution (CVE-2019-7797)
MTIS19-023-T

IMPORTANCE: Low
COVERED PRODUCTS: Vulnerability Manager
UNDER ANALYSIS: DAT | Web Gateway | Firewall Enterprise

Back to top

(APSB19-18) Adobe Acrobat Reader Out-of-Bounds Read Information Disclosure (CVE-2019-7798)
MTIS19-023-U

IMPORTANCE:	Low
COVERED PRODUCTS:	Vulnerability Manager
UNDER ANALYSIS:	DAT | Web Gateway | Firewall Enterprise

Back to top

(APSB19-18) Adobe Acrobat Reader Out-of-Bounds Read Information Disclosure (CVE-2019-7799)
MTIS19-023-V

IMPORTANCE:	Low
COVERED PRODUCTS:	Vulnerability Manager
UNDER ANALYSIS:	DAT | Web Gateway | Firewall Enterprise

Back to top

(APSB19-18) Adobe Acrobat Reader Out-of-Bounds Write Remote Code Execution (CVE-2019-7800)
MTIS19-023-W

IMPORTANCE:	Low
COVERED PRODUCTS:	Vulnerability Manager
UNDER ANALYSIS:	DAT | Web Gateway | Firewall Enterprise

Back to top

(APSB19-18) Adobe Acrobat Reader Out-of-Bounds Read Information Disclosure (CVE-2019-7801)
MTIS19-023-X

IMPORTANCE:	Low
COVERED PRODUCTS:	Vulnerability Manager
UNDER ANALYSIS:	DAT | Web Gateway | Firewall Enterprise

Back to top

(APSB19-18) Adobe Acrobat Reader Out-of-Bounds Read Information Disclosure (CVE-2019-7802)
MTIS19-023-Y

IMPORTANCE:	Low
COVERED PRODUCTS:	Vulnerability Manager
UNDER ANALYSIS:	DAT | Web Gateway | Firewall Enterprise

Back to top

(APSB19-18) Adobe Acrobat Reader Out-of-Bounds Read Information Disclosure (CVE-2019-7803)
MTIS19-023-Z

IMPORTANCE:	Low
COVERED PRODUCTS:	Vulnerability Manager
UNDER ANALYSIS:	DAT | Web Gateway | Firewall Enterprise

Back to top

THREAT DETAILS

(APSB19-18) Adobe Acrobat Reader Out-of-Bounds Read Information Disclosure (CVE-2019-7778)
MTIS19-023-A

THREAT IDENTIFIER(S)	CVE-2019-7778
THREAT TYPE	Vulnerability
RISK ASSESSMENT	Medium
MAIN THREAT VECTORS	Web
USER INTERACTION REQUIRED	Yes

DESCRIPTION	A vulnerability in some versions of Adobe Acrobat Reader could lead to information disclosure. The flaw lies in the Out-of-Bounds Read component. Successful exploitation by a remote attacker could result in the disclosure of sensitive information. The exploit requires the user to open a vulnerable website, email or document.
IMPORTANCE	Low. On May 14, Adobe released an update to address this vulnerability
MCAFEE PRODUCT COVERAGE	
DAT FILES	Under analysis
VIRUS SCAN ENTERPRISE SCAN BOP	Out of scope
HOST IPS	Out of scope
NETWORK SECURITY PLATFORM	Coverage not warranted
VULNERABILITY MANAGER	The FSL/MVM package of May 14 includes a vulnerability check to assess if your systems are at risk.
WEB GATEWAY	Under analysis
REMEDIATION MANAGER	Not applicable
POLICY AUDITOR	An upcoming SCAP content release will contain coverage for this issue.
NETWORK ACCESS CONTROL	An upcoming SCAP content release will contain coverage for this issue.
FIREWALL ENTERPRISE	Under analysis
APPLICATION CONTROL	Out of scope
DATABASE ACTIVITY MONITORING	Out of scope
VULNERABILITY MANAGER FOR DATABASES	Out of scope
ADDITIONAL INFORMATION	Adobe: Security Bulletins and Advisories

Back to top

(APSB19-18) Adobe Acrobat Reader Security bypass Remote Code Execution (CVE-2019-7779)

MTIS19-023-B

THREAT IDENTIFIER(S)	CVE-2019-7779
THREAT TYPE	Vulnerability
RISK ASSESSMENT	Medium
MAIN THREAT VECTORS	Web
USER INTERACTION REQUIRED	Yes
DESCRIPTION	A vulnerability in some versions of Adobe Acrobat Reader could lead to remote code execution. The flaw lies in the Security bypass component. Successful exploitation by a remote attacker could result in the execution of arbitrary code. The exploit requires the user to open a vulnerable website, email or document.
IMPORTANCE	Low. On May 14, Adobe released an update to address this vulnerability
MCAFEE PRODUCT COVERAGE	
DAT FILES	Under analysis
VIRUS SCAN ENTERPRISE SCAN BOP	Out of scope
HOST IPS	Out of scope
NETWORK SECURITY PLATFORM	Coverage not warranted
VULNERABILITY MANAGER	The FSL/MVM package of May 14 includes a vulnerability check to assess if your systems are at risk.
WEB GATEWAY	Under analysis
REMEDIATION MANAGER	Not applicable
POLICY AUDITOR	An upcoming SCAP content release will contain coverage for this issue.
NETWORK ACCESS CONTROL	An upcoming SCAP content release will contain coverage for this issue.
FIREWALL ENTERPRISE	Under analysis
APPLICATION CONTROL	Out of scope
DATABASE ACTIVITY MONITORING	Out of scope
VULNERABILITY MANAGER FOR DATABASES	Out of scope
ADDITIONAL INFORMATION	Adobe: Security Bulletins and Advisories

Back to top

(APSB19-18) Adobe Acrobat Reader Out-of-Bounds Read Information Disclosure (CVE-2019-7780)

MTIS19-023-C

THREAT IDENTIFIER(S)	CVE-2019-7780
THREAT TYPE	Vulnerability
RISK ASSESSMENT	Medium
MAIN THREAT VECTORS	Web
USER INTERACTION REQUIRED	Yes
DESCRIPTION	A vulnerability in some versions of Adobe Acrobat Reader could lead to information disclosure. The flaw lies in the Out-of-Bounds Read component. Successful exploitation by a remote attacker could result in the disclosure of sensitive information. The exploit requires the user to open a vulnerable website, email or document.
IMPORTANCE	Low. On May 14, Adobe released an update to address this vulnerability
MCAFEE PRODUCT COVERAGE	
DAT FILES	Under analysis
VIRUS SCAN ENTERPRISE SCAN BOP	Out of scope
HOST IPS	Out of scope
NETWORK SECURITY PLATFORM	Coverage not warranted
VULNERABILITY MANAGER	The FSL/MVM package of May 14 includes a vulnerability check to assess if your systems are at risk.
WEB GATEWAY	Under analysis
REMEDIATION MANAGER	Not applicable
POLICY AUDITOR	An upcoming SCAP content release will contain coverage for this issue.
NETWORK ACCESS CONTROL	An upcoming SCAP content release will contain coverage for this issue.
FIREWALL ENTERPRISE	Under analysis
APPLICATION CONTROL	Out of scope
DATABASE ACTIVITY MONITORING	Out of scope
VULNERABILITY MANAGER FOR DATABASES	Out of scope
ADDITIONAL INFORMATION	Adobe: Security Bulletins and Advisories

Back to top

(APSB19-18) Adobe Acrobat Reader Use After Free Remote Code Execution (CVE-2019-7781)

MTIS19-023-D

THREAT IDENTIFIER(S)	CVE-2019-7781
THREAT TYPE	Vulnerability
RISK ASSESSMENT	Medium
MAIN THREAT VECTORS	Web
USER INTERACTION REQUIRED	Yes
DESCRIPTION	A vulnerability in some versions of Adobe Acrobat Reader could lead to remote code execution. The flaw lies in the Use After Free component. Successful exploitation by a remote attacker could result in the execution of arbitrary code. The exploit requires the user to open a vulnerable website, email or document.
IMPORTANCE	Low. On May 14, Adobe released an update to address this vulnerability
MCAFEE PRODUCT COVERAGE	
DAT FILES	Under analysis
VIRUS SCAN ENTERPRISE SCAN BOP	Out of scope
HOST IPS	Out of scope
NETWORK SECURITY PLATFORM	Coverage not warranted
VULNERABILITY MANAGER	The FSL/MVM package of May 14 includes a vulnerability check to assess if your systems are at risk.
WEB GATEWAY	Under analysis
REMEDIATION MANAGER	Not applicable
POLICY AUDITOR	An upcoming SCAP content release will contain coverage for this issue.
NETWORK ACCESS CONTROL	An upcoming SCAP content release will contain coverage for this issue.

FIREWALL ENTERPRISE	Under analysis
APPLICATION CONTROL	Out of scope
DATABASE ACTIVITY MONITORING	Out of scope
VULNERABILITY MANAGER FOR DATABASES	Out of scope
ADDITIONAL INFORMATION	Adobe: Security Bulletins and Advisories

Back to top

(APSB19-18) Adobe Acrobat Reader Use After Free Remote Code Execution (CVE-2019-7782)

MTIS19-023-E

THREAT IDENTIFIER(S)	CVE-2019-7782
THREAT TYPE	Vulnerability
RISK ASSESSMENT	Medium
MAIN THREAT VECTORS	Web
USER INTERACTION REQUIRED	Yes
DESCRIPTION	A vulnerability in some versions of Adobe Acrobat Reader could lead to remote code execution. The flaw lies in the Use After Free component. Successful exploitation by a remote attacker could result in the execution of arbitrary code. The exploit requires the user to open a vulnerable website, email or document.
IMPORTANCE	Low. On May 14, Adobe released an update to address this vulnerability
MCAFEE PRODUCT COVERAGE	
DAT FILES	Under analysis
VIRUS SCAN ENTERPRISE SCAN BOP	Out of scope
HOST IPS	Out of scope
NETWORK SECURITY PLATFORM	Coverage not warranted
VULNERABILITY MANAGER	The FSL/MVM package of May 14 includes a vulnerability check to assess if your systems are at risk.
WEB GATEWAY	Under analysis
REMEDIATION MANAGER	Not applicable
POLICY AUDITOR	An upcoming SCAP content release will contain coverage for this issue.
NETWORK ACCESS CONTROL	An upcoming SCAP content release will contain coverage for this issue.
FIREWALL ENTERPRISE	Under analysis
APPLICATION CONTROL	Out of scope
DATABASE ACTIVITY MONITORING	Out of scope
VULNERABILITY MANAGER FOR DATABASES	Out of scope
ADDITIONAL INFORMATION	Adobe: Security Bulletins and Advisories

Back to top

(APSB19-18) Adobe Acrobat Reader Use After Free Remote Code Execution (CVE-2019-7783)

MTIS19-023-F

THREAT IDENTIFIER(S)	CVE-2019-7783
THREAT TYPE	Vulnerability
RISK ASSESSMENT	Medium
MAIN THREAT VECTORS	Web
USER INTERACTION REQUIRED	Yes
DESCRIPTION	A vulnerability in some versions of Adobe Acrobat Reader could lead to remote code execution. The flaw lies in the Use After Free component. Successful exploitation by a remote attacker could result in the execution of arbitrary code. The exploit requires the user to open a vulnerable website, email or document.
IMPORTANCE	Low. On May 14, Adobe released an update to address this vulnerability
MCAFEE PRODUCT COVERAGE	
DAT FILES	Under analysis
VIRUS SCAN ENTERPRISE SCAN BOP	Out of scope
HOST IPS	Out of scope

NETWORK SECURITY PLATFORM	Coverage not warranted
VULNERABILITY MANAGER	The FSL/MVM package of May 14 includes a vulnerability check to assess if your systems are at risk.
WEB GATEWAY	Under analysis
REMEDIATION MANAGER	Not applicable
POLICY AUDITOR	An upcoming SCAP content release will contain coverage for this issue.
NETWORK ACCESS CONTROL	An upcoming SCAP content release will contain coverage for this issue.
FIREWALL ENTERPRISE	Under analysis
APPLICATION CONTROL	Out of scope
DATABASE ACTIVITY MONITORING	Out of scope
VULNERABILITY MANAGER FOR DATABASES	Out of scope
ADDITIONAL INFORMATION	Adobe: Security Bulletins and Advisories

Back to top

(APSB19-18) Adobe Acrobat Reader Double Free Remote Code Execution (CVE-2019-7784)

MTIS19-023-G

THREAT IDENTIFIER(S)	CVE-2019-7784
THREAT TYPE	Vulnerability
RISK ASSESSMENT	Medium
MAIN THREAT VECTORS	Web
USER INTERACTION REQUIRED	Yes
DESCRIPTION	A vulnerability in some versions of Adobe Acrobat Reader could lead to remote code execution. The flaw lies in the Double Free component. Successful exploitation by a remote attacker could result in the execution of arbitrary code. The exploit requires the user to open a vulnerable website, email or document.
IMPORTANCE	Low. On May 14, Adobe released an update to address this vulnerability
MCAFEE PRODUCT COVERAGE	
DAT FILES	Under analysis
VIRUS SCAN ENTERPRISE SCAN BOP	Out of scope
HOST IPS	Out of scope
NETWORK SECURITY PLATFORM	Coverage not warranted
VULNERABILITY MANAGER	The FSL/MVM package of May 14 includes a vulnerability check to assess if your systems are at risk.
WEB GATEWAY	Under analysis
REMEDIATION MANAGER	Not applicable
POLICY AUDITOR	An upcoming SCAP content release will contain coverage for this issue.
NETWORK ACCESS CONTROL	An upcoming SCAP content release will contain coverage for this issue.
FIREWALL ENTERPRISE	Under analysis
APPLICATION CONTROL	Out of scope
DATABASE ACTIVITY MONITORING	Out of scope
VULNERABILITY MANAGER FOR DATABASES	Out of scope
ADDITIONAL INFORMATION	Adobe: Security Bulletins and Advisories

Back to top

(APSB19-18) Adobe Acrobat Reader Use After Free Remote Code Execution (CVE-2019-7785)

MTIS19-023-H

THREAT IDENTIFIER(S)	CVE-2019-7785
THREAT TYPE	Vulnerability
RISK ASSESSMENT	Medium
MAIN THREAT VECTORS	Web
USER INTERACTION REQUIRED	Yes
	A vulnerability in some versions of Adobe Acrobat Reader could lead to remote code

DESCRIPTION	execution. The flaw lies in the Use After Free component. Successful exploitation by a remote attacker could result in the execution of arbitrary code. The exploit requires the user to open a vulnerable website, email or document.
IMPORTANCE	Low. On May 14, Adobe released an update to address this vulnerability
MCAFEE PRODUCT COVERAGE	
DAT FILES	Under analysis
VIRUS SCAN ENTERPRISE SCAN BOP	Out of scope
HOST IPS	Out of scope
NETWORK SECURITY PLATFORM	Coverage not warranted
VULNERABILITY MANAGER	The FSL/MVM package of May 14 includes a vulnerability check to assess if your systems are at risk.
WEB GATEWAY	Under analysis
REMEDIATION MANAGER	Not applicable
POLICY AUDITOR	An upcoming SCAP content release will contain coverage for this issue.
NETWORK ACCESS CONTROL	An upcoming SCAP content release will contain coverage for this issue.
FIREWALL ENTERPRISE	Under analysis
APPLICATION CONTROL	Out of scope
DATABASE ACTIVITY MONITORING	Out of scope
VULNERABILITY MANAGER FOR DATABASES	Out of scope
ADDITIONAL INFORMATION	Adobe: Security Bulletins and Advisories

Back to top

(APSB19-18) Adobe Acrobat Reader Use After Free Remote Code Execution (CVE-2019-7786)

MTIS19-023-I

THREAT IDENTIFIER(S)	CVE-2019-7786
THREAT TYPE	Vulnerability
RISK ASSESSMENT	Medium
MAIN THREAT VECTORS	Web
USER INTERACTION REQUIRED	Yes
DESCRIPTION	A vulnerability in some versions of Adobe Acrobat Reader could lead to remote code execution. The flaw lies in the Use After Free component. Successful exploitation by a remote attacker could result in the execution of arbitrary code. The exploit requires the user to open a vulnerable website, email or document.
IMPORTANCE	Low. On May 14, Adobe released an update to address this vulnerability
MCAFEE PRODUCT COVERAGE	
DAT FILES	Under analysis
VIRUS SCAN ENTERPRISE SCAN BOP	Out of scope
HOST IPS	Out of scope
NETWORK SECURITY PLATFORM	Coverage not warranted
VULNERABILITY MANAGER	The FSL/MVM package of May 14 includes a vulnerability check to assess if your systems are at risk.
WEB GATEWAY	Under analysis
REMEDIATION MANAGER	Not applicable
POLICY AUDITOR	An upcoming SCAP content release will contain coverage for this issue.
NETWORK ACCESS CONTROL	An upcoming SCAP content release will contain coverage for this issue.
FIREWALL ENTERPRISE	Under analysis
APPLICATION CONTROL	Out of scope
DATABASE ACTIVITY MONITORING	Out of scope
VULNERABILITY MANAGER FOR DATABASES	Out of scope
ADDITIONAL INFORMATION	Adobe: Security Bulletins and Advisories

Back to top

(APSB19-18) Adobe Acrobat Reader Out-of-Bounds Read Information Disclosure (CVE-2019-7787)

MTIS19-023-J

THREAT IDENTIFIER(S)	CVE-2019-7787
THREAT TYPE	Vulnerability
RISK ASSESSMENT	Medium
MAIN THREAT VECTORS	Web
USER INTERACTION REQUIRED	Yes
DESCRIPTION	A vulnerability in some versions of Adobe Acrobat Reader could lead to information disclosure. The flaw lies in the Out-of-Bounds Read component. Successful exploitation by a remote attacker could result in the disclosure of sensitive information. The exploit requires the user to open a vulnerable website, email or document.
IMPORTANCE	Low. On May 14, Adobe released an update to address this vulnerability
MCAFEE PRODUCT COVERAGE	
DAT FILES	Under analysis
VIRUS SCAN ENTERPRISE SCAN BOP	Out of scope
HOST IPS	Out of scope
NETWORK SECURITY PLATFORM	Coverage not warranted
VULNERABILITY MANAGER	The FSL/MVM package of May 14 includes a vulnerability check to assess if your systems are at risk.
WEB GATEWAY	Under analysis
REMEDIATION MANAGER	Not applicable
POLICY AUDITOR	An upcoming SCAP content release will contain coverage for this issue.
NETWORK ACCESS CONTROL	An upcoming SCAP content release will contain coverage for this issue.
FIREWALL ENTERPRISE	Under analysis
APPLICATION CONTROL	Out of scope
DATABASE ACTIVITY MONITORING	Out of scope
VULNERABILITY MANAGER FOR DATABASES	Out of scope
ADDITIONAL INFORMATION	Adobe: Security Bulletins and Advisories

Back to top

(APSB19-18) Adobe Acrobat Reader Use After Free Remote Code Execution (CVE-2019-7788)

MTIS19-023-K

THREAT IDENTIFIER(S)	CVE-2019-7788
THREAT TYPE	Vulnerability
RISK ASSESSMENT	Medium
MAIN THREAT VECTORS	Web
USER INTERACTION REQUIRED	Yes
DESCRIPTION	A vulnerability in some versions of Adobe Acrobat Reader could lead to remote code execution. The flaw lies in the Use After Free component. Successful exploitation by a remote attacker could result in the execution of arbitrary code. The exploit requires the user to open a vulnerable website, email or document.
IMPORTANCE	Low. On May 14, Adobe released an update to address this vulnerability
MCAFEE PRODUCT COVERAGE	
DAT FILES	Under analysis
VIRUS SCAN ENTERPRISE SCAN BOP	Out of scope
HOST IPS	Out of scope
NETWORK SECURITY PLATFORM	Coverage not warranted
VULNERABILITY MANAGER	The FSL/MVM package of May 14 includes a vulnerability check to assess if your systems are at risk.
WEB GATEWAY	Under analysis
REMEDIATION MANAGER	Not applicable
POLICY AUDITOR	An upcoming SCAP content release will contain coverage for this issue.
NETWORK ACCESS CONTROL	An upcoming SCAP content release will contain coverage for this issue.
FIREWALL ENTERPRISE	Under analysis

APPLICATION CONTROL	Out of scope
DATABASE ACTIVITY MONITORING	Out of scope
VULNERABILITY MANAGER FOR DATABASES	Out of scope
ADDITIONAL INFORMATION	Adobe: Security Bulletins and Advisories

Back to top

(APSB19-18) Adobe Acrobat Reader Out-of-Bounds Read Information Disclosure (CVE-2019-7789)

MTIS19-023-L

THREAT IDENTIFIER(S)	CVE-2019-7789
THREAT TYPE	Vulnerability
RISK ASSESSMENT	Medium
MAIN THREAT VECTORS	Web
USER INTERACTION REQUIRED	Yes
DESCRIPTION	A vulnerability in some versions of Adobe Acrobat Reader could lead to information disclosure. The flaw lies in the Out-of-Bounds Read component. Successful exploitation by a remote attacker could result in the disclosure of sensitive information. The exploit requires the user to open a vulnerable website, email or document.
IMPORTANCE	Low. On May 14, Adobe released an update to address this vulnerability
MCAFEE PRODUCT COVERAGE	
DAT FILES	Under analysis
VIRUS SCAN ENTERPRISE SCAN BOP	Out of scope
HOST IPS	Out of scope
NETWORK SECURITY PLATFORM	Coverage not warranted
VULNERABILITY MANAGER	The FSL/MVM package of May 14 includes a vulnerability check to assess if your systems are at risk.
WEB GATEWAY	Under analysis
REMEDIATION MANAGER	Not applicable
POLICY AUDITOR	An upcoming SCAP content release will contain coverage for this issue.
NETWORK ACCESS CONTROL	An upcoming SCAP content release will contain coverage for this issue.
FIREWALL ENTERPRISE	Under analysis
APPLICATION CONTROL	Out of scope
DATABASE ACTIVITY MONITORING	Out of scope
VULNERABILITY MANAGER FOR DATABASES	Out of scope
ADDITIONAL INFORMATION	Adobe: Security Bulletins and Advisories

Back to top

(APSB19-18) Adobe Acrobat Reader Out-of-Bounds Read Information Disclosure (CVE-2019-7790)

MTIS19-023-M

THREAT IDENTIFIER(S)	CVE-2019-7790
THREAT TYPE	Vulnerability
RISK ASSESSMENT	Medium
MAIN THREAT VECTORS	Web
USER INTERACTION REQUIRED	Yes
DESCRIPTION	A vulnerability in some versions of Adobe Acrobat Reader could lead to information disclosure. The flaw lies in the Out-of-Bounds Read component. Successful exploitation by a remote attacker could result in the disclosure of sensitive information. The exploit requires the user to open a vulnerable website, email or document.
IMPORTANCE	Low. On May 14, Adobe released an update to address this vulnerability
MCAFEE PRODUCT COVERAGE	
DAT FILES	Under analysis
VIRUS SCAN ENTERPRISE SCAN BOP	Out of scope
HOST IPS	Out of scope

NETWORK SECURITY PLATFORM	Coverage not warranted
VULNERABILITY MANAGER	The FSL/MVM package of May 14 includes a vulnerability check to assess if your systems are at risk.
WEB GATEWAY	Under analysis
REMEDIATION MANAGER	Not applicable
POLICY AUDITOR	An upcoming SCAP content release will contain coverage for this issue.
NETWORK ACCESS CONTROL	An upcoming SCAP content release will contain coverage for this issue.
FIREWALL ENTERPRISE	Under analysis
APPLICATION CONTROL	Out of scope
DATABASE ACTIVITY MONITORING	Out of scope
VULNERABILITY MANAGER FOR DATABASES	Out of scope
ADDITIONAL INFORMATION	Adobe: Security Bulletins and Advisories

Back to top

(APSB19-18) Adobe Acrobat Reader Use After Free Remote Code Execution (CVE-2019-7791)

MTIS19-023-N

THREAT IDENTIFIER(S)	CVE-2019-7791
THREAT TYPE	Vulnerability
RISK ASSESSMENT	Medium
MAIN THREAT VECTORS	Web
USER INTERACTION REQUIRED	Yes
DESCRIPTION	A vulnerability in some versions of Adobe Acrobat Reader could lead to remote code execution. The flaw lies in the Use After Free component. Successful exploitation by a remote attacker could result in the execution of arbitrary code. The exploit requires the user to open a vulnerable website, email or document.
IMPORTANCE	Low. On May 14, Adobe released an update to address this vulnerability
MCAFEE PRODUCT COVERAGE	
DAT FILES	Under analysis
VIRUS SCAN ENTERPRISE SCAN BOP	Out of scope
HOST IPS	Out of scope
NETWORK SECURITY PLATFORM	Coverage not warranted
VULNERABILITY MANAGER	The FSL/MVM package of May 14 includes a vulnerability check to assess if your systems are at risk.
WEB GATEWAY	Under analysis
REMEDIATION MANAGER	Not applicable
POLICY AUDITOR	An upcoming SCAP content release will contain coverage for this issue.
NETWORK ACCESS CONTROL	An upcoming SCAP content release will contain coverage for this issue.
FIREWALL ENTERPRISE	Under analysis
APPLICATION CONTROL	Out of scope
DATABASE ACTIVITY MONITORING	Out of scope
VULNERABILITY MANAGER FOR DATABASES	Out of scope
ADDITIONAL INFORMATION	Adobe: Security Bulletins and Advisories

Back to top

(APSB19-18) Adobe Acrobat Reader Use After Free Remote Code Execution (CVE-2019-7792)

MTIS19-023-O

THREAT IDENTIFIER(S)	CVE-2019-7792
THREAT TYPE	Vulnerability
RISK ASSESSMENT	Medium
MAIN THREAT VECTORS	Web
USER INTERACTION REQUIRED	Yes
	A vulnerability in some versions of Adobe Acrobat Reader could lead to remote code

DESCRIPTION	execution. The flaw lies in the Use After Free component. Successful exploitation by a remote attacker could result in the execution of arbitrary code. The exploit requires the user to open a vulnerable website, email or document.
IMPORTANCE	Low. On May 14, Adobe released an update to address this vulnerability
MCAFEE PRODUCT COVERAGE	
DAT FILES	Under analysis
VIRUS SCAN ENTERPRISE SCAN BOP	Out of scope
HOST IPS	Out of scope
NETWORK SECURITY PLATFORM	Coverage not warranted
VULNERABILITY MANAGER	The FSL/MVM package of May 14 includes a vulnerability check to assess if your systems are at risk.
WEB GATEWAY	Under analysis
REMEDIATION MANAGER	Not applicable
POLICY AUDITOR	An upcoming SCAP content release will contain coverage for this issue.
NETWORK ACCESS CONTROL	An upcoming SCAP content release will contain coverage for this issue.
FIREWALL ENTERPRISE	Under analysis
APPLICATION CONTROL	Out of scope
DATABASE ACTIVITY MONITORING	Out of scope
VULNERABILITY MANAGER FOR DATABASES	Out of scope
ADDITIONAL INFORMATION	Adobe: Security Bulletins and Advisories

Back to top

(APSB19-18) Adobe Acrobat Reader Out-of-Bounds Read Information Disclosure (CVE-2019-7793)

MTIS19-023-P

THREAT IDENTIFIER(S)	CVE-2019-7793
THREAT TYPE	Vulnerability
RISK ASSESSMENT	Medium
MAIN THREAT VECTORS	Web
USER INTERACTION REQUIRED	Yes
DESCRIPTION	A vulnerability in some versions of Adobe Acrobat Reader could lead to information disclosure. The flaw lies in the Out-of-Bounds Read component. Successful exploitation by a remote attacker could result in the disclosure of sensitive information. The exploit requires the user to open a vulnerable website, email or document.
IMPORTANCE	Low. On May 14, Adobe released an update to address this vulnerability
MCAFEE PRODUCT COVERAGE	
DAT FILES	Under analysis
VIRUS SCAN ENTERPRISE SCAN BOP	Out of scope
HOST IPS	Out of scope
NETWORK SECURITY PLATFORM	Coverage not warranted
VULNERABILITY MANAGER	The FSL/MVM package of May 14 includes a vulnerability check to assess if your systems are at risk.
WEB GATEWAY	Under analysis
REMEDIATION MANAGER	Not applicable
POLICY AUDITOR	An upcoming SCAP content release will contain coverage for this issue.
NETWORK ACCESS CONTROL	An upcoming SCAP content release will contain coverage for this issue.
FIREWALL ENTERPRISE	Under analysis
APPLICATION CONTROL	Out of scope
DATABASE ACTIVITY MONITORING	Out of scope
VULNERABILITY MANAGER FOR DATABASES	Out of scope
ADDITIONAL INFORMATION	Adobe: Security Bulletins and Advisories

Back to top

(APSB19-18) Adobe Acrobat Reader Out-of-Bounds Read Information Disclosure (CVE-2019-7794)

MTIS19-023-Q

THREAT IDENTIFIER(S)	CVE-2019-7794
THREAT TYPE	Vulnerability
RISK ASSESSMENT	Medium
MAIN THREAT VECTORS	Web
USER INTERACTION REQUIRED	Yes
DESCRIPTION	A vulnerability in some versions of Adobe Acrobat Reader could lead to information disclosure. The flaw lies in the Out-of-Bounds Read component. Successful exploitation by a remote attacker could result in the disclosure of sensitive information. The exploit requires the user to open a vulnerable website, email or document.
IMPORTANCE	Low. On May 14, Adobe released an update to address this vulnerability
MCAFEE PRODUCT COVERAGE	
DAT FILES	Under analysis
VIRUS SCAN ENTERPRISE SCAN BOP	Out of scope
HOST IPS	Out of scope
NETWORK SECURITY PLATFORM	Coverage not warranted
VULNERABILITY MANAGER	The FSL/MVM package of May 14 includes a vulnerability check to assess if your systems are at risk.
WEB GATEWAY	Under analysis
REMEDIATION MANAGER	Not applicable
POLICY AUDITOR	An upcoming SCAP content release will contain coverage for this issue.
NETWORK ACCESS CONTROL	An upcoming SCAP content release will contain coverage for this issue.
FIREWALL ENTERPRISE	Under analysis
APPLICATION CONTROL	Out of scope
DATABASE ACTIVITY MONITORING	Out of scope
VULNERABILITY MANAGER FOR DATABASES	Out of scope
ADDITIONAL INFORMATION	Adobe: Security Bulletins and Advisories

Back to top

(APSB19-18) Adobe Acrobat Reader Out-of-Bounds Read Information Disclosure (CVE-2019-7795)

MTIS19-023-R

THREAT IDENTIFIER(S)	CVE-2019-7795
THREAT TYPE	Vulnerability
RISK ASSESSMENT	Medium
MAIN THREAT VECTORS	Web
USER INTERACTION REQUIRED	Yes
DESCRIPTION	A vulnerability in some versions of Adobe Acrobat Reader could lead to information disclosure. The flaw lies in the Out-of-Bounds Read component. Successful exploitation by a remote attacker could result in the disclosure of sensitive information. The exploit requires the user to open a vulnerable website, email or document.
IMPORTANCE	Low. On May 14, Adobe released an update to address this vulnerability
MCAFEE PRODUCT COVERAGE	
DAT FILES	Under analysis
VIRUS SCAN ENTERPRISE SCAN BOP	Out of scope
HOST IPS	Out of scope
NETWORK SECURITY PLATFORM	Coverage not warranted
VULNERABILITY MANAGER	The FSL/MVM package of May 14 includes a vulnerability check to assess if your systems are at risk.
WEB GATEWAY	Under analysis
REMEDIATION MANAGER	Not applicable
POLICY AUDITOR	An upcoming SCAP content release will contain coverage for this issue.
NETWORK ACCESS CONTROL	An upcoming SCAP content release will contain coverage for this issue.

FIREWALL ENTERPRISE	Under analysis
APPLICATION CONTROL	Out of scope
DATABASE ACTIVITY MONITORING	Out of scope
VULNERABILITY MANAGER FOR DATABASES	Out of scope
ADDITIONAL INFORMATION	Adobe: Security Bulletins and Advisories

Back to top

(APSB19-18) Adobe Acrobat Reader Use After Free Remote Code Execution (CVE-2019-7796)

MTIS19-023-S

THREAT IDENTIFIER(S)	CVE-2019-7796
THREAT TYPE	Vulnerability
RISK ASSESSMENT	Medium
MAIN THREAT VECTORS	Web
USER INTERACTION REQUIRED	Yes
DESCRIPTION	A vulnerability in some versions of Adobe Acrobat Reader could lead to remote code execution. The flaw lies in the Use After Free component. Successful exploitation by a remote attacker could result in the execution of arbitrary code. The exploit requires the user to open a vulnerable website, email or document.
IMPORTANCE	Low. On May 14, Adobe released an update to address this vulnerability
MCAFEE PRODUCT COVERAGE	
DAT FILES	Under analysis
VIRUS SCAN ENTERPRISE SCAN BOP	Out of scope
HOST IPS	Out of scope
NETWORK SECURITY PLATFORM	Coverage not warranted
VULNERABILITY MANAGER	The FSL/MVM package of May 14 includes a vulnerability check to assess if your systems are at risk.
WEB GATEWAY	Under analysis
REMEDIATION MANAGER	Not applicable
POLICY AUDITOR	An upcoming SCAP content release will contain coverage for this issue.
NETWORK ACCESS CONTROL	An upcoming SCAP content release will contain coverage for this issue.
FIREWALL ENTERPRISE	Under analysis
APPLICATION CONTROL	Out of scope
DATABASE ACTIVITY MONITORING	Out of scope
VULNERABILITY MANAGER FOR DATABASES	Out of scope
ADDITIONAL INFORMATION	Adobe: Security Bulletins and Advisories

Back to top

(APSB19-18) Adobe Acrobat Reader Use After Free Remote Code Execution (CVE-2019-7797)

MTIS19-023-T

THREAT IDENTIFIER(S)	CVE-2019-7797
THREAT TYPE	Vulnerability
RISK ASSESSMENT	Medium
MAIN THREAT VECTORS	Web
USER INTERACTION REQUIRED	Yes
DESCRIPTION	A vulnerability in some versions of Adobe Acrobat Reader could lead to remote code execution. The flaw lies in the Use After Free component. Successful exploitation by a remote attacker could result in the execution of arbitrary code. The exploit requires the user to open a vulnerable website, email or document.
IMPORTANCE	Low. On May 14, Adobe released an update to address this vulnerability
MCAFEE PRODUCT COVERAGE	
DAT FILES	Under analysis
VIRUS SCAN ENTERPRISE SCAN BOP	Out of scope
HOST IPS	Out of scope

NETWORK SECURITY PLATFORM	Coverage not warranted
VULNERABILITY MANAGER	The FSL/MVM package of May 14 includes a vulnerability check to assess if your systems are at risk.
WEB GATEWAY	Under analysis
REMEDIATION MANAGER	Not applicable
POLICY AUDITOR	An upcoming SCAP content release will contain coverage for this issue.
NETWORK ACCESS CONTROL	An upcoming SCAP content release will contain coverage for this issue.
FIREWALL ENTERPRISE	Under analysis
APPLICATION CONTROL	Out of scope
DATABASE ACTIVITY MONITORING	Out of scope
VULNERABILITY MANAGER FOR DATABASES	Out of scope
ADDITIONAL INFORMATION	Adobe: Security Bulletins and Advisories

Back to top

(APSB19-18) Adobe Acrobat Reader Out-of-Bounds Read Information Disclosure (CVE-2019-7798)

MTIS19-023-U

THREAT IDENTIFIER(S)	CVE-2019-7798
THREAT TYPE	Vulnerability
RISK ASSESSMENT	Medium
MAIN THREAT VECTORS	Web
USER INTERACTION REQUIRED	Yes
DESCRIPTION	A vulnerability in some versions of Adobe Acrobat Reader could lead to remote code execution. The flaw lies in the Out-of-Bounds Read component. Successful exploitation by a remote attacker could result in the execution of arbitrary code. The exploit requires the user to open a vulnerable website, email or document.
IMPORTANCE	Low. On May 14, Adobe released an update to address this vulnerability
MCAFEE PRODUCT COVERAGE	
DAT FILES	Under analysis
VIRUS SCAN ENTERPRISE SCAN BOP	Out of scope
HOST IPS	Out of scope
NETWORK SECURITY PLATFORM	Coverage not warranted
VULNERABILITY MANAGER	The FSL/MVM package of May 14 includes a vulnerability check to assess if your systems are at risk.
WEB GATEWAY	Under analysis
REMEDIATION MANAGER	Not applicable
POLICY AUDITOR	An upcoming SCAP content release will contain coverage for this issue.
NETWORK ACCESS CONTROL	An upcoming SCAP content release will contain coverage for this issue.
FIREWALL ENTERPRISE	Under analysis
APPLICATION CONTROL	Out of scope
DATABASE ACTIVITY MONITORING	Out of scope
VULNERABILITY MANAGER FOR DATABASES	Out of scope
ADDITIONAL INFORMATION	Adobe: Security Bulletins and Advisories

Back to top

(APSB19-18) Adobe Acrobat Reader Out-of-Bounds Read Information Disclosure (CVE-2019-7799)

MTIS19-023-V

THREAT IDENTIFIER(S)	CVE-2019-7799
THREAT TYPE	Vulnerability
RISK ASSESSMENT	Medium
MAIN THREAT VECTORS	Web
USER INTERACTION REQUIRED	Yes
	A vulnerability in some versions of Adobe Acrobat Reader could lead to information

DESCRIPTION	disclosure. The flaw lies in the Out-of-Bounds Read component. Successful exploitation by a remote attacker could result in the disclosure of sensitive information. The exploit requires the user to open a vulnerable website, email or document.
IMPORTANCE	Low. On May 14, Adobe released an update to address this vulnerability
MCAFEE PRODUCT COVERAGE	
DAT FILES	Under analysis
VIRUS SCAN ENTERPRISE SCAN BOP	Out of scope
HOST IPS	Out of scope
NETWORK SECURITY PLATFORM	Coverage not warranted
VULNERABILITY MANAGER	The FSL/MVM package of May 14 includes a vulnerability check to assess if your systems are at risk.
WEB GATEWAY	Under analysis
REMEDIATION MANAGER	Not applicable
POLICY AUDITOR	An upcoming SCAP content release will contain coverage for this issue.
NETWORK ACCESS CONTROL	An upcoming SCAP content release will contain coverage for this issue.
FIREWALL ENTERPRISE	Under analysis
APPLICATION CONTROL	Out of scope
DATABASE ACTIVITY MONITORING	Out of scope
VULNERABILITY MANAGER FOR DATABASES	Out of scope
ADDITIONAL INFORMATION	Adobe: Security Bulletins and Advisories

Back to top

(APSB19-18) Adobe Acrobat Reader Out-of-Bounds Write Remote Code Execution (CVE-2019-7800)

MTIS19-023-W

THREAT IDENTIFIER(S)	CVE-2019-7800
THREAT TYPE	Vulnerability
RISK ASSESSMENT	Medium
MAIN THREAT VECTORS	Web
USER INTERACTION REQUIRED	Yes
DESCRIPTION	A vulnerability in some versions of Adobe Acrobat Reader could lead to remote code execution. The flaw lies in the Out-of-Bounds Write component. Successful exploitation by a remote attacker could result in the execution of arbitrary code. The exploit requires the user to open a vulnerable website, email or document.
IMPORTANCE	Low. On May 14, Adobe released an update to address this vulnerability
MCAFEE PRODUCT COVERAGE	
DAT FILES	Under analysis
VIRUS SCAN ENTERPRISE SCAN BOP	Out of scope
HOST IPS	Out of scope
NETWORK SECURITY PLATFORM	Coverage not warranted
VULNERABILITY MANAGER	The FSL/MVM package of May 14 includes a vulnerability check to assess if your systems are at risk.
WEB GATEWAY	Under analysis
REMEDIATION MANAGER	Not applicable
POLICY AUDITOR	An upcoming SCAP content release will contain coverage for this issue.
NETWORK ACCESS CONTROL	An upcoming SCAP content release will contain coverage for this issue.
FIREWALL ENTERPRISE	Under analysis
APPLICATION CONTROL	Out of scope
DATABASE ACTIVITY MONITORING	Out of scope
VULNERABILITY MANAGER FOR DATABASES	Out of scope
ADDITIONAL INFORMATION	Adobe: Security Bulletins and Advisories

Back to top

(APSB19-18) Adobe Acrobat Reader Out-of-Bounds Read Information Disclosure (CVE-2019-7801)

MTIS19-023-X

THREAT IDENTIFIER(S)	CVE-2019-7801
THREAT TYPE	Vulnerability
RISK ASSESSMENT	Medium
MAIN THREAT VECTORS	Web
USER INTERACTION REQUIRED	Yes
DESCRIPTION	A vulnerability in some versions of Adobe Acrobat Reader could lead to information disclosure. The flaw lies in the Out-of-Bounds Read component. Successful exploitation by a remote attacker could result in the disclosure of sensitive information. The exploit requires the user to open a vulnerable website, email or document.
IMPORTANCE	Low. On May 14, Adobe released an update to address this vulnerability
MCAFEE PRODUCT COVERAGE	
DAT FILES	Under analysis
VIRUS SCAN ENTERPRISE SCAN BOP	Out of scope
HOST IPS	Out of scope
NETWORK SECURITY PLATFORM	Coverage not warranted
VULNERABILITY MANAGER	The FSL/MVM package of May 14 includes a vulnerability check to assess if your systems are at risk.
WEB GATEWAY	Under analysis
REMEDIATION MANAGER	Not applicable
POLICY AUDITOR	An upcoming SCAP content release will contain coverage for this issue.
NETWORK ACCESS CONTROL	An upcoming SCAP content release will contain coverage for this issue.
FIREWALL ENTERPRISE	Under analysis
APPLICATION CONTROL	Out of scope
DATABASE ACTIVITY MONITORING	Out of scope
VULNERABILITY MANAGER FOR DATABASES	Out of scope
ADDITIONAL INFORMATION	Adobe: Security Bulletins and Advisories

Back to top

(APSB19-18) Adobe Acrobat Reader Out-of-Bounds Read Information Disclosure (CVE-2019-7802)

MTIS19-023-Y

THREAT IDENTIFIER(S)	CVE-2019-7802
THREAT TYPE	Vulnerability
RISK ASSESSMENT	Medium
MAIN THREAT VECTORS	Web
USER INTERACTION REQUIRED	Yes
DESCRIPTION	A vulnerability in some versions of Adobe Acrobat Reader could lead to information disclosure. The flaw lies in the Out-of-Bounds Read component. Successful exploitation by a remote attacker could result in the disclosure of sensitive information. The exploit requires the user to open a vulnerable website, email or document.
IMPORTANCE	Low. On May 14, Adobe released an update to address this vulnerability
MCAFEE PRODUCT COVERAGE	
DAT FILES	Under analysis
VIRUS SCAN ENTERPRISE SCAN BOP	Out of scope
HOST IPS	Out of scope
NETWORK SECURITY PLATFORM	Coverage not warranted
VULNERABILITY MANAGER	The FSL/MVM package of May 14 includes a vulnerability check to assess if your systems are at risk.
WEB GATEWAY	Under analysis
REMEDIATION MANAGER	Not applicable
POLICY AUDITOR	An upcoming SCAP content release will contain coverage for this issue.
NETWORK ACCESS CONTROL	An upcoming SCAP content release will contain coverage for this issue.

FIREWALL ENTERPRISE	Under analysis
APPLICATION CONTROL	Out of scope
DATABASE ACTIVITY MONITORING	Out of scope
VULNERABILITY MANAGER FOR DATABASES	Out of scope
ADDITIONAL INFORMATION	Adobe: Security Bulletins and Advisories

Back to top

(APSB19-18) Adobe Acrobat Reader Out-of-Bounds Read Information Disclosure (CVE-2019-7803)

MTIS19-023-Z

THREAT IDENTIFIER(S)	CVE-2019-7803
THREAT TYPE	Vulnerability
RISK ASSESSMENT	Medium
MAIN THREAT VECTORS	Web
USER INTERACTION REQUIRED	Yes
DESCRIPTION	A vulnerability in some versions of Adobe Acrobat Reader could lead to information disclosure. The flaw lies in the Out-of-Bounds Read component. Successful exploitation by a remote attacker could result in the disclosure of sensitive information. The exploit requires the user to open a vulnerable website, email or document.
IMPORTANCE	Low. On May 14, Adobe released an update to address this vulnerability
MCAFEE PRODUCT COVERAGE	
DAT FILES	Under analysis
VIRUS SCAN ENTERPRISE SCAN BOP	Out of scope
HOST IPS	Out of scope
NETWORK SECURITY PLATFORM	Coverage not warranted
VULNERABILITY MANAGER	The FSL/MVM package of May 14 includes a vulnerability check to assess if your systems are at risk.
WEB GATEWAY	Under analysis
REMEDIATION MANAGER	Not applicable
POLICY AUDITOR	An upcoming SCAP content release will contain coverage for this issue.
NETWORK ACCESS CONTROL	An upcoming SCAP content release will contain coverage for this issue.
FIREWALL ENTERPRISE	Under analysis
APPLICATION CONTROL	Out of scope
DATABASE ACTIVITY MONITORING	Out of scope
VULNERABILITY MANAGER FOR DATABASES	Out of scope
ADDITIONAL INFORMATION	Adobe: Security Bulletins and Advisories

Back to top

For McAfee Technical Support, click here.

For Multi-National Phone Support, click here.

McAfee values your feedback on this Security Advisory. Please reply to this mail with your comments.

McAfee, Inc. 2821 Mission College Blvd, Santa Clara, CA 95054 888.847.8766 www.mcafee.com