NEW THREAT OVERVIEW | PREVIOUS THREATS UPDATES | THREAT DETAILS

EXECUTIVE SUMMARY

September 16, 2013 | MTIS13-147

Since the last McAfee® Labs Security Advisory (September 12), the following noteworthy event has taken place:

- McAfee product coverage has been updated for vulnerabilities in Adobe and Apple products.

NEW THREAT OVERVIEW

Apple Mac OS X CoreGraphics JBIG2 PDF Remote Code Execution

MTIS13-147-A

IMPORTANCE:	High
COVERED PRODUCTS:	Application Control
UNDER ANALYSIS:	DAT | BOP | Host IPS | Network Security Platform | Vulnerability Manager | Web Gateway | Remediation Manager | Policy Auditor SCAP | MNAC 2.x | Firewall Enterprise

Back to top

Apple Mac OS X ImageIO JPEG2000 PDF Remote Code Execution

MTIS13-147-B

IMPORTANCE:	High
COVERED PRODUCTS:	Application Control
UNDER ANALYSIS:	DAT | BOP | Host IPS | Network Security Platform | Vulnerability Manager | Web Gateway | Remediation Manager | Policy Auditor SCAP | MNAC 2.x | Firewall Enterprise

Back to top

Apple Mac OS X PHP Remote Code Execution IV

MTIS13-147-C

IMPORTANCE:	High
COVERED PRODUCTS:	Application Control
UNDER ANALYSIS:	DAT | BOP | Host IPS | Network Security Platform | Vulnerability Manager | Web Gateway | Remediation Manager | Policy Auditor SCAP | MNAC 2.x | Firewall Enterprise

Back to top

Apple Mac OS X PHP Remote Code Execution V

MTIS13-147-D

IMPORTANCE:	High
COVERED PRODUCTS:	Application Control
UNDER ANALYSIS:	DAT | BOP | Host IPS | Network Security Platform | Vulnerability Manager | Web Gateway | Remediation Manager | Policy Auditor SCAP | MNAC 2.x | Firewall Enterprise

Back to top

Apple Mac OS X PHP Remote Code Execution VI
MTIS13-147-E

IMPORTANCE:	High
COVERED PRODUCTS:	Application Control
UNDER ANALYSIS:	DAT | BOP | Host IPS | Network Security Platform | Vulnerability Manager | Web Gateway | Remediation Manager | Policy Auditor SCAP | MNAC 2.x | Firewall Enterprise

Back to top

Apple Mac OS X QuickTime idsc Atoms Remote Code Execution
MTIS13-147-F

IMPORTANCE:	High
COVERED PRODUCTS:	Application Control
UNDER ANALYSIS:	DAT | BOP | Host IPS | Network Security Platform | Vulnerability Manager | Web Gateway | Remediation Manager | Policy Auditor SCAP | MNAC 2.x | Firewall Enterprise

Back to top

PREVIOUS THREAT UPDATES

(APSB13-21) Adobe Flash Player Remote Code Execution I
MTIS13-146-A

IMPORTANCE:	High
NOW COVERED:	BOP | Host IPS | Vulnerability Manager | Application Control

Back to top

(APSB13-21) Adobe Flash Player Remote Code Execution II
MTIS13-146-B

IMPORTANCE:	High
NOW COVERED:	BOP | Host IPS | Vulnerability Manager | Application Control

Back to top

(APSB13-21) Adobe Flash Player Remote Code Execution III
MTIS13-146-C

IMPORTANCE:	High
NOW COVERED:	BOP | Host IPS | Vulnerability Manager | Application Control

Back to top

(APSB13-21) Adobe Flash Player Remote Code Execution IV
MTIS13-146-D

IMPORTANCE:	High
NOW COVERED:	BOP | Host IPS | Vulnerability Manager | Application Control

Back to top

(APSB13-22) Adobe Reader and Acrobat Remote Code Execution I
MTIS13-146-E

IMPORTANCE:	High
NOW COVERED:	BOP | Host IPS | Vulnerability Manager | Application Control

Back to top

(APSB13-22) Adobe Reader and Acrobat Remote Code Execution II
MTIS13-146-F

IMPORTANCE:	High
NOW COVERED:	BOP | Host IPS | Vulnerability Manager | Application Control

Back to top

(APSB13-22) Adobe Reader and Acrobat Remote Code Execution III

MTIS13-146-G

IMPORTANCE: High
NOW COVERED: BOP | Host IPS | Vulnerability Manager | Application Control

Back to top

(APSB13-22) Adobe Reader and Acrobat Remote Code Execution IV

MTIS13-146-H

IMPORTANCE: High
NOW COVERED: BOP | Host IPS | Vulnerability Manager | Application Control

Back to top

(APSB13-22) Adobe Reader and Acrobat Remote Code Execution V

MTIS13-146-I

IMPORTANCE: High
NOW COVERED: BOP | Host IPS | Vulnerability Manager | Application Control

Back to top

(APSB13-22) Adobe Reader and Acrobat Remote Code Execution VI

MTIS13-146-J

IMPORTANCE: High
NOW COVERED: BOP | Host IPS | Vulnerability Manager | Application Control

Back to top

(APSB13-22) Adobe Reader and Acrobat Remote Code Execution VII

MTIS13-146-K

IMPORTANCE: High
NOW COVERED: BOP | Host IPS | Vulnerability Manager | Application Control

Back to top

(APSB13-22) Adobe Reader and Acrobat Remote Code Execution VIII

MTIS13-146-L

IMPORTANCE: High
NOW COVERED: BOP | Host IPS | Vulnerability Manager | Application Control

Back to top

(APSB13-23) Adobe Shockwave Player Remote Code Execution I

MTIS13-146-M

IMPORTANCE: High
NOW COVERED: BOP | Host IPS | Vulnerability Manager | Application Control

Back to top

(APSB13-23) Adobe Shockwave Player Remote Code Execution II

MTIS13-146-N

IMPORTANCE: High
NOW COVERED: BOP | Host IPS | Vulnerability Manager | Application Control

Back to top

THREAT DETAILS

Apple Mac OS X CoreGraphics JBIG2 PDF Remote Code Execution

MTIS13-147-A

THREAT IDENTIFIER(S)	CVE-2013-1025
THREAT TYPE	Vulnerability
RISK ASSESSMENT	High
MAIN THREAT VECTORS	Web; E-Mail
USER INTERACTION REQUIRED	Yes
DESCRIPTION	A vulnerability in some versions of Apple Mac OS X could lead to remote code execution. The flaw is due to how JBIG2-encoded data in PDF files is handled. Successful exploitation by a remote attacker could result in the execution of arbitrary code or a denial of service.
IMPORTANCE	High. On September 12, Apple released an update to address this vulnerability.
MCAFEE PRODUCT COVERAGE	
DAT FILES	Under analysis
VIRUS SCAN ENTERPRISE SCAN BOP	Under analysis
HOST IPS	Under analysis
NETWORK SECURITY PLATFORM	Under analysis
VULNERABILITY MANAGER	Under analysis
WEB GATEWAY	Under analysis
REMEDIATION MANAGER	Under analysis
POLICY AUDITOR	Under analysis
NETWORK ACCESS CONTROL	Under analysis
FIREWALL ENTERPRISE	Under analysis
APPLICATION CONTROL	Run-Time Control locks down systems and provides protection in the form of Execution Control and Memory Protection.
DATABASE ACTIVITY MONITORING	Out of scope
VULNERABILITY MANAGER FOR DATABASES	Out of scope
ADDITIONAL INFORMATION	Apple: About the security content of OS X Mountain Lion v10.8.5 and Security Update 2013-004

Back to top

Apple Mac OS X ImageIO JPEG2000 PDF Remote Code Execution

MTIS13-147-B

THREAT IDENTIFIER(S)	CVE-2013-1026
THREAT TYPE	Vulnerability
RISK ASSESSMENT	High
MAIN THREAT VECTORS	Web; E-Mail
USER INTERACTION REQUIRED	Yes
DESCRIPTION	A vulnerability in some versions of Apple Mac OS X could lead to remote code execution. The flaw is due to how JPEG2000-encoded data in PDF files is handled. Successful exploitation by a remote attacker could result in the execution of arbitrary code or a denial of service.
IMPORTANCE	High. On September 12, Apple released an update to address this vulnerability.
MCAFEE PRODUCT COVERAGE	
DAT FILES	Under analysis
VIRUS SCAN ENTERPRISE SCAN BOP	Under analysis
HOST IPS	Under analysis
NETWORK SECURITY PLATFORM	Under analysis
VULNERABILITY MANAGER	Under analysis
WEB GATEWAY	Under analysis
REMEDIATION MANAGER	Under analysis
POLICY AUDITOR	Under analysis
NETWORK ACCESS CONTROL	Under analysis
FIREWALL ENTERPRISE	Under analysis
APPLICATION CONTROL	Run-Time Control locks down systems and provides protection in the form of Execution Control and Memory Protection.

DATABASE ACTIVITY MONITORING	Out of scope
VULNERABILITY MANAGER FOR DATABASES	Out of scope
ADDITIONAL INFORMATION	Apple: About the security content of OS X Mountain Lion v10.8.5 and Security Update 2013-004

Back to top

Apple Mac OS X PHP Remote Code Execution IV

MTIS13-147-C

THREAT IDENTIFIER(S)	CVE-2013-1635
THREAT TYPE	Vulnerability
RISK ASSESSMENT	High
MAIN THREAT VECTORS	WAN; LAN
USER INTERACTION REQUIRED	No
DESCRIPTION	A vulnerability in some versions of Apple Mac OS X could lead to remote code execution. The flaw lies in the PHP component. Successful exploitation by a remote attacker could result in the execution of arbitrary code.
IMPORTANCE	High. On September 12, Apple released an update to address this vulnerability.
MCAFEE PRODUCT COVERAGE	
DAT FILES	Under analysis
VIRUS SCAN ENTERPRISE SCAN BOP	Under analysis
HOST IPS	Under analysis
NETWORK SECURITY PLATFORM	Under analysis
VULNERABILITY MANAGER	Under analysis
WEB GATEWAY	Under analysis
REMEDIATION MANAGER	Under analysis
POLICY AUDITOR	Under analysis
NETWORK ACCESS CONTROL	Under analysis
FIREWALL ENTERPRISE	Under analysis
APPLICATION CONTROL	Run-Time Control locks down systems and provides protection in the form of Execution Control and Memory Protection.
DATABASE ACTIVITY MONITORING	Out of scope
VULNERABILITY MANAGER FOR DATABASES	Out of scope
ADDITIONAL INFORMATION	Apple: About the security content of OS X Mountain Lion v10.8.5 and Security Update 2013-004

Back to top

Apple Mac OS X PHP Remote Code Execution V

MTIS13-147-D

THREAT IDENTIFIER(S)	CVE-2013-1643
THREAT TYPE	Vulnerability
RISK ASSESSMENT	High
MAIN THREAT VECTORS	WAN; LAN
USER INTERACTION REQUIRED	No
DESCRIPTION	A vulnerability in some versions of Apple Mac OS X could lead to remote code execution. The flaw lies in the PHP component. Successful exploitation by a remote attacker could result in the execution of arbitrary code.
IMPORTANCE	High. On September 12, Apple released an update to address this vulnerability.
MCAFEE PRODUCT COVERAGE	
DAT FILES	Under analysis
VIRUS SCAN ENTERPRISE SCAN BOP	Under analysis
HOST IPS	Under analysis
NETWORK SECURITY PLATFORM	Under analysis
VULNERABILITY MANAGER	Under analysis
WEB GATEWAY	Under analysis

REMEDIATION MANAGER	Under analysis
POLICY AUDITOR	Under analysis
NETWORK ACCESS CONTROL	Under analysis
FIREWALL ENTERPRISE	Under analysis
APPLICATION CONTROL	Run-Time Control locks down systems and provides protection in the form of Execution Control and Memory Protection.
DATABASE ACTIVITY MONITORING	Out of scope
VULNERABILITY MANAGER FOR DATABASES	Out of scope
ADDITIONAL INFORMATION	Apple: About the security content of OS X Mountain Lion v10.8.5 and Security Update 2013-004

Back to top

Apple Mac OS X PHP Remote Code Execution VI

MTIS13-147-E

THREAT IDENTIFIER(S)	CVE-2013-1824
THREAT TYPE	Vulnerability
RISK ASSESSMENT	High
MAIN THREAT VECTORS	WAN; LAN
USER INTERACTION REQUIRED	No
DESCRIPTION	A vulnerability in some versions of Apple Mac OS X could lead to remote code execution. The flaw lies in the PHP component. Successful exploitation by a remote attacker could result in the execution of arbitrary code.
IMPORTANCE	High. On September 12, Apple released an update to address this vulnerability.
MCAFEE PRODUCT COVERAGE	
DAT FILES	Under analysis
VIRUS SCAN ENTERPRISE SCAN BOP	Under analysis
HOST IPS	Under analysis
NETWORK SECURITY PLATFORM	Under analysis
VULNERABILITY MANAGER	Under analysis
WEB GATEWAY	Under analysis
REMEDIATION MANAGER	Under analysis
POLICY AUDITOR	Under analysis
NETWORK ACCESS CONTROL	Under analysis
FIREWALL ENTERPRISE	Under analysis
APPLICATION CONTROL	Run-Time Control locks down systems and provides protection in the form of Execution Control and Memory Protection.
DATABASE ACTIVITY MONITORING	Out of scope
VULNERABILITY MANAGER FOR DATABASES	Out of scope
ADDITIONAL INFORMATION	Apple: About the security content of OS X Mountain Lion v10.8.5 and Security Update 2013-004

Back to top

Apple Mac OS X QuickTime idsc Atoms Remote Code Execution

MTIS13-147-F

THREAT IDENTIFIER(S)	CVE-2013-1032
THREAT TYPE	Vulnerability
RISK ASSESSMENT	High
MAIN THREAT VECTORS	Web; E-Mail
USER INTERACTION REQUIRED	Yes
DESCRIPTION	A vulnerability in some versions of Apple Mac OS X could lead to remote code execution. The flaw is due to how idsc atoms in QuickTime movie files are handled. Successful exploitation by a remote attacker could result in the execution of arbitrary code or a denial of service.
IMPORTANCE	High. On September 12, Apple released an update to address this vulnerability.
MCAFEE PRODUCT COVERAGE	

DAT FILES	Under analysis
VIRUS SCAN ENTERPRISE SCAN BOP	Under analysis
HOST IPS	Under analysis
NETWORK SECURITY PLATFORM	Under analysis
VULNERABILITY MANAGER	Under analysis
WEB GATEWAY	Under analysis
REMEDIATION MANAGER	Under analysis
POLICY AUDITOR	Under analysis
NETWORK ACCESS CONTROL	Under analysis
FIREWALL ENTERPRISE	Under analysis
APPLICATION CONTROL	Run-Time Control locks down systems and provides protection in the form of Execution Control and Memory Protection.
DATABASE ACTIVITY MONITORING	Out of scope
VULNERABILITY MANAGER FOR DATABASES	Out of scope
ADDITIONAL INFORMATION	Apple: About the security content of OS X Mountain Lion v10.8.5 and Security Update 2013-004

Back to top

(APSB13-21) Adobe Flash Player Remote Code Execution I

MTIS13-146-A

THREAT IDENTIFIER(S)	CVE-2013-3361
THREAT TYPE	Vulnerability
RISK ASSESSMENT	High
MAIN THREAT VECTORS	E-Mail; Web
USER INTERACTION REQUIRED	Yes
DESCRIPTION	A vulnerability in some versions of Adobe Flash Player could lead to remote code execution. The flaw is due to memory corruption. Successful exploitation by a remote attacker could result in the execution of arbitrary code or a denial of service.
IMPORTANCE	High. On September 10, Adobe released an update to address this vulnerability.
MCAFEE PRODUCT COVERAGE	
DAT FILES	Under analysis
VIRUS SCAN ENTERPRISE SCAN BOP	Generic buffer overflow protection is expected to cover code execution exploits.
HOST IPS	Generic buffer overflow protection is expected to cover code execution exploits.
NETWORK SECURITY PLATFORM	Under analysis
VULNERABILITY MANAGER	The FSL/MVM package of September 11 includes a vulnerability check to assess if your systems are at risk.
WEB GATEWAY	Under analysis
REMEDIATION MANAGER	Under analysis
POLICY AUDITOR	Under analysis
NETWORK ACCESS CONTROL	Under analysis
FIREWALL ENTERPRISE	Under analysis
APPLICATION CONTROL	Run-Time Control locks down systems and provides protection in the form of Execution Control and Memory Protection.
DATABASE ACTIVITY MONITORING	Out of scope
VULNERABILITY MANAGER FOR DATABASES	Out of scope
ADDITIONAL INFORMATION	Adobe: Security updates available for Adobe Flash Player

Back to top

(APSB13-21) Adobe Flash Player Remote Code Execution II

MTIS13-146-B

THREAT IDENTIFIER(S)	CVE-2013-3362
THREAT TYPE	Vulnerability
RISK ASSESSMENT	High
MAIN THREAT VECTORS	E-Mail; Web

USER INTERACTION REQUIRED	Yes
DESCRIPTION	A vulnerability in some versions of Adobe Flash Player could lead to remote code execution. The flaw is due to memory corruption. Successful exploitation by a remote attacker could result in the execution of arbitrary code or a denial of service.
IMPORTANCE	High. On September 10, Adobe released an update to address this vulnerability.
MCAFEE PRODUCT COVERAGE	
DAT FILES	Under analysis
VIRUS SCAN ENTERPRISE SCAN BOP	Generic buffer overflow protection is expected to cover code execution exploits.
HOST IPS	Generic buffer overflow protection is expected to cover code execution exploits.
NETWORK SECURITY PLATFORM	Under analysis
VULNERABILITY MANAGER	The FSL/MVM package of September 11 includes a vulnerability check to assess if your systems are at risk.
WEB GATEWAY	Under analysis
REMEDIATION MANAGER	Under analysis
POLICY AUDITOR	Under analysis
NETWORK ACCESS CONTROL	Under analysis
FIREWALL ENTERPRISE	Under analysis
APPLICATION CONTROL	Run-Time Control locks down systems and provides protection in the form of Execution Control and Memory Protection.
DATABASE ACTIVITY MONITORING	Out of scope
VULNERABILITY MANAGER FOR DATABASES	Out of scope
ADDITIONAL INFORMATION	Adobe: Security updates available for Adobe Flash Player

Back to top

(APSB13-21) Adobe Flash Player Remote Code Execution III

MTIS13-146-C

THREAT IDENTIFIER(S)	CVE-2013-3363
THREAT TYPE	Vulnerability
RISK ASSESSMENT	High
MAIN THREAT VECTORS	E-Mail; Web
USER INTERACTION REQUIRED	Yes
DESCRIPTION	A vulnerability in some versions of Adobe Flash Player could lead to remote code execution. The flaw is due to memory corruption. Successful exploitation by a remote attacker could result in the execution of arbitrary code or a denial of service.
IMPORTANCE	High. On September 10, Adobe released an update to address this vulnerability.
MCAFEE PRODUCT COVERAGE	
DAT FILES	Under analysis
VIRUS SCAN ENTERPRISE SCAN BOP	Generic buffer overflow protection is expected to cover code execution exploits.
HOST IPS	Generic buffer overflow protection is expected to cover code execution exploits.
NETWORK SECURITY PLATFORM	Under analysis
VULNERABILITY MANAGER	The FSL/MVM package of September 11 includes a vulnerability check to assess if your systems are at risk.
WEB GATEWAY	Under analysis
REMEDIATION MANAGER	Under analysis
POLICY AUDITOR	Under analysis
NETWORK ACCESS CONTROL	Under analysis
FIREWALL ENTERPRISE	Under analysis
APPLICATION CONTROL	Run-Time Control locks down systems and provides protection in the form of Execution Control and Memory Protection.
DATABASE ACTIVITY MONITORING	Out of scope
VULNERABILITY MANAGER FOR DATABASES	Out of scope
ADDITIONAL INFORMATION	Adobe: Security updates available for Adobe Flash Player

Back to top

(APSB13-21) Adobe Flash Player Remote Code Execution IV

MTIS13-146-D

THREAT IDENTIFIER(S)	CVE-2013-5324
THREAT TYPE	Vulnerability
RISK ASSESSMENT	High
MAIN THREAT VECTORS	E-Mail; Web
USER INTERACTION REQUIRED	Yes
DESCRIPTION	A vulnerability in some versions of Adobe Flash Player could lead to remote code execution. The flaw is due to memory corruption. Successful exploitation by a remote attacker could result in the execution of arbitrary code or a denial of service.
IMPORTANCE	High. On September 10, Adobe released an update to address this vulnerability.
MCAFEE PRODUCT COVERAGE	
DAT FILES	Under analysis
VIRUS SCAN ENTERPRISE SCAN BOP	Generic buffer overflow protection is expected to cover code execution exploits.
HOST IPS	Generic buffer overflow protection is expected to cover code execution exploits.
NETWORK SECURITY PLATFORM	Under analysis
VULNERABILITY MANAGER	The FSL/MVM package of September 11 includes a vulnerability check to assess if your systems are at risk.
WEB GATEWAY	Under analysis
REMEDIATION MANAGER	Under analysis
POLICY AUDITOR	Under analysis
NETWORK ACCESS CONTROL	Under analysis
FIREWALL ENTERPRISE	Under analysis
APPLICATION CONTROL	Run-Time Control locks down systems and provides protection in the form of Execution Control and Memory Protection.
DATABASE ACTIVITY MONITORING	Out of scope
VULNERABILITY MANAGER FOR DATABASES	Out of scope
ADDITIONAL INFORMATION	Adobe: Security updates available for Adobe Flash Player

Back to top

(APSB13-22) Adobe Reader and Acrobat Remote Code Execution I

MTIS13-146-E

THREAT IDENTIFIER(S)	CVE-2013-3351
THREAT TYPE	Vulnerability
RISK ASSESSMENT	High
MAIN THREAT VECTORS	E-Mail; Web
USER INTERACTION REQUIRED	Yes
DESCRIPTION	A vulnerability in some versions of Adobe Reader and Acrobat could lead to remote code execution. The flaw is due to a stack overflow. Successful exploitation by a remote attacker could result in the execution of arbitrary code.
IMPORTANCE	High. On September 10, Adobe released an update to address this vulnerability.
MCAFEE PRODUCT COVERAGE	
DAT FILES	Under analysis
VIRUS SCAN ENTERPRISE SCAN BOP	Generic buffer overflow protection is expected to cover code execution exploits.
HOST IPS	Generic buffer overflow protection is expected to cover code execution exploits.
NETWORK SECURITY PLATFORM	Under analysis
VULNERABILITY MANAGER	The FSL/MVM package of September 11 includes a vulnerability check to assess if your systems are at risk.
WEB GATEWAY	Under analysis
REMEDIATION MANAGER	Under analysis
POLICY AUDITOR	Under analysis
NETWORK ACCESS CONTROL	Under analysis
FIREWALL ENTERPRISE	Under analysis
APPLICATION CONTROL	Run-Time Control locks down systems and provides protection in the form of Execution Control and Memory Protection.
DATABASE ACTIVITY MONITORING	Out of scope

VULNERABILITY MANAGER FOR DATABASES	Out of scope
ADDITIONAL INFORMATION	Adobe: Security updates available for Adobe Reader and Acrobat

Back to top

(APSB13-22) Adobe Reader and Acrobat Remote Code Execution II

MTIS13-146-F

THREAT IDENTIFIER(S)	CVE-2013-3352
THREAT TYPE	Vulnerability
RISK ASSESSMENT	High
MAIN THREAT VECTORS	E-Mail; Web
USER INTERACTION REQUIRED	Yes
DESCRIPTION	A vulnerability in some versions of Adobe Reader and Acrobat could lead to remote code execution. The flaw is due to memory corruption. Successful exploitation by a remote attacker could result in the execution of arbitrary code.
IMPORTANCE	High. On September 10, Adobe released an update to address this vulnerability.
MCAFEE PRODUCT COVERAGE	
DAT FILES	Under analysis
VIRUS SCAN ENTERPRISE SCAN BOP	Generic buffer overflow protection is expected to cover code execution exploits.
HOST IPS	Generic buffer overflow protection is expected to cover code execution exploits.
NETWORK SECURITY PLATFORM	Under analysis
VULNERABILITY MANAGER	The FSL/MVM package of September 11 includes a vulnerability check to assess if your systems are at risk.
WEB GATEWAY	Under analysis
REMEDIATION MANAGER	Under analysis
POLICY AUDITOR	Under analysis
NETWORK ACCESS CONTROL	Under analysis
FIREWALL ENTERPRISE	Under analysis
APPLICATION CONTROL	Run-Time Control locks down systems and provides protection in the form of Execution Control and Memory Protection.
DATABASE ACTIVITY MONITORING	Out of scope
VULNERABILITY MANAGER FOR DATABASES	Out of scope
ADDITIONAL INFORMATION	Adobe: Security updates available for Adobe Reader and Acrobat

Back to top

(APSB13-22) Adobe Reader and Acrobat Remote Code Execution III

MTIS13-146-G

THREAT IDENTIFIER(S)	CVE-2013-3353
THREAT TYPE	Vulnerability
RISK ASSESSMENT	High
MAIN THREAT VECTORS	E-Mail; Web
USER INTERACTION REQUIRED	Yes
DESCRIPTION	A vulnerability in some versions of Adobe Reader and Acrobat could lead to remote code execution. The flaw is due to a buffer overflow. Successful exploitation by a remote attacker could result in the execution of arbitrary code.
IMPORTANCE	High. On September 10, Adobe released an update to address this vulnerability.
MCAFEE PRODUCT COVERAGE	
DAT FILES	Under analysis
VIRUS SCAN ENTERPRISE SCAN BOP	Generic buffer overflow protection is expected to cover code execution exploits.
HOST IPS	Generic buffer overflow protection is expected to cover code execution exploits.
NETWORK SECURITY PLATFORM	Under analysis
VULNERABILITY MANAGER	The FSL/MVM package of September 11 includes a vulnerability check to assess if your systems are at risk.
WEB GATEWAY	Under analysis
REMEDIATION MANAGER	Under analysis

POLICY AUDITOR	Under analysis
NETWORK ACCESS CONTROL	Under analysis
FIREWALL ENTERPRISE	Under analysis
APPLICATION CONTROL	Run-Time Control locks down systems and provides protection in the form of Execution Control and Memory Protection.
DATABASE ACTIVITY MONITORING	Out of scope
VULNERABILITY MANAGER FOR DATABASES	Out of scope
ADDITIONAL INFORMATION	Adobe: Security updates available for Adobe Reader and Acrobat

Back to top

(APSB13-22) Adobe Reader and Acrobat Remote Code Execution IV

MTIS13-146-H

THREAT IDENTIFIER(S)	CVE-2013-3354
THREAT TYPE	Vulnerability
RISK ASSESSMENT	High
MAIN THREAT VECTORS	E-Mail; Web
USER INTERACTION REQUIRED	Yes
DESCRIPTION	A vulnerability in some versions of Adobe Reader and Acrobat could lead to remote code execution. The flaw is due to memory corruption. Successful exploitation by a remote attacker could result in the execution of arbitrary code.
IMPORTANCE	High. On September 10, Adobe released an update to address this vulnerability.
MCAFEE PRODUCT COVERAGE	
DAT FILES	Under analysis
VIRUS SCAN ENTERPRISE SCAN BOP	Generic buffer overflow protection is expected to cover code execution exploits.
HOST IPS	Generic buffer overflow protection is expected to cover code execution exploits.
NETWORK SECURITY PLATFORM	Under analysis
VULNERABILITY MANAGER	The FSL/MVM package of September 11 includes a vulnerability check to assess if your systems are at risk.
WEB GATEWAY	Under analysis
REMEDIATION MANAGER	Under analysis
POLICY AUDITOR	Under analysis
NETWORK ACCESS CONTROL	Under analysis
FIREWALL ENTERPRISE	Under analysis
APPLICATION CONTROL	Run-Time Control locks down systems and provides protection in the form of Execution Control and Memory Protection.
DATABASE ACTIVITY MONITORING	Out of scope
VULNERABILITY MANAGER FOR DATABASES	Out of scope
ADDITIONAL INFORMATION	Adobe: Security updates available for Adobe Reader and Acrobat

Back to top

(APSB13-22) Adobe Reader and Acrobat Remote Code Execution V

MTIS13-146-I

THREAT IDENTIFIER(S)	CVE-2013-3355
THREAT TYPE	Vulnerability
RISK ASSESSMENT	High
MAIN THREAT VECTORS	E-Mail; Web
USER INTERACTION REQUIRED	Yes
DESCRIPTION	A vulnerability in some versions of Adobe Reader and Acrobat could lead to remote code execution. The flaw is due to memory corruption. Successful exploitation by a remote attacker could result in the execution of arbitrary code.
IMPORTANCE	High. On September 10, Adobe released an update to address this vulnerability.
MCAFEE PRODUCT COVERAGE	
DAT FILES	Under analysis
VIRUS SCAN ENTERPRISE SCAN BOP	Generic buffer overflow protection is expected to cover code execution exploits.

HOST IPS	Generic buffer overflow protection is expected to cover code execution exploits.
NETWORK SECURITY PLATFORM	Under analysis
VULNERABILITY MANAGER	The FSL/MVM package of September 11 includes a vulnerability check to assess if your systems are at risk.
WEB GATEWAY	Under analysis
REMEDIATION MANAGER	Under analysis
POLICY AUDITOR	Under analysis
NETWORK ACCESS CONTROL	Under analysis
FIREWALL ENTERPRISE	Under analysis
APPLICATION CONTROL	Run-Time Control locks down systems and provides protection in the form of Execution Control and Memory Protection.
DATABASE ACTIVITY MONITORING	Out of scope
VULNERABILITY MANAGER FOR DATABASES	Out of scope
ADDITIONAL INFORMATION	Adobe: Security updates available for Adobe Reader and Acrobat

Back to top

(APSB13-22) Adobe Reader and Acrobat Remote Code Execution VI

MTIS13-146-J

THREAT IDENTIFIER(S)	CVE-2013-3356
THREAT TYPE	Vulnerability
RISK ASSESSMENT	High
MAIN THREAT VECTORS	E-Mail; Web
USER INTERACTION REQUIRED	Yes
DESCRIPTION	A vulnerability in some versions of Adobe Reader and Acrobat could lead to remote code execution. The flaw is due to a buffer overflow. Successful exploitation by a remote attacker could result in the execution of arbitrary code.
IMPORTANCE	High. On September 10, Adobe released an update to address this vulnerability.
MCAFEE PRODUCT COVERAGE	
DAT FILES	Under analysis
VIRUS SCAN ENTERPRISE SCAN BOP	Generic buffer overflow protection is expected to cover code execution exploits.
HOST IPS	Generic buffer overflow protection is expected to cover code execution exploits.
NETWORK SECURITY PLATFORM	Under analysis
VULNERABILITY MANAGER	The FSL/MVM package of September 11 includes a vulnerability check to assess if your systems are at risk.
WEB GATEWAY	Under analysis
REMEDIATION MANAGER	Under analysis
POLICY AUDITOR	Under analysis
NETWORK ACCESS CONTROL	Under analysis
FIREWALL ENTERPRISE	Under analysis
APPLICATION CONTROL	Run-Time Control locks down systems and provides protection in the form of Execution Control and Memory Protection.
DATABASE ACTIVITY MONITORING	Out of scope
VULNERABILITY MANAGER FOR DATABASES	Out of scope
ADDITIONAL INFORMATION	Adobe: Security updates available for Adobe Reader and Acrobat

Back to top

(APSB13-22) Adobe Reader and Acrobat Remote Code Execution VII

MTIS13-146-K

THREAT IDENTIFIER(S)	CVE-2013-3357
THREAT TYPE	Vulnerability
RISK ASSESSMENT	High
MAIN THREAT VECTORS	E-Mail; Web
USER INTERACTION REQUIRED	Yes
	A vulnerability in some versions of Adobe Reader and Acrobat could lead to remote

DESCRIPTION	code execution. The flaw is due to an integer overflow. Successful exploitation by a remote attacker could result in the execution of arbitrary code.
IMPORTANCE	High. On September 10, Adobe released an update to address this vulnerability.
MCAFEE PRODUCT COVERAGE	
DAT FILES	Under analysis
VIRUS SCAN ENTERPRISE SCAN BOP	Generic buffer overflow protection is expected to cover code execution exploits.
HOST IPS	Generic buffer overflow protection is expected to cover code execution exploits.
NETWORK SECURITY PLATFORM	Under analysis
VULNERABILITY MANAGER	The FSL/MVM package of September 11 includes a vulnerability check to assess if your systems are at risk.
WEB GATEWAY	Under analysis
REMEDIATION MANAGER	Under analysis
POLICY AUDITOR	Under analysis
NETWORK ACCESS CONTROL	Under analysis
FIREWALL ENTERPRISE	Under analysis
APPLICATION CONTROL	Run-Time Control locks down systems and provides protection in the form of Execution Control and Memory Protection.
DATABASE ACTIVITY MONITORING	Out of scope
VULNERABILITY MANAGER FOR DATABASES	Out of scope
ADDITIONAL INFORMATION	Adobe: Security updates available for Adobe Reader and Acrobat

Back to top

(APSB13-22) Adobe Reader and Acrobat Remote Code Execution VIII

MTIS13-146-L

THREAT IDENTIFIER(S)	CVE-2013-3358
THREAT TYPE	Vulnerability
RISK ASSESSMENT	High
MAIN THREAT VECTORS	E-Mail; Web
USER INTERACTION REQUIRED	Yes
DESCRIPTION	A vulnerability in some versions of Adobe Reader and Acrobat could lead to remote code execution. The flaw is due to an integer overflow. Successful exploitation by a remote attacker could result in the execution of arbitrary code.
IMPORTANCE	High. On September 10, Adobe released an update to address this vulnerability.
MCAFEE PRODUCT COVERAGE	
DAT FILES	Under analysis
VIRUS SCAN ENTERPRISE SCAN BOP	Generic buffer overflow protection is expected to cover code execution exploits.
HOST IPS	Generic buffer overflow protection is expected to cover code execution exploits.
NETWORK SECURITY PLATFORM	Under analysis
VULNERABILITY MANAGER	The FSL/MVM package of September 11 includes a vulnerability check to assess if your systems are at risk.
WEB GATEWAY	Under analysis
REMEDIATION MANAGER	Under analysis
POLICY AUDITOR	Under analysis
NETWORK ACCESS CONTROL	Under analysis
FIREWALL ENTERPRISE	Under analysis
APPLICATION CONTROL	Run-Time Control locks down systems and provides protection in the form of Execution Control and Memory Protection.
DATABASE ACTIVITY MONITORING	Out of scope
VULNERABILITY MANAGER FOR DATABASES	Out of scope
ADDITIONAL INFORMATION	Adobe: Security updates available for Adobe Reader and Acrobat

Back to top

(APSB13-23) Adobe Shockwave Player Remote Code Execution I

MTIS13-146-M

THREAT IDENTIFIER(S)	CVE-2013-3359
THREAT TYPE	Vulnerability
RISK ASSESSMENT	High
MAIN THREAT VECTORS	E-Mail; Web
USER INTERACTION REQUIRED	Yes
DESCRIPTION	A vulnerability in some versions of Adobe Shockwave Player could lead to remote code execution. The flaw is due to memory corruption. Successful exploitation by a remote attacker could result in the execution of arbitrary code.
IMPORTANCE	High. On September 10, Adobe released an update to address this vulnerability.
MCAFEE PRODUCT COVERAGE	
DAT FILES	Under analysis
VIRUS SCAN ENTERPRISE SCAN BOP	Generic buffer overflow protection is expected to cover code execution exploits.
HOST IPS	Generic buffer overflow protection is expected to cover code execution exploits.
NETWORK SECURITY PLATFORM	Under analysis
VULNERABILITY MANAGER	The FSL/MVM package of September 11 includes a vulnerability check to assess if your systems are at risk.
WEB GATEWAY	Under analysis
REMEDIATION MANAGER	Under analysis
POLICY AUDITOR	Under analysis
NETWORK ACCESS CONTROL	Under analysis
FIREWALL ENTERPRISE	Under analysis
APPLICATION CONTROL	Run-Time Control locks down systems and provides protection in the form of Execution Control and Memory Protection.
DATABASE ACTIVITY MONITORING	Out of scope
VULNERABILITY MANAGER FOR DATABASES	Out of scope
ADDITIONAL INFORMATION	Adobe: Security update available for Adobe Shockwave Player

Back to top

(APSB13-23) Adobe Shockwave Player Remote Code Execution II

MTIS13-146-N

THREAT IDENTIFIER(S)	CVE-2013-3360
THREAT TYPE	Vulnerability
RISK ASSESSMENT	High
MAIN THREAT VECTORS	E-Mail; Web
USER INTERACTION REQUIRED	Yes
DESCRIPTION	A vulnerability in some versions of Adobe Shockwave Player could lead to remote code execution. The flaw is due to memory corruption. Successful exploitation by a remote attacker could result in the execution of arbitrary code.
IMPORTANCE	High. On September 10, Adobe released an update to address this vulnerability.
MCAFEE PRODUCT COVERAGE	
DAT FILES	Under analysis
VIRUS SCAN ENTERPRISE SCAN BOP	Generic buffer overflow protection is expected to cover code execution exploits.
HOST IPS	Generic buffer overflow protection is expected to cover code execution exploits.
NETWORK SECURITY PLATFORM	Under analysis
VULNERABILITY MANAGER	The FSL/MVM package of September 11 includes a vulnerability check to assess if your systems are at risk.
WEB GATEWAY	Under analysis
REMEDIATION MANAGER	Under analysis
POLICY AUDITOR	Under analysis
NETWORK ACCESS CONTROL	Under analysis
FIREWALL ENTERPRISE	Under analysis
APPLICATION CONTROL	Run-Time Control locks down systems and provides protection in the form of Execution Control and Memory Protection.
DATABASE ACTIVITY MONITORING	Out of scope
VULNERABILITY MANAGER FOR DATABASES	Out of scope

ADDITIONAL INFORMATION	Adobe: Security update available for Adobe Shockwave Player

Back to top

Detailed descriptions of the Security Advisories can be found in the Users Guide:
https://kc.mcafee.com/content/mtis/McAfee_Avert_Labs_Security_Advisory_UsersGuide.pdf

For more information on McAfee Labs Security Advisories, see:
https://kc.mcafee.com/content/mtis/McAfee_Avert_Labs_Security_Advisory_FAQ.pdf

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.

*The information provided is only for the use and convenience of McAfee's customers in connection with their McAfee products, and applies only to the threats described herein. McAfee product coverage statements are limited to known attack vectors and should not be considered comprehensive. THE INFORMATION PROVIDED HEREIN IS PROVIDED "AS IS" AND IS SUBJECT TO CHANGE WITHOUT NOTICE.

McAfee, Inc. 3965 Freedom Circle, Santa Clara, CA 95054 888.847.8766 www.mcafee.com