EXECUTIVE SUMMARY

March 5, 2014 | MTIS14-037

Since the last McAfee® Labs Security Advisory (March 3), the following noteworthy event has taken place:

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

NEW THREAT OVERVIEW

Schneider Electric Multiple SCADA Products Exception Handler Denial of Service

MTIS14-037-A

IMPORTANCE:	High
COVERED PRODUCTS:	
UNDER ANALYSIS:	DAT | Web Gateway | Policy Auditor SCAP | MNAC 2.x | Firewall Enterprise | Application Control

Back to top

PREVIOUS THREAT UPDATES

Apple Safari WebKit Crafted Website Remote Code Execution I

MTIS14-035-G

IMPORTANCE:	High
NOW COVERED:	BOP | Host IPS

Back to top

Apple Safari WebKit Crafted Website Remote Code Execution II

MTIS14-035-H

IMPORTANCE:	High
NOW COVERED:	BOP | Host IPS

Back to top

Apple Safari WebKit Crafted Website Remote Code Execution III

MTIS14-035-I

IMPORTANCE:	High
NOW COVERED:	BOP | Host IPS

Back to top

Apple Safari WebKit Crafted Website Remote Code Execution IV

MTIS14-035-J

IMPORTANCE:	High
NOW COVERED:	BOP | Host IPS

Back to top

THREAT DETAILS

Schneider Electric Multiple SCADA Products Exception Handler Denial of Service

MTIS14-037-A

THREAT IDENTIFIER(S)	CVE-2013-2824
THREAT TYPE	Vulnerability
RISK ASSESSMENT	High
MAIN THREAT VECTORS	LAN; WAN
USER INTERACTION REQUIRED	No
DESCRIPTION	A vulnerability in some versions of multiple Schneider Electric SCADA products could lead to a denial of service. The flaw lies in the handling of a specially crafted packet sent to any of the server processes. Successful exploitation by a remote attacker could result in a denial of service condition.
IMPORTANCE	High. On February 20, Schneider Electric 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	A future FSL/MVM package will include a vulnerability check to assess if your systems are at risk.
WEB GATEWAY	Under analysis
REMEDIATION MANAGER	Not applicable
POLICY AUDITOR	Under analysis
NETWORK ACCESS CONTROL	Under analysis
FIREWALL ENTERPRISE	Under analysis
APPLICATION CONTROL	Under analysis
DATABASE ACTIVITY MONITORING	Out of scope
VULNERABILITY MANAGER FOR DATABASES	Out of scope
ADDITIONAL INFORMATION	Schneider Electric: Important security & quality notification – Cumulative update for SCADA Expert Vijeo Citect / CitectSCADA / PowerSCADA Expert ICS-CERT: Schneider Electric SCADA Products Exception Handler Vulnerability

Back to top

Apple Safari WebKit Crafted Website Remote Code Execution I

MTIS14-035-G

THREAT IDENTIFIER(S)	CVE-2013-6635
THREAT TYPE	Vulnerability
RISK ASSESSMENT	High
MAIN THREAT VECTORS	Web
USER INTERACTION REQUIRED	Yes
DESCRIPTION	A vulnerability in some versions of Apple Safari could lead to remote code execution. The flaw lies in the WebKit component. Successful exploitation by a remote attacker could result in the execution of arbitrary code or a denial of service.
IMPORTANCE	High. On February 25, Apple 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	Coverage not warranted
VULNERABILITY MANAGER	A future FSL/MVM package will include a vulnerability check to assess if your systems are at risk.
WEB GATEWAY	Under analysis
REMEDIATION MANAGER	Not applicable

POLICY AUDITOR	Under analysis
NETWORK ACCESS CONTROL	Under analysis
FIREWALL ENTERPRISE	Under analysis
APPLICATION CONTROL	Under analysis
DATABASE ACTIVITY MONITORING	Out of scope
VULNERABILITY MANAGER FOR DATABASES	Out of scope
ADDITIONAL INFORMATION	Apple: About the security content of Safari 6.1.2 and Safari 7.0.2

Back to top

Apple Safari WebKit Crafted Website Remote Code Execution II

MTIS14-035-H

THREAT IDENTIFIER(S)	CVE-2014-1268
THREAT TYPE	Vulnerability
RISK ASSESSMENT	High
MAIN THREAT VECTORS	Web
USER INTERACTION REQUIRED	Yes
DESCRIPTION	A vulnerability in some versions of Apple Safari could lead to remote code execution. The flaw lies in the WebKit component. Successful exploitation by a remote attacker could result in the execution of arbitrary code or a denial of service.
IMPORTANCE	High. On February 25, Apple 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	Coverage not warranted
VULNERABILITY MANAGER	A future FSL/MVM package will include a vulnerability check to assess if your systems are at risk.
WEB GATEWAY	Under analysis
REMEDIATION MANAGER	Not applicable
POLICY AUDITOR	Under analysis
NETWORK ACCESS CONTROL	Under analysis
FIREWALL ENTERPRISE	Under analysis
APPLICATION CONTROL	Under analysis
DATABASE ACTIVITY MONITORING	Out of scope
VULNERABILITY MANAGER FOR DATABASES	Out of scope
ADDITIONAL INFORMATION	Apple: About the security content of Safari 6.1.2 and Safari 7.0.2

Back to top

Apple Safari WebKit Crafted Website Remote Code Execution III

MTIS14-035-I

THREAT IDENTIFIER(S)	CVE-2014-1269
THREAT TYPE	Vulnerability
RISK ASSESSMENT	High
MAIN THREAT VECTORS	Web
USER INTERACTION REQUIRED	Yes
DESCRIPTION	A vulnerability in some versions of Apple Safari could lead to remote code execution. The flaw lies in the WebKit component. Successful exploitation by a remote attacker could result in the execution of arbitrary code or a denial of service.
IMPORTANCE	High. On February 25, Apple 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	Coverage not warranted
VULNERABILITY MANAGER	A future FSL/MVM package will include a vulnerability check to assess if your systems are at risk.
WEB GATEWAY	Under analysis
REMEDIATION MANAGER	Not applicable
POLICY AUDITOR	Under analysis
NETWORK ACCESS CONTROL	Under analysis
FIREWALL ENTERPRISE	Under analysis
APPLICATION CONTROL	Under analysis
DATABASE ACTIVITY MONITORING	Out of scope
VULNERABILITY MANAGER FOR DATABASES	Out of scope
ADDITIONAL INFORMATION	Apple: About the security content of Safari 6.1.2 and Safari 7.0.2

Back to top

Apple Safari WebKit Crafted Website Remote Code Execution IV

MTIS14-035-J

THREAT IDENTIFIER(S)	CVE-2014-1270
THREAT TYPE	Vulnerability
RISK ASSESSMENT	High
MAIN THREAT VECTORS	Web
USER INTERACTION REQUIRED	Yes
DESCRIPTION	A vulnerability in some versions of Apple Safari could lead to remote code execution. The flaw lies in the WebKit component. Successful exploitation by a remote attacker could result in the execution of arbitrary code or a denial of service.
IMPORTANCE	High. On February 25, Apple 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	Coverage not warranted
VULNERABILITY MANAGER	A future FSL/MVM package will include a vulnerability check to assess if your systems are at risk.
WEB GATEWAY	Under analysis
REMEDIATION MANAGER	Not applicable
POLICY AUDITOR	Under analysis
NETWORK ACCESS CONTROL	Under analysis
FIREWALL ENTERPRISE	Under analysis
APPLICATION CONTROL	Under analysis
DATABASE ACTIVITY MONITORING	Out of scope
VULNERABILITY MANAGER FOR DATABASES	Out of scope
ADDITIONAL INFORMATION	Apple: About the security content of Safari 6.1.2 and Safari 7.0.2

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.

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