

EXECUTIVE SUMMARY

July 15, 2020 | MTIS20-037

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

- Patches are available for multiple Microsoft security vulnerabilities

NEW THREAT OVERVIEW

(MSPT-Jul2020) Microsoft Windows Push Notification Service Privilege Escalation (CVE-2020-1387)

MTIS20-037-A

IMPORTANCE: Medium
COVERED PRODUCTS:
UNDER ANALYSIS: Firewall Enterprise

[Back to top](#)

(MSPT-Jul2020) Microsoft Windows psmsrv.dll Privilege Escalation (CVE-2020-1388)

MTIS20-037-B

IMPORTANCE: Medium
COVERED PRODUCTS:
UNDER ANALYSIS: Firewall Enterprise

[Back to top](#)

(MSPT-Jul2020) Microsoft Windows WER Information Disclosure (CVE-2020-1389)

MTIS20-037-C

IMPORTANCE: Medium
COVERED PRODUCTS:
UNDER ANALYSIS: Firewall Enterprise

[Back to top](#)

(MSPT-Jul2020) Microsoft Windows Network Connections Service Privilege Escalation (CVE-2020-1390)

MTIS20-037-D

IMPORTANCE: Medium
COVERED PRODUCTS:
UNDER ANALYSIS: Firewall Enterprise

[Back to top](#)

(MSPT-Jul2020) Microsoft Windows Kernel Information Disclosure (CVE-2020-1391)

MTIS20-037-E

IMPORTANCE: Medium
COVERED PRODUCTS:
UNDER ANALYSIS: Firewall Enterprise

[Back to top](#)

(MSPT-Jul2020) Microsoft Windows Delivery Optimization Service Privilege Escalation (CVE-2020-1392)

MTIS20-037-F

IMPORTANCE: Medium
COVERED PRODUCTS:
UNDER ANALYSIS: Firewall Enterprise

[Back to top](#)

(MSPT-Jul2020) Microsoft Windows Diagnostics Hub Standard Collector Service Privilege Escalation (CVE-2020-1393)

MTIS20-037-G

IMPORTANCE: Medium
COVERED PRODUCTS:
UNDER ANALYSIS: Firewall Enterprise

[Back to top](#)

(MSPT-Jul2020) Microsoft Windows Geolocation Framework Privilege Escalation (CVE-2020-1394)

MTIS20-037-H

IMPORTANCE: Medium
COVERED PRODUCTS:
UNDER ANALYSIS: Firewall Enterprise

[Back to top](#)

(MSPT-Jul2020) Microsoft Windows Speech Brokered Api Privilege Escalation (CVE-2020-1395)

MTIS20-037-I

IMPORTANCE: Medium
COVERED PRODUCTS:
UNDER ANALYSIS: Firewall Enterprise

[Back to top](#)

(MSPT-Jul2020) Microsoft Windows ALPC Privilege Escalation (CVE-2020-1396)

MTIS20-037-J

IMPORTANCE: Medium
COVERED PRODUCTS:
UNDER ANALYSIS: Firewall Enterprise

[Back to top](#)

(MSPT-Jul2020) Microsoft Windows Imaging Information Disclosure (CVE-2020-1397)

MTIS20-037-K

IMPORTANCE: Medium
COVERED PRODUCTS:
UNDER ANALYSIS: Firewall Enterprise

[Back to top](#)

(MSPT-Jul2020) Microsoft Windows Lockscreen Privilege Escalation (CVE-2020-1398)

MTIS20-037-L

IMPORTANCE: Medium
COVERED PRODUCTS:
UNDER ANALYSIS: Firewall Enterprise

[Back to top](#)

(MSPT-Jul2020) Microsoft Windows Runtime Privilege Escalation (CVE-2020-1399)

MTIS20-037-M

IMPORTANCE: Medium
COVERED PRODUCTS:
UNDER ANALYSIS: DAT | Web Gateway | Firewall Enterprise

[Back to top](#)

(MSPT-Jul2020) Microsoft Windows Jet Database Engine Remote Code Execution (CVE-2020-1400)

MTIS20-037-N

IMPORTANCE: Medium
COVERED PRODUCTS:
UNDER ANALYSIS: Firewall Enterprise

[Back to top](#)

(MSPT-Jul2020) Microsoft Windows Jet Database Engine Remote Code Execution (CVE-2020-1401)

MTIS20-037-O

IMPORTANCE: Medium
COVERED PRODUCTS:
UNDER ANALYSIS: Firewall Enterprise

[Back to top](#)

(MSPT-Jul2020) Microsoft Windows ActiveX Installer Service Privilege Escalation (CVE-2020-1402)

MTIS20-037-P

IMPORTANCE: Medium
COVERED PRODUCTS:
UNDER ANALYSIS: Firewall Enterprise

[Back to top](#)

(MSPT-Jul2020) Microsoft VBScript Improperly Handles Objects in Memory Remote Code Execution (CVE-2020-1403)

MTIS20-037-Q

IMPORTANCE: High
COVERED PRODUCTS:
UNDER ANALYSIS: DAT | Web Gateway | Firewall Enterprise

[Back to top](#)

(MSPT-Jul2020) Microsoft Windows Runtime Privilege Escalation (CVE-2020-1404)

MTIS20-037-R

IMPORTANCE: Medium
COVERED PRODUCTS:
UNDER ANALYSIS: Firewall Enterprise

[Back to top](#)

(MSPT-Jul2020) Microsoft Windows MDM Privilege Escalation (CVE-2020-1405)

MTIS20-037-S

IMPORTANCE: Medium
COVERED PRODUCTS:
UNDER ANALYSIS: Firewall Enterprise

[Back to top](#)

(MSPT-Jul2020) Microsoft Windows Network List Service Privilege Escalation (CVE-2020-1406)

MTIS20-037-T

IMPORTANCE: Medium
COVERED PRODUCTS:

UNDER ANALYSIS: Firewall Enterprise

[Back to top](#)

(MSPT-Jul2020) Microsoft Windows Jet Database Engine Remote Code Execution (CVE-2020-1407)

MTIS20-037-U

IMPORTANCE: Medium
COVERED PRODUCTS:
UNDER ANALYSIS: Firewall Enterprise

[Back to top](#)

(MSPT-Jul2020) Microsoft Windows Font Library Remote Code Execution (CVE-2020-1408)

MTIS20-037-V

IMPORTANCE: Medium
COVERED PRODUCTS:
UNDER ANALYSIS: Firewall Enterprise

[Back to top](#)

(MSPT-Jul2020) Microsoft DirectWrite Improperly Handles Objects in Memory Remote Code Execution (CVE-2020-1409)

MTIS20-037-W

IMPORTANCE: High
COVERED PRODUCTS:
UNDER ANALYSIS: Firewall Enterprise

[Back to top](#)

(MSPT-Jul2020) Microsoft Windows Address Book Remote Code Execution (CVE-2020-1410)

MTIS20-037-X

IMPORTANCE: High
COVERED PRODUCTS:
UNDER ANALYSIS: Firewall Enterprise

[Back to top](#)

(MSPT-Jul2020) Microsoft Windows Kernel Privilege Escalation (CVE-2020-1411)

MTIS20-037-Y

IMPORTANCE: Medium
COVERED PRODUCTS:
UNDER ANALYSIS: Firewall Enterprise

[Back to top](#)

(MSPT-Jul2020) Microsoft Graphics Components improperly handle objects in memory Remote Code Execution (CVE-2020-1412)

MTIS20-037-Z

IMPORTANCE: Medium
COVERED PRODUCTS:
UNDER ANALYSIS: Firewall Enterprise

[Back to top](#)

THREAT DETAILS

(MSPT-Jul2020) Microsoft Windows Push Notification Service Privilege Escalation (CVE-2020-1387)

MTIS20-037-A

THREAT IDENTIFIER(S) CVE-2020-1387
THREAT TYPE Vulnerability

RISK ASSESSMENT	Medium
MAIN THREAT VECTORS	Locally logged-on user
USER INTERACTION REQUIRED	No
DESCRIPTION	A vulnerability in some versions of Microsoft Windows could lead to privilege escalation. The flaw lies in the Push Notification Service component. Successful exploitation could allow a local user to gain elevated privileges. The exploit requires the attacker to have valid credentials to the vulnerable system.
IMPORTANCE	Medium. On July 14, Microsoft released an update to address this vulnerability
MCAFEE PRODUCT COVERAGE	
DAT FILES	Out of scope
VIRUS SCAN ENTERPRISE SCAN BOP	Out of scope
HOST IPS	Out of scope
NETWORK SECURITY PLATFORM	No Coverage Status
VULNERABILITY MANAGER	An upcoming FSL/MVM content release will contain coverage for this issue.
WEB GATEWAY	Out of scope
REMEDATION 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	Microsoft: Security Update Summary

[Back to top](#)

(MSPT-Jul2020) Microsoft Windows psmsrv.dll Privilege Escalation (CVE-2020-1388)

MTIS20-037-B

THREAT IDENTIFIER(S)	CVE-2020-1388
THREAT TYPE	Vulnerability
RISK ASSESSMENT	Medium
MAIN THREAT VECTORS	Locally logged-on user
USER INTERACTION REQUIRED	No
DESCRIPTION	A vulnerability in some versions of Microsoft Windows could lead to privilege escalation. The flaw lies in the psmsrv.dll component. Successful exploitation could allow a local user to gain elevated privileges. The exploit requires the attacker to have valid credentials to the vulnerable system.
IMPORTANCE	Medium. On July 14, Microsoft released an update to address this vulnerability
MCAFEE PRODUCT COVERAGE	
DAT FILES	Out of scope
VIRUS SCAN ENTERPRISE SCAN BOP	Out of scope
HOST IPS	Out of scope
NETWORK SECURITY PLATFORM	No Coverage Status
VULNERABILITY MANAGER	An upcoming FSL/MVM content release will contain coverage for this issue.
WEB GATEWAY	Out of scope
REMEDATION 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	Microsoft: Security Update Summary

[Back to top](#)

(MSPT-Jul2020) Microsoft Windows WER Information Disclosure (CVE-2020-1389)

MTIS20-037-C

THREAT IDENTIFIER(S)	CVE-2020-1389
THREAT TYPE	Vulnerability
RISK ASSESSMENT	Medium
MAIN THREAT VECTORS	Locally logged-on user
USER INTERACTION REQUIRED	No
DESCRIPTION	A vulnerability in some versions of Microsoft Windows could lead to information disclosure. The flaw lies in the WER component. Successful exploitation by a remote attacker could result in the disclosure of sensitive information. The exploit requires the attacker to have valid credentials to the vulnerable system.
IMPORTANCE	Medium. On July 14, Microsoft released an update to address this vulnerability
MCAFFEE PRODUCT COVERAGE	
DAT FILES	Out of scope
VIRUS SCAN ENTERPRISE SCAN BOP	Out of scope
HOST IPS	Out of scope
NETWORK SECURITY PLATFORM	No Coverage Status
VULNERABILITY MANAGER	An upcoming FSL/MVM content release will contain coverage for this issue.
WEB GATEWAY	Out of scope
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	Microsoft: Security Update Summary

[Back to top](#)

(MSPT-Jul2020) Microsoft Windows Network Connections Service Privilege Escalation (CVE-2020-1390)

MTIS20-037-D

THREAT IDENTIFIER(S)	CVE-2020-1390
THREAT TYPE	Vulnerability
RISK ASSESSMENT	Medium
MAIN THREAT VECTORS	Locally logged-on user
USER INTERACTION REQUIRED	No
DESCRIPTION	A vulnerability in some versions of Microsoft Windows could lead to privilege escalation. The flaw lies in the Network Connections Service component. Successful exploitation could allow a local user to gain elevated privileges. The exploit requires the attacker to have valid credentials to the vulnerable system.
IMPORTANCE	Medium. On July 14, Microsoft released an update to address this vulnerability
MCAFFEE PRODUCT COVERAGE	
DAT FILES	Out of scope
VIRUS SCAN ENTERPRISE SCAN BOP	Out of scope
HOST IPS	Out of scope
NETWORK SECURITY PLATFORM	No Coverage Status
VULNERABILITY MANAGER	An upcoming FSL/MVM content release will contain coverage for this issue.
WEB GATEWAY	Out of scope
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	Microsoft: Security Update Summary

[Back to top](#)

(MSPT-Jul2020) Microsoft Windows Kernel Information Disclosure (CVE-2020-1391)

MTIS20-037-E

THREAT IDENTIFIER(S)	CVE-2020-1391
THREAT TYPE	Vulnerability
RISK ASSESSMENT	Medium
MAIN THREAT VECTORS	Locally logged-on user
USER INTERACTION REQUIRED	No
DESCRIPTION	A vulnerability in some versions of Microsoft Windows could lead to information disclosure. The flaw lies in the Kernel component. Successful exploitation by a remote attacker could result in the disclosure of sensitive information. The exploit requires the attacker to have valid credentials to the vulnerable system.
IMPORTANCE	Medium. On July 14, Microsoft released an update to address this vulnerability
MCAFEE PRODUCT COVERAGE	
DAT FILES	Out of scope
VIRUS SCAN ENTERPRISE SCAN BOP	Out of scope
HOST IPS	Out of scope
NETWORK SECURITY PLATFORM	No Coverage Status
VULNERABILITY MANAGER	An upcoming FSL/MVM content release will contain coverage for this issue.
WEB GATEWAY	Out of scope
REMEDATION 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	Microsoft: Security Update Summary

[Back to top](#)

(MSPT-Jul2020) Microsoft Windows Delivery Optimization Service Privilege Escalation (CVE-2020-1392)

MTIS20-037-F

THREAT IDENTIFIER(S)	CVE-2020-1392
THREAT TYPE	Vulnerability
RISK ASSESSMENT	Medium
MAIN THREAT VECTORS	Locally logged-on user
USER INTERACTION REQUIRED	No
DESCRIPTION	A vulnerability in some versions of Microsoft Windows could lead to privilege escalation. The flaw lies in the Delivery Optimization component. Successful exploitation could allow a local user to gain elevated privileges. The exploit requires the attacker to have valid credentials to the vulnerable system.
IMPORTANCE	Medium. On July 14, Microsoft released an update to address this vulnerability
MCAFEE PRODUCT COVERAGE	
DAT FILES	Out of scope
VIRUS SCAN ENTERPRISE SCAN BOP	Out of scope

HOST IPS	Out of scope
NETWORK SECURITY PLATFORM	No Coverage Status
VULNERABILITY MANAGER	An upcoming FSL/MVM content release will contain coverage for this issue.
WEB GATEWAY	Out of scope
REMEDATION 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	Microsoft: Security Update Summary

[Back to top](#)

(MSPT-Jul2020) Microsoft Windows Diagnostics Hub Standard Collector Service Privilege Escalation (CVE-2020-1393)

MTIS20-037-G

THREAT IDENTIFIER(S)	CVE-2020-1393
THREAT TYPE	Vulnerability
RISK ASSESSMENT	Medium
MAIN THREAT VECTORS	Locally logged-on user
USER INTERACTION REQUIRED	No
DESCRIPTION	A vulnerability in some versions of Microsoft Windows could lead to privilege escalation. The flaw lies in the Diagnostics Hub Standard Collector Service component. Successful exploitation could allow a local user to gain elevated privileges. The exploit requires the attacker to have valid credentials to the vulnerable system.
IMPORTANCE	Medium. On July 14, Microsoft released an update to address this vulnerability
MCAFFEE PRODUCT COVERAGE	
DAT FILES	Out of scope
VIRUS SCAN ENTERPRISE SCAN BOP	Out of scope
HOST IPS	Out of scope
NETWORK SECURITY PLATFORM	No Coverage Status
VULNERABILITY MANAGER	An upcoming FSL/MVM content release will contain coverage for this issue.
WEB GATEWAY	Out of scope
REMEDATION 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	Microsoft: Security Update Summary

[Back to top](#)

(MSPT-Jul2020) Microsoft Windows Geolocation Framework Privilege Escalation (CVE-2020-1394)

MTIS20-037-H

THREAT IDENTIFIER(S)	CVE-2020-1394
THREAT TYPE	Vulnerability
RISK ASSESSMENT	Medium
MAIN THREAT VECTORS	Locally logged-on user
USER INTERACTION REQUIRED	No

DESCRIPTION	A vulnerability in some versions of Microsoft Windows could lead to privilege escalation. The flaw lies in the Geolocation Framework component. Successful exploitation could allow a local user to gain elevated privileges. The exploit requires the attacker to have valid credentials to the vulnerable system.
IMPORTANCE	Medium. On July 14, Microsoft released an update to address this vulnerability
MCAFFEE PRODUCT COVERAGE	
DAT FILES	Out of scope
VIRUS SCAN ENTERPRISE SCAN BOP	Out of scope
HOST IPS	Out of scope
NETWORK SECURITY PLATFORM	No Coverage Status
VULNERABILITY MANAGER	An upcoming FSL/MVM content release will contain coverage for this issue.
WEB GATEWAY	Out of scope
REMEDATION 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	Microsoft: Security Update Summary

[Back to top](#)

(MSPT-Jul2020) Microsoft Windows Speech Brokered Api Privilege Escalation (CVE-2020-1395)

MTIS20-037-1

THREAT IDENTIFIER(S)	CVE-2020-1395
THREAT TYPE	Vulnerability
RISK ASSESSMENT	Medium
MAIN THREAT VECTORS	Locally logged-on user
USER INTERACTION REQUIRED	No
DESCRIPTION	A vulnerability in some versions of Microsoft Windows could lead to privilege escalation. The flaw lies in the Speech Brokered Api component. Successful exploitation could allow a local user to gain elevated privileges. The exploit requires the attacker to have valid credentials to the vulnerable system.
IMPORTANCE	Medium. On July 14, Microsoft released an update to address this vulnerability
MCAFFEE PRODUCT COVERAGE	
DAT FILES	Out of scope
VIRUS SCAN ENTERPRISE SCAN BOP	Out of scope
HOST IPS	Out of scope
NETWORK SECURITY PLATFORM	No Coverage Status
VULNERABILITY MANAGER	An upcoming FSL/MVM content release will contain coverage for this issue.
WEB GATEWAY	Out of scope
REMEDATION 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	Microsoft: Security Update Summary

[Back to top](#)

(MSPT-Jul2020) Microsoft Windows ALPC Privilege Escalation (CVE-2020-1396)

MTIS20-037-J

THREAT IDENTIFIER(S)	CVE-2020-1396
THREAT TYPE	Vulnerability
RISK ASSESSMENT	Medium
MAIN THREAT VECTORS	Locally logged-on user
USER INTERACTION REQUIRED	No
DESCRIPTION	A vulnerability in some versions of Microsoft Windows could lead to privilege escalation. The flaw lies in the ALPC component. Successful exploitation could allow a local user to gain elevated privileges. The exploit requires the attacker to have valid credentials to the vulnerable system.
IMPORTANCE	Medium. On July 14, Microsoft released an update to address this vulnerability
MCAFFEE PRODUCT COVERAGE	
DAT FILES	Out of scope
VIRUS SCAN ENTERPRISE SCAN BOP	Out of scope
HOST IPS	Out of scope
NETWORK SECURITY PLATFORM	No Coverage Status
VULNERABILITY MANAGER	An upcoming FSL/MVM content release will contain coverage for this issue.
WEB GATEWAY	Out of scope
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	Microsoft: Security Update Summary

[Back to top](#)

(MSPT-Jul2020) Microsoft Windows Imaging Information Disclosure (CVE-2020-1397)

MTIS20-037-K

THREAT IDENTIFIER(S)	CVE-2020-1397
THREAT TYPE	Vulnerability
RISK ASSESSMENT	Medium
MAIN THREAT VECTORS	Locally logged-on user
USER INTERACTION REQUIRED	Yes
DESCRIPTION	A vulnerability in some versions of Microsoft Windows could lead to information disclosure. The flaw lies in the Imaging 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	Medium. On July 14, Microsoft released an update to address this vulnerability
MCAFFEE PRODUCT COVERAGE	
DAT FILES	Coverage not warranted at this time
VIRUS SCAN ENTERPRISE SCAN BOP	Out of scope
HOST IPS	Out of scope
NETWORK SECURITY PLATFORM	No Coverage Status
VULNERABILITY MANAGER	An upcoming FSL/MVM content release will contain coverage for this issue.
WEB GATEWAY	Coverage not warrantedat this time
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	Microsoft: Security Update Summary

[Back to top](#)

(MSPT-Jul2020) Microsoft Windows Lockscreen Privilege Escalation (CVE-2020-1398)

MTIS20-037-L

THREAT IDENTIFIER(S)	CVE-2020-1398
THREAT TYPE	Vulnerability
RISK ASSESSMENT	Medium
MAIN THREAT VECTORS	Web
USER INTERACTION REQUIRED	No
DESCRIPTION	A vulnerability in some versions of Microsoft Windows could lead to privilege escalation. The flaw lies in the Lockscreen component. Successful exploitation could allow a local user to gain elevated privileges. The exploit requires the attacker to have valid credentials to the vulnerable system.
IMPORTANCE	Medium. On July 14, Microsoft released an update to address this vulnerability
MCAFFEE PRODUCT COVERAGE	
DAT FILES	Out of scope
VIRUS SCAN ENTERPRISE SCAN BOP	Out of scope
HOST IPS	Out of scope
NETWORK SECURITY PLATFORM	No Coverage Status
VULNERABILITY MANAGER	An upcoming FSL/MVM content release will contain coverage for this issue.
WEB GATEWAY	Out of scope
REMEDATION 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	Microsoft: Security Update Summary

[Back to top](#)

(MSPT-Jul2020) Microsoft Windows Runtime Privilege Escalation (CVE-2020-1399)

MTIS20-037-M

THREAT IDENTIFIER(S)	CVE-2020-1399
THREAT TYPE	Vulnerability
RISK ASSESSMENT	Medium
MAIN THREAT VECTORS	Locally logged-on user
USER INTERACTION REQUIRED	No
DESCRIPTION	A vulnerability in some versions of Microsoft Windows could lead to privilege escalation. The flaw lies in the Runtime component. Successful exploitation could allow a local user to gain elevated privileges. The exploit requires the attacker to have valid credentials to the vulnerable system.
IMPORTANCE	Medium. On July 14, Microsoft released an update to address this vulnerability
MCAFFEE PRODUCT COVERAGE	
DAT FILES	Under analysis
VIRUS SCAN ENTERPRISE SCAN BOP	Out of scope
HOST IPS	Out of scope
NETWORK SECURITY PLATFORM	No Coverage Status
VULNERABILITY MANAGER	An upcoming FSL/MVM content release will contain coverage for this issue.

WEB GATEWAY	Under analysis
REMIEDIATION 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	Microsoft: Security Update Summary

[Back to top](#)

(MSPT-Jul2020) Microsoft Windows Jet Database Engine Remote Code Execution (CVE-2020-1400)

MTIS20-037-N

THREAT IDENTIFIER(S)	CVE-2020-1400
THREAT TYPE	Vulnerability
RISK ASSESSMENT	Medium
MAIN THREAT VECTORS	Locally logged-on user
USER INTERACTION REQUIRED	Yes
DESCRIPTION	A vulnerability in some versions of Microsoft Windows could lead to remote code execution. The flaw lies in the Jet Database Engine 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	Medium. On July 14, Microsoft released an update to address this vulnerability
MCAFFEE PRODUCT COVERAGE	
DAT FILES	Coverage not warranted at this time
VIRUS SCAN ENTERPRISE SCAN BOP	Out of scope
HOST IPS	Out of scope
NETWORK SECURITY PLATFORM	No Coverage Status
VULNERABILITY MANAGER	An upcoming FSL/MVM content release will contain coverage for this issue.
WEB GATEWAY	Coverage not warrantedat this time
REMIEDIATION 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	Microsoft: Security Update Summary

[Back to top](#)

(MSPT-Jul2020) Microsoft Windows Jet Database Engine Remote Code Execution (CVE-2020-1401)

MTIS20-037-O

THREAT IDENTIFIER(S)	CVE-2020-1401
THREAT TYPE	Vulnerability
RISK ASSESSMENT	Medium
MAIN THREAT VECTORS	Web
USER INTERACTION REQUIRED	Yes
DESCRIPTION	A vulnerability in some versions of Microsoft Windows could lead to remote code execution. The flaw lies in the Jet Database Engine 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	Medium. On July 14, Microsoft released an update to address this vulnerability

MCAFFEE PRODUCT COVERAGE	
DAT FILES	Coverage not warranted at this time
VIRUS SCAN ENTERPRISE SCAN BOP	Out of scope
HOST IPS	Out of scope
NETWORK SECURITY PLATFORM	No Coverage Status
VULNERABILITY MANAGER	An upcoming FSL/MVM content release will contain coverage for this issue.
WEB GATEWAY	Coverage not warrantedat this time
REMIEDIATION 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	Microsoft: Security Update Summary

[Back to top](#)

(MSPT-Jul2020) Microsoft Windows ActiveX Installer Service Privilege Escalation (CVE-2020-1402)

MTIS20-037-P

THREAT IDENTIFIER(S)	CVE-2020-1402
THREAT TYPE	Vulnerability
RISK ASSESSMENT	Medium
MAIN THREAT VECTORS	Web
USER INTERACTION REQUIRED	No
DESCRIPTION	A vulnerability in some versions of Microsoft Windows could lead to privilege escalation. The flaw lies in the ActiveX Installer Service component. Successful exploitation could allow a local user to gain elevated privileges. The exploit requires the attacker to have valid credentials to the vulnerable system.
IMPORTANCE	Medium. On July 14, Microsoft released an update to address this vulnerability

MCAFFEE PRODUCT COVERAGE	
DAT FILES	Out of scope
VIRUS SCAN ENTERPRISE SCAN BOP	Out of scope
HOST IPS	Out of scope
NETWORK SECURITY PLATFORM	No Coverage Status
VULNERABILITY MANAGER	An upcoming FSL/MVM content release will contain coverage for this issue.
WEB GATEWAY	Out of scope
REMIEDIATION 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	Microsoft: Security Update Summary

[Back to top](#)

(MSPT-Jul2020) Microsoft VBScript Improperly Handles Objects in Memory Remote Code Execution (CVE-2020-1403)

MTIS20-037-Q

THREAT IDENTIFIER(S)	CVE-2020-1403
THREAT TYPE	Vulnerability

RISK ASSESSMENT	High
MAIN THREAT VECTORS	Locally logged-on user
USER INTERACTION REQUIRED	No
DESCRIPTION	A vulnerability in some versions of Microsoft VBScript could lead to remote code execution. The flaw lies in improperly handle objects in memory. Successful exploitation by a remote attacker could result in the execution of arbitrary code. The exploit requires the attacker to have valid credentials to the vulnerable system.
IMPORTANCE	High. On July 14, Microsoft released an update to address this vulnerability
MCAFFEE PRODUCT COVERAGE	
DAT FILES	Under analysis
VIRUS SCAN ENTERPRISE SCAN BOP	Out of scope
HOST IPS	Out of scope
NETWORK SECURITY PLATFORM	No Coverage Status
VULNERABILITY MANAGER	An upcoming FSL/MVM content release will contain coverage for this issue.
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	Microsoft: Security Update Summary

[Back to top](#)

(MSPT-Jul2020) Microsoft Windows Runtime Privilege Escalation (CVE-2020-1404)

MTIS20-037-R

THREAT IDENTIFIER(S)	CVE-2020-1404
THREAT TYPE	Vulnerability
RISK ASSESSMENT	Medium
MAIN THREAT VECTORS	Locally logged-on user
USER INTERACTION REQUIRED	No
DESCRIPTION	A vulnerability in some versions of Microsoft Windows could lead to privilege escalation. The flaw lies in the Runtime component. Successful exploitation could allow a local user to gain elevated privileges. The exploit requires the attacker to have valid credentials to the vulnerable system.
IMPORTANCE	Medium. On July 14, Microsoft released an update to address this vulnerability
MCAFFEE PRODUCT COVERAGE	
DAT FILES	Out of scope
VIRUS SCAN ENTERPRISE SCAN BOP	Out of scope
HOST IPS	Out of scope
NETWORK SECURITY PLATFORM	No Coverage Status
VULNERABILITY MANAGER	An upcoming FSL/MVM content release will contain coverage for this issue.
WEB GATEWAY	Out of scope
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	Microsoft: Security Update Summary

[Back to top](#)

(MSPT-Jul2020) Microsoft Windows MDM Privilege Escalation (CVE-2020-1405)

MTIS20-037-S

THREAT IDENTIFIER(S)	CVE-2020-1405
THREAT TYPE	Vulnerability
RISK ASSESSMENT	Medium
MAIN THREAT VECTORS	Locally logged-on user
USER INTERACTION REQUIRED	No
DESCRIPTION	A vulnerability in some versions of Microsoft Windows could lead to privilege escalation. The flaw lies in the MDM component. Successful exploitation could allow a local user to gain elevated privileges. The exploit requires the attacker to have valid credentials to the vulnerable system.
IMPORTANCE	Medium. On July 14, Microsoft released an update to address this vulnerability
MCAFFEE PRODUCT COVERAGE	
DAT FILES	Out of scope
VIRUS SCAN ENTERPRISE SCAN BOP	Out of scope
HOST IPS	Out of scope
NETWORK SECURITY PLATFORM	No Coverage Status
VULNERABILITY MANAGER	An upcoming FSL/MVM content release will contain coverage for this issue.
WEB GATEWAY	Out of scope
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	Microsoft: Security Update Summary

[Back to top](#)

(MSPT-Jul2020) Microsoft Windows Network List Service Privilege Escalation (CVE-2020-1406)

MTIS20-037-T

THREAT IDENTIFIER(S)	CVE-2020-1406
THREAT TYPE	Vulnerability
RISK ASSESSMENT	Medium
MAIN THREAT VECTORS	Locally logged-on user
USER INTERACTION REQUIRED	No
DESCRIPTION	A vulnerability in some versions of Microsoft Windows could lead to privilege escalation. The flaw lies in the Network List Service component. Successful exploitation could allow a local user to gain elevated privileges. The exploit requires the attacker to have valid credentials to the vulnerable system.
IMPORTANCE	Medium. On July 14, Microsoft released an update to address this vulnerability
MCAFFEE PRODUCT COVERAGE	
DAT FILES	Out of scope
VIRUS SCAN ENTERPRISE SCAN BOP	Out of scope
HOST IPS	Out of scope
NETWORK SECURITY PLATFORM	No Coverage Status
VULNERABILITY MANAGER	An upcoming FSL/MVM content release will contain coverage for this issue.
WEB GATEWAY	Out of scope
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	Microsoft: Security Update Summary

[Back to top](#)

(MSPT-Jul2020) Microsoft Windows Jet Database Engine Remote Code Execution (CVE-2020-1407)

MTIS20-037-U

THREAT IDENTIFIER(S)	CVE-2020-1407
THREAT TYPE	Vulnerability
RISK ASSESSMENT	Medium
MAIN THREAT VECTORS	Locally logged-on user
USER INTERACTION REQUIRED	Yes
DESCRIPTION	A vulnerability in some versions of Microsoft Windows could lead to remote code execution. The flaw lies in the Jet Database Engine 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	Medium. On July 14, Microsoft released an update to address this vulnerability
MCAFFEE PRODUCT COVERAGE	
DAT FILES	Coverage not warranted at this time
VIRUS SCAN ENTERPRISE SCAN BOP	Out of scope
HOST IPS	Out of scope
NETWORK SECURITY PLATFORM	No Coverage Status
VULNERABILITY MANAGER	An upcoming FSL/MVM content release will contain coverage for this issue.
WEB GATEWAY	Coverage not warrantedat this time
REMEDATION 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	Microsoft: Security Update Summary

[Back to top](#)

(MSPT-Jul2020) Microsoft Windows Font Library Remote Code Execution (CVE-2020-1408)

MTIS20-037-V

THREAT IDENTIFIER(S)	CVE-2020-1408
THREAT TYPE	Vulnerability
RISK ASSESSMENT	Medium
MAIN THREAT VECTORS	Web
USER INTERACTION REQUIRED	Yes
DESCRIPTION	A vulnerability in some versions of Microsoft Windows could lead to remote code execution. The flaw lies in the Font Library 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	Medium. On July 14, Microsoft released an update to address this vulnerability
MCAFFEE PRODUCT COVERAGE	
DAT FILES	Coverage not warranted at this time
VIRUS SCAN ENTERPRISE SCAN BOP	Out of scope

HOST IPS	Out of scope
NETWORK SECURITY PLATFORM	No Coverage Status
VULNERABILITY MANAGER	An upcoming FSL/MVM content release will contain coverage for this issue.
WEB GATEWAY	Coverage not warrantedat this time
REMEDATION 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	Microsoft: Security Update Summary

[Back to top](#)

(MSPT-Jul2020) Microsoft DirectWrite Improperly Handles Objects in Memory Remote Code Execution (CVE-2020-1409)

MTIS20-037-W

THREAT IDENTIFIER(S)	CVE-2020-1409
THREAT TYPE	Vulnerability
RISK ASSESSMENT	High
MAIN THREAT VECTORS	Web
USER INTERACTION REQUIRED	Yes
DESCRIPTION	A vulnerability in some versions of Microsoft DirectWrite could lead to remote code execution. The flaw lies in improperly handle objects in memory. 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	High. On July 14, Microsoft released an update to address this vulnerability
MCAFFEE PRODUCT COVERAGE	
DAT FILES	Coverage not warranted at this time
VIRUS SCAN ENTERPRISE SCAN BOP	Out of scope
HOST IPS	Out of scope
NETWORK SECURITY PLATFORM	No Coverage Status
VULNERABILITY MANAGER	An upcoming FSL/MVM content release will contain coverage for this issue.
WEB GATEWAY	Coverage not warrantedat this time
REMEDATION 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	Microsoft: Security Update Summary

[Back to top](#)

(MSPT-Jul2020) Microsoft Windows Address Book Remote Code Execution (CVE-2020-1410)

MTIS20-037-X

THREAT IDENTIFIER(S)	CVE-2020-1410
THREAT TYPE	Vulnerability
RISK ASSESSMENT	High
MAIN THREAT VECTORS	Web
USER INTERACTION REQUIRED	Yes

DESCRIPTION	A vulnerability in some versions of Microsoft Windows could lead to remote code execution. The flaw lies in the Address Book 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	High. On July 14, Microsoft released an update to address this vulnerability
MCAFFEE PRODUCT COVERAGE	
DAT FILES	Coverage not warranted at this time
VIRUS SCAN ENTERPRISE SCAN BOP	Out of scope
HOST IPS	Out of scope
NETWORK SECURITY PLATFORM	No Coverage Status
VULNERABILITY MANAGER	An upcoming FSL/MVM content release will contain coverage for this issue.
WEB GATEWAY	Coverage not warrantedat this time
REMEDATION 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	Microsoft: Security Update Summary

[Back to top](#)

(MSPT-Jul2020) Microsoft Windows Kernel Privilege Escalation (CVE-2020-1411)

MTIS20-037-Y

THREAT IDENTIFIER(S)	CVE-2020-1411
THREAT TYPE	Vulnerability
RISK ASSESSMENT	Medium
MAIN THREAT VECTORS	Web
USER INTERACTION REQUIRED	No
DESCRIPTION	A vulnerability in some versions of Microsoft Windows could lead to privilege escalation. The flaw lies in the Kernel component. Successful exploitation could allow a local user to gain elevated privileges. The exploit requires the attacker to have valid credentials to the vulnerable system.
IMPORTANCE	Medium. On July 14, Microsoft released an update to address this vulnerability
MCAFFEE PRODUCT COVERAGE	
DAT FILES	Out of scope
VIRUS SCAN ENTERPRISE SCAN BOP	Out of scope
HOST IPS	Out of scope
NETWORK SECURITY PLATFORM	No Coverage Status
VULNERABILITY MANAGER	An upcoming FSL/MVM content release will contain coverage for this issue.
WEB GATEWAY	Out of scope
REMEDATION 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	Microsoft: Security Update Summary

[Back to top](#)

(MSPT-Jul2020) Microsoft Graphics Components improperly handle objects in memory Remote Code Execution (CVE-2020-1412)

MTIS20-037-Z

THREAT IDENTIFIER(S)	CVE-2020-1412
THREAT TYPE	Vulnerability
RISK ASSESSMENT	Medium
MAIN THREAT VECTORS	Locally logged-on user
USER INTERACTION REQUIRED	Yes
DESCRIPTION	A vulnerability in some versions of Microsoft Graphics Components could lead to remote code execution. The flaw lies in improperly handle objects in memory. 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	Medium. On July 14, Microsoft released an update to address this vulnerability
MCAFFEE PRODUCT COVERAGE	
DAT FILES	Coverage not warranted at this time
VIRUS SCAN ENTERPRISE SCAN BOP	Out of scope
HOST IPS	Out of scope
NETWORK SECURITY PLATFORM	No Coverage Status
VULNERABILITY MANAGER	An upcoming FSL/MVM content release will contain coverage for this issue.
WEB GATEWAY	Coverage not warrantedat this time
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	Microsoft: Security Update Summary

[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.

*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.

The information contained herein is the property of McAfee, LLC and may not be reproduced or disseminated without the expressed written consent of McAfee, LLC.

McAfee and the McAfee logo are trademarks or registered trademarks of McAfee, LLC or its subsidiaries in the US and other countries. Other marks and brands may be claimed as the property of others.

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

© 2018 McAfee, LLC. All rights reserved.