

EXECUTIVE SUMMARY

July 15, 2020 | MTIS20-036

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 Font Driver Host Remote Code Execution (CVE-2020-1355)

MTIS20-036-A

IMPORTANCE: Medium
COVERED PRODUCTS:
UNDER ANALYSIS: Firewall Enterprise

[Back to top](#)

(MSPT-Jul2020) Microsoft Windows iSCSI Target Service Privilege Escalation (CVE-2020-1356)

MTIS20-036-B

IMPORTANCE: Medium
COVERED PRODUCTS:
UNDER ANALYSIS: Firewall Enterprise

[Back to top](#)

(MSPT-Jul2020) Microsoft Windows System Events Broker Privilege Escalation (CVE-2020-1357)

MTIS20-036-C

IMPORTANCE: Medium
COVERED PRODUCTS:
UNDER ANALYSIS: Firewall Enterprise

[Back to top](#)

(MSPT-Jul2020) Microsoft Windows Resource Policy Information Disclosure (CVE-2020-1358)

MTIS20-036-D

IMPORTANCE: Medium
COVERED PRODUCTS:
UNDER ANALYSIS: Firewall Enterprise

[Back to top](#)

(MSPT-Jul2020) Microsoft Windows CNG Privilege Escalation (CVE-2020-1359)

MTIS20-036-E

IMPORTANCE: Medium
COVERED PRODUCTS:
UNDER ANALYSIS: Firewall Enterprise

[Back to top](#)

(MSPT-Jul2020) Microsoft Windows Profile Service Privilege Escalation (CVE-2020-1360)

MTIS20-036-F

IMPORTANCE: Medium
COVERED PRODUCTS:
UNDER ANALYSIS: Firewall Enterprise

[Back to top](#)

(MSPT-Jul2020) Microsoft Windows Wallet Service Information Disclosure (CVE-2020-1361)

MTIS20-036-G

IMPORTANCE: Medium
COVERED PRODUCTS:
UNDER ANALYSIS: Firewall Enterprise

[Back to top](#)

(MSPT-Jul2020) Microsoft Windows WalletService Privilege Escalation (CVE-2020-1362)

MTIS20-036-H

IMPORTANCE: Medium
COVERED PRODUCTS:
UNDER ANALYSIS: Firewall Enterprise

[Back to top](#)

(MSPT-Jul2020) Microsoft Windows Picker Platform Privilege Escalation (CVE-2020-1363)

MTIS20-036-I

IMPORTANCE: Medium
COVERED PRODUCTS:
UNDER ANALYSIS: Firewall Enterprise

[Back to top](#)

(MSPT-Jul2020) Microsoft Windows Wallet Service Denial of Service (CVE-2020-1364)

MTIS20-036-J

IMPORTANCE: Medium
COVERED PRODUCTS:
UNDER ANALYSIS: Firewall Enterprise

[Back to top](#)

(MSPT-Jul2020) Microsoft Windows Event Logging Service Privilege Escalation (CVE-2020-1365)

MTIS20-036-K

IMPORTANCE: Medium
COVERED PRODUCTS:
UNDER ANALYSIS: Firewall Enterprise

[Back to top](#)

(MSPT-Jul2020) Microsoft Windows Print Workflow Service Privilege Escalation (CVE-2020-1366)

MTIS20-036-L

IMPORTANCE: Medium
COVERED PRODUCTS:
UNDER ANALYSIS: Firewall Enterprise

[Back to top](#)

(MSPT-Jul2020) Microsoft Windows Kernel Information Disclosure (CVE-2020-1367)

MTIS20-036-M

IMPORTANCE: Medium
COVERED PRODUCTS:
UNDER ANALYSIS: Firewall Enterprise

[Back to top](#)

(MSPT-Jul2020) Microsoft Windows Credential Enrollment Manager Service Privilege Escalation (CVE-2020-1368)
MTIS20-036-N

IMPORTANCE: Medium
COVERED PRODUCTS:
UNDER ANALYSIS: Firewall Enterprise

[Back to top](#)

(MSPT-Jul2020) Microsoft Windows WalletService Privilege Escalation (CVE-2020-1369)
MTIS20-036-O

IMPORTANCE: Medium
COVERED PRODUCTS:
UNDER ANALYSIS: Firewall Enterprise

[Back to top](#)

(MSPT-Jul2020) Microsoft Windows Runtime Privilege Escalation (CVE-2020-1370)
MTIS20-036-P

IMPORTANCE: Medium
COVERED PRODUCTS:
UNDER ANALYSIS: Firewall Enterprise

[Back to top](#)

(MSPT-Jul2020) Microsoft Windows Event Logging Service Privilege Escalation (CVE-2020-1371)
MTIS20-036-Q

IMPORTANCE: Medium
COVERED PRODUCTS:
UNDER ANALYSIS: Firewall Enterprise

[Back to top](#)

(MSPT-Jul2020) Microsoft Windows MDM Privilege Escalation (CVE-2020-1372)
MTIS20-036-R

IMPORTANCE: Medium
COVERED PRODUCTS:
UNDER ANALYSIS: Firewall Enterprise

[Back to top](#)

(MSPT-Jul2020) Microsoft Windows Network Connections Service Privilege Escalation (CVE-2020-1373)
MTIS20-036-S

IMPORTANCE: Medium
COVERED PRODUCTS:
UNDER ANALYSIS: Firewall Enterprise

[Back to top](#)

(MSPT-Jul2020) Microsoft Windows Remote Desktop Client Remote Code Execution (CVE-2020-1374)
MTIS20-036-T

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

[Back to top](#)

(MSPT-Jul2020) Microsoft Windows COM Object Creation Privilege Escalation (CVE-2020-1375)

MTIS20-036-U

IMPORTANCE: Medium
COVERED PRODUCTS:
UNDER ANALYSIS: Firewall Enterprise

[Back to top](#)

(MSPT-Jul2020) Microsoft Windows Graphics Privilege Escalation (CVE-2020-1381)

MTIS20-036-V

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

[Back to top](#)

(MSPT-Jul2020) Microsoft Windows Graphics Privilege Escalation (CVE-2020-1382)

MTIS20-036-W

IMPORTANCE: Medium
COVERED PRODUCTS: DAT
UNDER ANALYSIS: Firewall Enterprise

[Back to top](#)

(MSPT-Jul2020) Microsoft Windows CNG Privilege Escalation (CVE-2020-1384)

MTIS20-036-X

IMPORTANCE: Medium
COVERED PRODUCTS:
UNDER ANALYSIS: Firewall Enterprise

[Back to top](#)

(MSPT-Jul2020) Microsoft Windows Credential Picker Privilege Escalation (CVE-2020-1385)

MTIS20-036-Y

IMPORTANCE: Medium
COVERED PRODUCTS:
UNDER ANALYSIS: Firewall Enterprise

[Back to top](#)

(MSPT-Jul2020) Microsoft Windows Feedback Hub Information Disclosure (CVE-2020-1386)

MTIS20-036-Z

IMPORTANCE: Medium
COVERED PRODUCTS:
UNDER ANALYSIS: Firewall Enterprise

[Back to top](#)

THREAT DETAILS

(MSPT-Jul2020) Microsoft Windows Font Driver Host Remote Code Execution (CVE-2020-1355)

MTIS20-036-A

THREAT IDENTIFIER(S)	CVE-2020-1355
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 remote code execution. The flaw lies in the Font Driver Host component. 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	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 iSCSI Target Service Privilege Escalation (CVE-2020-1356)

MTIS20-036-B

THREAT IDENTIFIER(S)	CVE-2020-1356
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 iSCSI Target 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	No Coverage Status
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 System Events Broker Privilege Escalation (CVE-2020-1357)

MTIS20-036-C

THREAT IDENTIFIER(S)	CVE-2020-1357
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 System Events Broker 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 Resource Policy Information Disclosure (CVE-2020-1358)

MTIS20-036-D

THREAT IDENTIFIER(S)	CVE-2020-1358
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 Resource Policy 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
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 CNG Privilege Escalation (CVE-2020-1359)

MTIS20-036-E

THREAT IDENTIFIER(S)	CVE-2020-1359
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 CNG 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 Profile Service Privilege Escalation (CVE-2020-1360)

MTIS20-036-F

THREAT IDENTIFIER(S)	CVE-2020-1360
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 Profile 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 Windows Wallet Service Information Disclosure (CVE-2020-1361)

MTIS20-036-G

THREAT IDENTIFIER(S)	CVE-2020-1361
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 Wallet Service 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
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 WalletService Privilege Escalation (CVE-2020-1362)

MTIS20-036-H

THREAT IDENTIFIER(S)	CVE-2020-1362
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 WalletService 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 Picker Platform Privilege Escalation (CVE-2020-1363)

MTIS20-036-1

THREAT IDENTIFIER(S)	CVE-2020-1363
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 Picker Platform 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 Wallet Service Denial of Service (CVE-2020-1364)

MTIS20-036-J

THREAT IDENTIFIER(S)	CVE-2020-1364
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 a denial of service. The flaw lies in the Wallet Service component. Successful exploitation by a remote attacker could result in a denial of service condition. 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 Event Logging Service Privilege Escalation (CVE-2020-1365)

MTIS20-036-K

THREAT IDENTIFIER(S)	CVE-2020-1365
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 Event Logging 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 Print Workflow Service Privilege Escalation (CVE-2020-1366)

MTIS20-036-L

THREAT IDENTIFIER(S)	CVE-2020-1366
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 Print Workflow 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-2020-1367)

MTIS20-036-M

THREAT IDENTIFIER(S)	CVE-2020-1367
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
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 Credential Enrollment Manager Service Privilege Escalation (CVE-2020-1368)

MTIS20-036-N

THREAT IDENTIFIER(S)	CVE-2020-1368
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 Credential Enrollment Manager 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 WalletService Privilege Escalation (CVE-2020-1369)

MTIS20-036-O

THREAT IDENTIFIER(S)	CVE-2020-1369
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 WalletService 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-2020-1370)

MTIS20-036-P

THREAT IDENTIFIER(S)	CVE-2020-1370
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
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 Event Logging Service Privilege Escalation (CVE-2020-1371)

MTIS20-036-Q

THREAT IDENTIFIER(S)	CVE-2020-1371
THREAT TYPE	Vulnerability
RISK ASSESSMENT	Medium
MAIN THREAT VECTORS	Locally logged-on user
USER INTERACTION REQUIRED	No
	A vulnerability in some versions of Microsoft Windows could lead to privilege

DESCRIPTION	escalation. The flaw lies in the Event Logging 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 MDM Privilege Escalation (CVE-2020-1372)

MTIS20-036-R

THREAT IDENTIFIER(S)	CVE-2020-1372
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 an attacker 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 Network Connections Service Privilege Escalation (CVE-2020-1373)

THREAT IDENTIFIER(S)	CVE-2020-1373
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
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 Remote Desktop Client Remote Code Execution (CVE-2020-1374)

MTIS20-036-T

THREAT IDENTIFIER(S)	CVE-2020-1374
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 Windows could lead to remote code execution. The flaw lies in the Remote Desktop Client component. 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
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 COM Object Creation Privilege Escalation (CVE-2020-1375)

MTIS20-036-U

THREAT IDENTIFIER(S)	CVE-2020-1375
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 improperly handles COM object creation. 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 Graphics Privilege Escalation (CVE-2020-1381)

MTIS20-036-V

THREAT IDENTIFIER(S)	CVE-2020-1381
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 Graphics 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	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 Graphics Privilege Escalation (CVE-2020-1382)

MTIS20-036-W

THREAT IDENTIFIER(S)	CVE-2020-1382
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 Graphics 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	The upcoming package includes a vulnerability check to assess if your systems are at risk.
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	The upcoming package includes a vulnerability check to assess if your systems are at risk.
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 CNG Privilege Escalation (CVE-2020-1384)

MTIS20-036-X

THREAT IDENTIFIER(S)	CVE-2020-1384
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 CNG 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 Credential Picker Privilege Escalation (CVE-2020-1385)***MTIS20-036-Y*

THREAT IDENTIFIER(S)	CVE-2020-1385
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 Credential Picker 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 Feedback Hub Information Disclosure (CVE-2020-1386)***MTIS20-036-Z*

THREAT IDENTIFIER(S)	CVE-2020-1386
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 Feedback Hub component. Successful exploitation by an 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](#)

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.