EXECUTIVE SUMMARY

December 8, 2020 | MTIS20-060

Since the last McAfee® Labs Security Advisory (December 8), the following noteworthy event has taken place:

- Patches are available for multiple Microsoft security vulnerabilities

NEW THREAT OVERVIEW

(MSPT-Dec2020) Microsoft Windows Backup Engine Privilege Escalation (CVE-2020-16958)

MTIS20-060-A

IMPORTANCE: Medium
COVERED PRODUCTS:
UNDER ANALYSIS: Firewall Enterprise

Back to top

(MSPT-Dec2020) Microsoft Windows Backup Engine Privilege Escalation (CVE-2020-16959)

MTIS20-060-B

IMPORTANCE: Medium
COVERED PRODUCTS:
UNDER ANALYSIS: Firewall Enterprise

Back to top

(MSPT-Dec2020) Microsoft Windows Backup Engine Privilege Escalation (CVE-2020-16960)

MTIS20-060-C

IMPORTANCE: Medium
COVERED PRODUCTS:
UNDER ANALYSIS: Firewall Enterprise

Back to top

(MSPT-Dec2020) Microsoft Windows Backup Engine Privilege Escalation (CVE-2020-16961)

MTIS20-060-D

IMPORTANCE: Medium
COVERED PRODUCTS:
UNDER ANALYSIS: Firewall Enterprise

Back to top

(MSPT-Dec2020) Microsoft Windows Backup Engine Privilege Escalation (CVE-2020-16962)

MTIS20-060-E

IMPORTANCE: Medium
COVERED PRODUCTS:
UNDER ANALYSIS: Firewall Enterprise

Back to top

(MSPT-Dec2020) Microsoft Windows Backup Engine Privilege Escalation (CVE-2020-16963)

MTIS20-060-F

IMPORTANCE: Medium
COVERED PRODUCTS:
UNDER ANALYSIS: Firewall Enterprise

Back to top

(MSPT-Dec2020) Microsoft Windows Backup Engine Privilege Escalation (CVE-2020-16964)

MTIS20-060-G

IMPORTANCE: Medium
COVERED PRODUCTS:
UNDER ANALYSIS: Firewall Enterprise

Back to top

(MSPT-Dec2020) Microsoft Azure SDK Privilege Escalation (CVE-2020-16971)

MTIS20-060-H

IMPORTANCE: Medium
COVERED PRODUCTS:
UNDER ANALYSIS: Firewall Enterprise

Back to top

(MSPT-Dec2020) Microsoft Windows Kerberos Remote Code Execution (CVE-2020-16996)

MTIS20-060-I

IMPORTANCE: Medium
COVERED PRODUCTS:
UNDER ANALYSIS: Firewall Enterprise

Back to top

(MSPT-Dec2020) Microsoft Azure SDK Privilege Escalation (CVE-2020-17002)

MTIS20-060-J

IMPORTANCE: Medium
COVERED PRODUCTS:
UNDER ANALYSIS: Firewall Enterprise

Back to top

(MSPT-Dec2020) Microsoft Office SharePoint Privilege Escalation (CVE-2020-17089)

MTIS20-060-K

IMPORTANCE: Medium
COVERED PRODUCTS:
UNDER ANALYSIS: Firewall Enterprise

Back to top

(MSPT-Dec2020) Microsoft Windows Network Connections Privilege Escalation (CVE-2020-17092)

MTIS20-060-L

IMPORTANCE: Medium
COVERED PRODUCTS:
UNDER ANALYSIS: Firewall Enterprise

Back to top

(MSPT-Dec2020) Microsoft Windows Error Reporting Information Disclosure (CVE-2020-17094)

MTIS20-060-M

IMPORTANCE: Medium
COVERED PRODUCTS:
UNDER ANALYSIS: Firewall Enterprise

Back to top

(MSPT-Dec2020) Microsoft Windows Hyper-V Remote Code Execution (CVE-2020-17095)
MTIS20-060-N

IMPORTANCE: High
COVERED PRODUCTS:
UNDER ANALYSIS: Firewall Enterprise

Back to top

(MSPT-Dec2020) Microsoft Windows NTFS Remote Code Execution (CVE-2020-17096)
MTIS20-060-O

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

Back to top

(MSPT-Dec2020) Microsoft Windows Media Privilege Escalation (CVE-2020-17097)
MTIS20-060-P

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

Back to top

(MSPT-Dec2020) Microsoft Windows Graphics Information Disclosure (CVE-2020-17098)
MTIS20-060-Q

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

Back to top

(MSPT-Dec2020) Microsoft Windows Lock Screen Remote Code Execution (CVE-2020-17099)
MTIS20-060-R

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

Back to top

(MSPT-Dec2020) Microsoft Windows Cloud Files Mini Filter Driver Privilege Escalation (CVE-2020-17103)
MTIS20-060-S

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

Back to top

(MSPT-Dec2020) Microsoft Office SharePoint Spoofing Vulnerability (CVE-2020-17115)
MTIS20-060-T

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

Back to top

(MSPT-Dec2020) Microsoft Windows Exchange Server Remote Code Execution (CVE-2020-17117)

MTIS20-060-U

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

Back to top

(MSPT-Dec2020) Microsoft Office SharePoint Remote Code Execution (CVE-2020-17118)

MTIS20-060-V

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

Back to top

(MSPT-Dec2020) Microsoft Office Outlook Information Disclosure (CVE-2020-17119)

MTIS20-060-W

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

Back to top

(MSPT-Dec2020) Microsoft Office SharePoint Information Disclosure (CVE-2020-17120)

MTIS20-060-X

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

Back to top

(MSPT-Dec2020) Microsoft Office SharePoint Remote Code Execution (CVE-2020-17121)

MTIS20-060-Y

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

Back to top

(MSPT-Dec2020) Microsoft Office Excel Remote Code Execution (CVE-2020-17122)

MTIS20-060-Z

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

Back to top

THREAT DETAILS

(MSPT-Dec2020) Microsoft Windows Backup Engine Privilege Escalation (CVE-2020-16958)

MTIS20-060-A

THREAT IDENTIFIER(S)	CVE-2020-16958
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 Backup Engine component. Successful exploitation could allow a local user to gain elevated privileges.
IMPORTANCE	Medium. On December 8, 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	Coverage not warranted
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-Dec2020) Microsoft Windows Backup Engine Privilege Escalation (CVE-2020-16959)

MTIS20-060-B

THREAT IDENTIFIER(S)	CVE-2020-16959
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 Backup Engine component. Successful exploitation could allow a local user to gain elevated privileges.
IMPORTANCE	Medium. On December 8, 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	Coverage not warranted
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-Dec2020) Microsoft Windows Backup Engine Privilege Escalation (CVE-2020-16960)

MTIS20-060-C

THREAT IDENTIFIER(S)	CVE-2020-16960
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 Backup Engine component. Successful exploitation could allow a local user to gain elevated privileges.
IMPORTANCE	Medium. On December 8, 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	Coverage not warranted
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-Dec2020) Microsoft Windows Backup Engine Privilege Escalation (CVE-2020-16961)

MTIS20-060-D

THREAT IDENTIFIER(S)	CVE-2020-16961
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 Backup Engine component. Successful exploitation could allow a local user to gain elevated privileges.
IMPORTANCE	Medium. On December 8, 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	Coverage not warranted
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-Dec2020) Microsoft Windows Backup Engine Privilege Escalation (CVE-2020-16962)

MTIS20-060-E

THREAT IDENTIFIER(S)	CVE-2020-16962
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 Backup Engine component. Successful exploitation could allow a local user to gain elevated privileges.
IMPORTANCE	Medium. On December 8, 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	Coverage not warranted
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-Dec2020) Microsoft Windows Backup Engine Privilege Escalation (CVE-2020-16963)

MTIS20-060-F

THREAT IDENTIFIER(S)	CVE-2020-16963
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 Backup Engine component. Successful exploitation could allow a local user to gain elevated privileges.
IMPORTANCE	Medium. On December 8, 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	Coverage not warranted
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-Dec2020) Microsoft Windows Backup Engine Privilege Escalation (CVE-2020-16964)

MTIS20-060-G

THREAT IDENTIFIER(S)	CVE-2020-16964
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 Backup Engine component. Successful exploitation could allow a local user to gain elevated privileges.
IMPORTANCE	Medium. On December 8, 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	Coverage not warranted
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-Dec2020) Microsoft Azure SDK Privilege Escalation (CVE-2020-16971)

MTIS20-060-H

THREAT IDENTIFIER(S)	CVE-2020-16971
THREAT TYPE	Vulnerability
RISK ASSESSMENT	Medium
MAIN THREAT VECTORS	Web
USER INTERACTION REQUIRED	No
DESCRIPTION	A vulnerability in some versions of Microsoft Azure could lead to privilege escalation. The flaw lies in the SDK component. Successful exploitation could allow a local user to gain elevated privileges.
IMPORTANCE	Medium. On December 8, 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	Coverage not warranted
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-Dec2020) Microsoft Windows Kerberos Remote Code Execution (CVE-2020-16996)

MTIS20-060-I

THREAT IDENTIFIER(S)	CVE-2020-16996
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 remote code execution. The flaw lies in the Kerberos component. Successful exploitation by a remote attacker could result in the execution of arbitrary code.
IMPORTANCE	Medium. On December 8, 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	Coverage not warranted
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-Dec2020) Microsoft Azure SDK Privilege Escalation (CVE-2020-17002)

MTIS20-060-J

THREAT IDENTIFIER(S)	CVE-2020-17002
THREAT TYPE	Vulnerability
RISK ASSESSMENT	Medium
MAIN THREAT VECTORS	Web
USER INTERACTION REQUIRED	No
DESCRIPTION	A vulnerability in some versions of Microsoft Azure could lead to privilege escalation. The flaw lies in the SDK component. Successful exploitation could allow a local user to gain elevated privileges.

IMPORTANCE	Medium. On December 8, 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	Coverage not warranted
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-Dec2020) Microsoft Office SharePoint Privilege Escalation (CVE-2020-17089)

MTIS20-060-K

THREAT IDENTIFIER(S)	CVE-2020-17089
THREAT TYPE	Vulnerability
RISK ASSESSMENT	Medium
MAIN THREAT VECTORS	Web
USER INTERACTION REQUIRED	No
DESCRIPTION	A vulnerability in some versions of Microsoft Office could lead to privilege escalation. The flaw lies in the SharePoint component. Successful exploitation could allow an attacker to gain elevated privileges.
IMPORTANCE	Medium. On December 8, 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	Coverage not warranted
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-Dec2020) Microsoft Windows Network Connections Privilege Escalation (CVE-2020-17092)

MTIS20-060-L

THREAT IDENTIFIER(S)	CVE-2020-17092
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 Network Connections component. Successful exploitation could allow a local user to gain elevated privileges.
IMPORTANCE	Medium. On December 8, 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	Coverage not warranted
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-Dec2020) Microsoft Windows Error Reporting Information Disclosure (CVE-2020-17094)

MTIS20-060-M

THREAT IDENTIFIER(S)	CVE-2020-17094
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 information disclosure. The flaw lies in the Error Reporting component. Successful exploitation by an attacker could result in the disclosure of sensitive information.
IMPORTANCE	Medium. On December 8, 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	Coverage not warranted
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-Dec2020) Microsoft Windows Hyper-V Remote Code Execution (CVE-2020-17095)

MTIS20-060-N

THREAT IDENTIFIER(S)	CVE-2020-17095
THREAT TYPE	Vulnerability
RISK ASSESSMENT	High
MAIN THREAT VECTORS	Web
USER INTERACTION REQUIRED	No
DESCRIPTION	A vulnerability in some versions of Microsoft Windows could lead to remote code execution. The flaw lies in the Hyper-V component. Successful exploitation by a remote attacker could result in the execution of arbitrary code.
IMPORTANCE	High. On December 8, 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	Coverage not warranted
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-Dec2020) Microsoft Windows NTFS Remote Code Execution (CVE-2020-17096)

MTIS20-060-O

THREAT IDENTIFIER(S)	CVE-2020-17096
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 remote code execution. The flaw lies in the NTFS component. Successful exploitation by a remote attacker could result in the execution of arbitrary code.
IMPORTANCE	Medium. On December 8, 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	Coverage not warranted
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-Dec2020) Microsoft Windows Media Privilege Escalation (CVE-2020-17097)

MTIS20-060-P

THREAT IDENTIFIER(S)	CVE-2020-17097
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 Media component. Successful exploitation could allow a local user to gain elevated privileges.
IMPORTANCE	Medium. On December 8, 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	Coverage not warranted
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-Dec2020) Microsoft Windows Graphics Information Disclosure (CVE-2020-17098)

MTIS20-060-Q

THREAT IDENTIFIER(S)	CVE-2020-17098
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 information disclosure. The flaw lies in the Graphics component. Successful exploitation by a remote attacker could result in the disclosure of sensitive information.
IMPORTANCE	Medium. On December 8, 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	Coverage not warranted
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-Dec2020) Microsoft Windows Lock Screen Remote Code Execution (CVE-2020-17099)

MTIS20-060-R

THREAT IDENTIFIER(S)	CVE-2020-17099
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 remote code execution. The flaw lies in the Lock Screen component. Successful exploitation by a remote attacker could result in the execution of arbitrary code.
IMPORTANCE	Medium. On December 8, 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	Coverage not warranted
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-Dec2020) Microsoft Windows Cloud Files Mini Filter Driver Privilege Escalation (CVE-2020-17103)

MTIS20-060-S

THREAT IDENTIFIER(S)	CVE-2020-17103
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 Cloud Files Mini Filter Driver component. Successful exploitation could allow a local user to gain elevated privileges.
IMPORTANCE	Medium. On December 8, 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	Coverage not warranted
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-Dec2020) Microsoft Office SharePoint Spoofing Vulnerability (CVE-2020-17115)

MTIS20-060-T

THREAT IDENTIFIER(S)	CVE-2020-17115
THREAT TYPE	Vulnerability
RISK ASSESSMENT	Low
MAIN THREAT VECTORS	Web
USER INTERACTION REQUIRED	No
DESCRIPTION	A vulnerability in some versions of Microsoft Office could lead to spoofing. The flaw lies in the SharePoint component. Successful exploitation by a remote attacker could result in the spoofing vulnerability.
IMPORTANCE	Low. On December 8, 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	Coverage not warranted
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-Dec2020) Microsoft Windows Exchange Server Remote Code Execution (CVE-2020-17117)

MTIS20-060-U

THREAT IDENTIFIER(S)	CVE-2020-17117
THREAT TYPE	Vulnerability
RISK ASSESSMENT	High
MAIN THREAT VECTORS	Web

USER INTERACTION REQUIRED	No
DESCRIPTION	A vulnerability in some versions of Microsoft Windows could lead to remote code execution. The flaw lies in the Exchange Server component. Successful exploitation by a remote attacker could result in the execution of arbitrary code.
IMPORTANCE	High. On December 8, 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	Coverage not warranted
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-Dec2020) Microsoft Office SharePoint Remote Code Execution (CVE-2020-17118)

MTIS20-060-V

THREAT IDENTIFIER(S)	CVE-2020-17118
THREAT TYPE	Vulnerability
RISK ASSESSMENT	High
MAIN THREAT VECTORS	Web
USER INTERACTION REQUIRED	No
DESCRIPTION	A vulnerability in some versions of Microsoft Office could lead to remote code execution. The flaw lies in the SharePoint component. Successful exploitation by a remote attacker could result in the execution of arbitrary code.
IMPORTANCE	High. On December 8, 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	Coverage not warranted
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-Dec2020) Microsoft Office Outlook Information Disclosure (CVE-2020-17119)

MTIS20-060-W

THREAT IDENTIFIER(S)	CVE-2020-17119
THREAT TYPE	Vulnerability
RISK ASSESSMENT	Medium
MAIN THREAT VECTORS	Web
USER INTERACTION REQUIRED	No
DESCRIPTION	A vulnerability in some versions of Microsoft Office could lead to information disclosure. The flaw lies in the Outlook component. Successful exploitation by a remote attacker could result in the disclosure of sensitive information.
IMPORTANCE	Medium. On December 8, 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	Coverage not warranted
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-Dec2020) Microsoft Office SharePoint Information Disclosure (CVE-2020-17120)

MTIS20-060-X

THREAT IDENTIFIER(S)	CVE-2020-17120
THREAT TYPE	Vulnerability
RISK ASSESSMENT	Medium
MAIN THREAT VECTORS	Web
USER INTERACTION REQUIRED	No
DESCRIPTION	A vulnerability in some versions of Microsoft Office could lead to information disclosure. The flaw lies in the SharePoint component. Successful exploitation by a remote attacker could result in the disclosure of sensitive information.
IMPORTANCE	Medium. On December 8, 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	Coverage not warranted
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-Dec2020) Microsoft Office SharePoint Remote Code Execution (CVE-2020-17121)

MTIS20-060-Y

THREAT IDENTIFIER(S)	CVE-2020-17121
THREAT TYPE	Vulnerability
RISK ASSESSMENT	High
MAIN THREAT VECTORS	Web
USER INTERACTION REQUIRED	No
DESCRIPTION	A vulnerability in some versions of Microsoft Office could lead to remote code execution. The flaw lies in the SharePoint component. Successful exploitation by a remote attacker could result in the execution of arbitrary code.
IMPORTANCE	High. On December 8, 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	Coverage not warranted
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-Dec2020) Microsoft Office Excel Remote Code Execution (CVE-2020-17122)

MTIS20-060-Z

THREAT IDENTIFIER(S)	CVE-2020-17122
THREAT TYPE	Vulnerability
RISK ASSESSMENT	Medium
MAIN THREAT VECTORS	Web
USER INTERACTION REQUIRED	No
DESCRIPTION	A vulnerability in some versions of Microsoft Office could lead to remote code execution. The flaw lies in the Excel component. Successful exploitation by an attacker could result in the execution of arbitrary code.
IMPORTANCE	Medium. On December 8, 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	Coverage not warranted
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

For McAfee Technical Support, click here.

For Multi-National Phone Support, click here.

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

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

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