EXECUTIVE SUMMARY

July 15, 2020 | MTIS20-039

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 SharePoint Server Improperly Sanitize a Specially Crafted Request Spoofing (CVE-2020-1443)

MTIS20-039-A

IMPORTANCE: Medium
COVERED PRODUCTS:
UNDER ANALYSIS: Firewall Enterprise

Back to top

(MSPT-Jul2020) Microsoft SharePoint Software Parses Specially Crafted Email Messages Remote Code Execution (CVE-2020-1444)

MTIS20-039-B

IMPORTANCE: Medium
COVERED PRODUCTS:
UNDER ANALYSIS: Firewall Enterprise

Back to top

(MSPT-Jul2020) Microsoft Office Improperly Discloses The Contents Of Its Memory Information Disclosure (CVE-2020-1445)

MTIS20-039-C

IMPORTANCE: Medium
COVERED PRODUCTS:
UNDER ANALYSIS: Firewall Enterprise

Back to top

(MSPT-Jul2020) Microsoft Word improperly handle objects in memory Remote Code Execution (CVE-2020-1446)

MTIS20-039-D

IMPORTANCE: Medium
COVERED PRODUCTS:
UNDER ANALYSIS: Firewall Enterprise

Back to top

(MSPT-Jul2020) Microsoft Word improperly handle objects in memory Remote Code Execution (CVE-2020-1447)

MTIS20-039-E

IMPORTANCE: Medium

COVERED PRODUCTS:
UNDER ANALYSIS: Firewall Enterprise

Back to top

(MSPT-Jul2020) Microsoft Word improperly handle objects in memory Remote Code Execution (CVE-2020-1448)

MTIS20-039-F

IMPORTANCE: Medium
COVERED PRODUCTS:
UNDER ANALYSIS: Firewall Enterprise

Back to top

(MSPT-Jul2020) Microsoft Project Improperly Execute Macros Remote Code Execution (CVE-2020-1449)

MTIS20-039-G

IMPORTANCE: Medium
COVERED PRODUCTS:
UNDER ANALYSIS: Firewall Enterprise

Back to top

(MSPT-Jul2020) Microsoft SharePoint Server Improperly Sanitize a Specially Crafted Web Request Remote Code Execution (CVE-2020-1450)

MTIS20-039-H

IMPORTANCE: Medium
COVERED PRODUCTS:
UNDER ANALYSIS: Firewall Enterprise

Back to top

(MSPT-Jul2020) Microsoft SharePoint Server Improperly Sanitize a Specially Crafted Web Request Remote Code Execution (CVE-2020-1451)

MTIS20-039-I

IMPORTANCE: Medium
COVERED PRODUCTS:
UNDER ANALYSIS: Firewall Enterprise

Back to top

(MSPT-Jul2020) Microsoft SharePoint Server Improperly Sanitize a Specially Crafted Web Request Remote Code Execution (CVE-2020-1454)

MTIS20-039-J

IMPORTANCE: Medium
COVERED PRODUCTS:
UNDER ANALYSIS: Firewall Enterprise

Back to top

(MSPT-Jul2020) Microsoft SharePoint Server Improperly Sanitize a Specially Crafted Web Request Remote Code Execution (CVE-2020-1456)

MTIS20-039-K

IMPORTANCE: Medium
COVERED PRODUCTS:
UNDER ANALYSIS: Firewall Enterprise

Back to top

(MSPT-Jul2020) Microsoft Office DLL Remote Code Execution (CVE-2020-1458)

MTIS20-039-L

IMPORTANCE: Medium

COVERED PRODUCTS:
UNDER ANALYSIS: Firewall Enterprise

Back to top

(MSPT-Jul2020) Microsoft Defender MpSigStub.exe Privilege Escalation (CVE-2020-1461)

MTIS20-039-M

IMPORTANCE: Medium
COVERED PRODUCTS:
UNDER ANALYSIS: Firewall Enterprise

Back to top

(MSPT-Jul2020) Microsoft Edge Skype Information Disclosure (CVE-2020-1462)

MTIS20-039-N

IMPORTANCE: Medium
COVERED PRODUCTS:
UNDER ANALYSIS: Firewall Enterprise

Back to top

(MSPT-Jul2020) Microsoft SharedStream Library Improperly Handles Objects in Memory Privilege Escalation (CVE-2020-1463)

MTIS20-039-O

IMPORTANCE: Medium
COVERED PRODUCTS:
UNDER ANALYSIS: Firewall Enterprise

Back to top

(MSPT-Jul2020) Microsoft Windows OneDrive Privilege Escalation (CVE-2020-1465)

MTIS20-039-P

IMPORTANCE: Medium
COVERED PRODUCTS:
UNDER ANALYSIS: Firewall Enterprise

Back to top

(MSPT-Jul2020) Microsoft Windows GDI Information Disclosure (CVE-2020-1468)

MTIS20-039-Q

IMPORTANCE: Medium
COVERED PRODUCTS:
UNDER ANALYSIS: Firewall Enterprise

Back to top

(MSPT-Jul2020) Microsoft .NET Bond Denial of Service (CVE-2020-1469)

MTIS20-039-R

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

Back to top

(MSPT-Jul2020) Microsoft Windows Visual Studio Remote Code Execution (CVE-2020-1481)

MTIS20-039-S

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

Back to top

THREAT DETAILS

(MSPT-Jul2020) Microsoft SharePoint Server Improperly Sanitize a Specially Crafted Request Spoofing (CVE-2020-1443)

MTIS20-039-A

THREAT IDENTIFIER(S)	CVE-2020-1443
THREAT TYPE	Vulnerability
RISK ASSESSMENT	Medium
MAIN THREAT VECTORS	Web
USER INTERACTION REQUIRED	Yes
DESCRIPTION	A vulnerability in some versions of Microsoft SharePoint Server could lead to spoofing. The flaw lies improperly sanitize a specially crafted request. Successful exploitation by a remote attacker could result in spoofing 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
MCAFEE 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	No Coverage Status
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 SharePoint Software Parses Specially Crafted Email Messages Remote Code Execution (CVE-2020-1444)

MTIS20-039-B

THREAT IDENTIFIER(S)	CVE-2020-1444
THREAT TYPE	Vulnerability
RISK ASSESSMENT	Medium
MAIN THREAT VECTORS	Web
USER INTERACTION REQUIRED	Yes
DESCRIPTION	A vulnerability in some versions of Microsoft SharePoint could lead to remote code execution. The flaw lies in the Software Parses Specially Crafted Email Messages 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
MCAFEE 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	No Coverage Status
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 Office Improperly Discloses The Contents Of Its Memory Information Disclosure (CVE-2020-1445)

MTIS20-039-C

THREAT IDENTIFIER(S)	CVE-2020-1445
THREAT TYPE	Vulnerability
RISK ASSESSMENT	Medium
MAIN THREAT VECTORS	Web
USER INTERACTION REQUIRED	Yes
DESCRIPTION	A vulnerability in some versions of Microsoft Office could lead to information disclosure. The flaw lies in improperly discloses the contents of its memory. 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
MCAFEE 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	No Coverage Status
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 Word improperly handle objects in memory Remote Code Execution (CVE-2020-1446)

MTIS20-039-D

THREAT IDENTIFIER(S)	CVE-2020-1446
THREAT TYPE	Vulnerability
RISK ASSESSMENT	Medium
MAIN THREAT VECTORS	Web
USER INTERACTION REQUIRED	Yes
DESCRIPTION	A vulnerability in some versions of Microsoft Word 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
MCAFEE 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	No Coverage Status
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 Word improperly handle objects in memory Remote Code Execution (CVE-2020-1447)

MTIS20-039-E

THREAT IDENTIFIER(S)	CVE-2020-1447
THREAT TYPE	Vulnerability
RISK ASSESSMENT	Medium
MAIN THREAT VECTORS	Web
USER INTERACTION REQUIRED	Yes
DESCRIPTION	A vulnerability in some versions of Microsoft Word 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
MCAFEE 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	No Coverage Status
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 Word improperly handle objects in memory Remote Code Execution (CVE-2020-1448)

MTIS20-039-F

THREAT IDENTIFIER(S)	CVE-2020-1448

THREAT TYPE	Vulnerability
RISK ASSESSMENT	Medium
MAIN THREAT VECTORS	Web
USER INTERACTION REQUIRED	Yes
DESCRIPTION	A vulnerability in some versions of Microsoft Word 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
MCAFEE 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	No Coverage Status
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 Project Improperly Execute Macros Remote Code Execution (CVE-2020-1449)

MTIS20-039-G

THREAT IDENTIFIER(S)	CVE-2020-1449
THREAT TYPE	Vulnerability
RISK ASSESSMENT	Medium
MAIN THREAT VECTORS	Web
USER INTERACTION REQUIRED	Yes
DESCRIPTION	A vulnerability in some versions of Microsoft Project could lead to remote code execution. The flaw lies in improperly execute macros. 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
MCAFEE 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	No Coverage Status
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 SharePoint Server Improperly Sanitize a Specially Crafted Web Request Remote Code Execution (CVE-2020-1450)

MTIS20-039-H

THREAT IDENTIFIER(S)	CVE-2020-1450
THREAT TYPE	Vulnerability
RISK ASSESSMENT	Medium
MAIN THREAT VECTORS	Web
USER INTERACTION REQUIRED	No
DESCRIPTION	A vulnerability in some versions of Microsoft SharePoint Server could lead to remote code execution. The flaw lies in improperly sanitize a specially crafted web request. Successful exploitation by a remote attacker could result in the execution of arbitrary code.
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	No Coverage Status
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 SharePoint Server Improperly Sanitize a Specially Crafted Web Request Remote Code Execution (CVE-2020-1451)

MTIS20-039-I

THREAT IDENTIFIER(S)	CVE-2020-1451
THREAT TYPE	Vulnerability
RISK ASSESSMENT	Medium
MAIN THREAT VECTORS	Web
USER INTERACTION REQUIRED	No
DESCRIPTION	A vulnerability in some versions of Microsoft SharePoint Server could lead to remote code execution. The flaw lies in improperly sanitize a specially crafted web request. Successful exploitation by a remote attacker could result in the execution of arbitrary code.
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	No Coverage Status
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 SharePoint Server Improperly Sanitize a Specially Crafted Web Request Remote Code Execution (CVE-2020-1454)

MTIS20-039-J

THREAT IDENTIFIER(S)	CVE-2020-1454
THREAT TYPE	Vulnerability
RISK ASSESSMENT	Medium
MAIN THREAT VECTORS	Web
USER INTERACTION REQUIRED	No
DESCRIPTION	A vulnerability in some versions of Microsoft SharePoint Server could lead to remote code execution. The flaw lies in improperly sanitize a specially crafted web request. 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
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	No Coverage Status
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 SharePoint Server Improperly Sanitize a Specially Crafted Web Request Remote Code Execution (CVE-2020-1456)

MTIS20-039-K

THREAT IDENTIFIER(S)	CVE-2020-1456
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 SharePoint Server could lead to remote code execution. The flaw lies in improperly sanitize a specially crafted web request. 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
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	No Coverage Status
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 Office DLL Remote Code Execution (CVE-2020-1458)

MTIS20-039-L

THREAT IDENTIFIER(S)	CVE-2020-1458
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 Office could lead to remote code execution. The flaw lies in the DLL 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
MCAFEE 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	No Coverage Status
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 Defender MpSigStub.exe Privilege Escalation (CVE-2020-1461)

MTIS20-039-M

THREAT IDENTIFIER(S)	CVE-2020-1461

THREAT TYPE	Vulnerability
RISK ASSESSMENT	Medium
MAIN THREAT VECTORS	Web
USER INTERACTION REQUIRED	No
DESCRIPTION	A vulnerability in some versions of Microsoft Defender could lead to privilege escalation. The flaw lies in the MpSigStub.exe 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	No Coverage Status
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 Edge Skype Information Disclosure (CVE-2020-1462)

MTIS20-039-N

THREAT IDENTIFIER(S)	CVE-2020-1462
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 Edge could lead to information disclosure. The flaw lies in the Skype 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
MCAFEE 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 SharedStream Library Improperly Handles Objects in Memory Privilege Escalation (CVE-2020-1463)

MTIS20-039-O

THREAT IDENTIFIER(S)	CVE-2020-1463
THREAT TYPE	Vulnerability
RISK ASSESSMENT	Medium
MAIN THREAT VECTORS	Web
USER INTERACTION REQUIRED	No
DESCRIPTION	A vulnerability in some versions of Microsoft SharedStream Library could lead to privilege escalation. The flaw lies in improperly handle objects in memory. 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
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 OneDrive Privilege Escalation (CVE-2020-1465)

MTIS20-039-P

THREAT IDENTIFIER(S)	CVE-2020-1465
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 OneDrive 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	No Coverage Status
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 GDI Information Disclosure (CVE-2020-1468)

MTIS20-039-Q

THREAT IDENTIFIER(S)	CVE-2020-1468
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 GDI 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
MCAFEE 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	No Coverage Status
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 .NET Bond Denial of Service (CVE-2020-1469)

MTIS20-039-R

THREAT IDENTIFIER(S)	CVE-2020-1469
THREAT TYPE	Vulnerability
RISK ASSESSMENT	Medium
MAIN THREAT VECTORS	Web
USER INTERACTION REQUIRED	No
DESCRIPTION	A vulnerability in some versions of Microsoft .NET could lead to a denial of service. The flaw lies in the Bond 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
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	No Coverage Status
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 Visual Studio Remote Code Execution (CVE-2020-1481)

MTIS20-039-S

THREAT IDENTIFIER(S)	CVE-2020-1481
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 Visual Studio 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
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	No Coverage Status
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