EXECUTIVE SUMMARY

May 13, 2020 | MTIS20-023

Since the last McAfee® Labs Security Advisory (May 13), the following noteworthy event has taken place:

- Patches are available for multiple Microsoft security vulnerabilities

NEW THREAT OVERVIEW

(MSPT-May2020) Microsoft Excel Remote Code Execution (CVE-2020-0901)

MTIS20-023-A

IMPORTANCE: Medium
COVERED PRODUCTS:
UNDER ANALYSIS: Firewall Enterprise

Back to top

(MSPT-May2020) Microsoft Hyper-V Properly Validate Specific Malicious Data Denial of Service (CVE-2020-0909)

MTIS20-023-B

IMPORTANCE: Medium
COVERED PRODUCTS:
UNDER ANALYSIS: Firewall Enterprise

Back to top

(MSPT-May2020) Microsoft Windows GDI Information Disclosure (CVE-2020-0963)

MTIS20-023-C

IMPORTANCE: Medium
COVERED PRODUCTS:
UNDER ANALYSIS: Firewall Enterprise

Back to top

(MSPT-May2020) Microsoft Windows Wbengine Privilege Escalation (CVE-2020-1010)

MTIS20-023-D

IMPORTANCE: Medium
COVERED PRODUCTS:
UNDER ANALYSIS: Firewall Enterprise

Back to top

(MSPT-May2020) Microsoft Windows WER Privilege Escalation (CVE-2020-1021)

MTIS20-023-E

IMPORTANCE: Medium
COVERED PRODUCTS:
UNDER ANALYSIS: Firewall Enterprise

Back to top

(MSPT-May2020) Microsoft SharePoint Remote Code Execution (CVE-2020-1023)

MTIS20-023-F

IMPORTANCE: High
COVERED PRODUCTS:
UNDER ANALYSIS: Firewall Enterprise

Back to top

(MSPT-May2020) Microsoft SharePoint Remote Code Execution (CVE-2020-1024)

MTIS20-023-G

IMPORTANCE: High
COVERED PRODUCTS:
UNDER ANALYSIS: Firewall Enterprise

Back to top

(MSPT-May2020) Microsoft Windows Media Foundation Memory Corruption Vulnerability (CVE-2020-1028)

MTIS20-023-H

IMPORTANCE: High
COVERED PRODUCTS:
UNDER ANALYSIS: Firewall Enterprise

Back to top

(MSPT-May2020) Microsoft VBScript Improperly Handles Objects in Memory Remote Code Execution (CVE-2020-1035)

MTIS20-023-I

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

Back to top

(MSPT-May2020) Microsoft Edge Chakra Remote Code Execution (CVE-2020-1037)

MTIS20-023-J

IMPORTANCE: Medium
COVERED PRODUCTS:
UNDER ANALYSIS: Firewall Enterprise

Back to top

(MSPT-May2020) Microsoft Windows Print Spooler Privilege Escalation (CVE-2020-1048)

MTIS20-023-K

IMPORTANCE: Medium
COVERED PRODUCTS:
UNDER ANALYSIS: Firewall Enterprise

Back to top

(MSPT-May2020) Microsoft Windows Jet Database Engine Remote Code Execution (CVE-2020-1051)

MTIS20-023-L

IMPORTANCE: Medium
COVERED PRODUCTS:
UNDER ANALYSIS: Firewall Enterprise

Back to top

(MSPT-May2020) Microsoft Windows Kernel-Mode Privilege Escalation (CVE-2020-1054)

MTIS20-023-M

IMPORTANCE: Medium
COVERED PRODUCTS:
UNDER ANALYSIS: Firewall Enterprise

Back to top

(MSPT-May2020) Microsoft ADFS Improperly Sanitize User Inputs Spoofing (CVE-2020-1055)

MTIS20-023-N

IMPORTANCE: Medium
COVERED PRODUCTS:
UNDER ANALYSIS: Firewall Enterprise

Back to top

(MSPT-May2020) Microsoft Edge Improperly Enforce Cross-Domain Policies Privilege Escalation (CVE-2020-1056)

MTIS20-023-O

IMPORTANCE: Medium
COVERED PRODUCTS:
UNDER ANALYSIS: Firewall Enterprise

Back to top

(MSPT-May2020) Microsoft VBScript Improperly Handles Objects in Memory Remote Code Execution (CVE-2020-1058)

MTIS20-023-P

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

Back to top

(MSPT-May2020) Microsoft Edge Properly Parse HTTP Content Spoofing (CVE-2020-1059)

MTIS20-023-Q

IMPORTANCE: Medium
COVERED PRODUCTS:
UNDER ANALYSIS: Firewall Enterprise

Back to top

(MSPT-May2020) Microsoft VBScript Improperly Handles Objects in Memory Remote Code Execution (CVE-2020-1060)

MTIS20-023-R

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

Back to top

(MSPT-May2020) Microsoft VBScript Improperly Handles Objects in Memory Remote Code Execution (CVE-2020-1061)

MTIS20-023-S

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

Back to top

(MSPT-May2020) Microsoft Internet Explorer Improperly Access Objects in Memory Remote Code Execution (CVE-

2020-1062)
MTIS20-023-T

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

Back to top

(MSPT-May2020) Microsoft Dynamics 365 Improperly Sanitize a Specially Crafted Web Request Spoofing (CVE-2020-1063)

MTIS20-023-U

IMPORTANCE: Medium
COVERED PRODUCTS:
UNDER ANALYSIS: Firewall Enterprise

Back to top

(MSPT-May2020) Microsoft MSHTML Improperly Validates Input Remote Code Execution (CVE-2020-1064)

MTIS20-023-V

IMPORTANCE: High
COVERED PRODUCTS:
UNDER ANALYSIS: Firewall Enterprise

Back to top

(MSPT-May2020) Microsoft ChakraCore Improperly Handles Objects in Memory Remote Code Execution (CVE-2020-1065)

MTIS20-023-W

IMPORTANCE: High
COVERED PRODUCTS:
UNDER ANALYSIS: Firewall Enterprise

Back to top

(MSPT-May2020) Microsoft Windows .NET Framework Privilege Escalation (CVE-2020-1066)

MTIS20-023-X

IMPORTANCE: Medium
COVERED PRODUCTS:
UNDER ANALYSIS: Firewall Enterprise

Back to top

(MSPT-May2020) Microsoft Windows Improperly Handles Objects in Memory Remote Code Execution (CVE-2020-1067)

MTIS20-023-Y

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

Back to top

(MSPT-May2020) Microsoft Windows Privilege Escalation (CVE-2020-1068)

MTIS20-023-Z

IMPORTANCE: Medium
COVERED PRODUCTS:
UNDER ANALYSIS: Firewall Enterprise

Back to top

THREAT DETAILS

(MSPT-May2020) Microsoft Excel Remote Code Execution (CVE-2020-0901)

MTIS20-023-A

THREAT IDENTIFIER(S)	CVE-2020-0901
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 Excel 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 May 12, 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	Coverage not warranted
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-May2020) Microsoft Hyper-V Properly Validate Specific Malicious Data Denial of Service (CVE-2020-0909)

MTIS20-023-B

THREAT IDENTIFIER(S)	CVE-2020-0909
THREAT TYPE	Vulnerability
RISK ASSESSMENT	Medium
MAIN THREAT VECTORS	Web
USER INTERACTION REQUIRED	No
DESCRIPTION	A vulnerability in some versions of Microsoft Hyper-V could lead to a denial of service. The flaw lies in properly validate specific malicious data. 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 May 12, 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-May2020) Microsoft Windows GDI Information Disclosure (CVE-2020-0963)

MTIS20-023-C

THREAT IDENTIFIER(S)	CVE-2020-0963
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 May 12, 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	Coverage not warranted
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-May2020) Microsoft Windows Wbengine Privilege Escalation (CVE-2020-1010)

MTIS20-023-D

THREAT IDENTIFIER(S)	CVE-2020-1010
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 Wbengine 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 May 12, 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-May2020) Microsoft Windows WER Privilege Escalation (CVE-2020-1021)

MTIS20-023-E

THREAT IDENTIFIER(S)	CVE-2020-1021
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 WER 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 May 12, 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-May2020) Microsoft SharePoint Remote Code Execution (CVE-2020-1023)

MTIS20-023-F

THREAT IDENTIFIER(S)	CVE-2020-1023
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 SharePoint could lead to remote code execution. The flaw lies in fails to check the source markup. Successful exploitation by a remote attacker could result in the execution of arbitrary code.
IMPORTANCE	High. On May 12, 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-May2020) Microsoft SharePoint Remote Code Execution (CVE-2020-1024)

MTIS20-023-G

THREAT IDENTIFIER(S)	CVE-2020-1024
THREAT TYPE	Vulnerability
RISK ASSESSMENT	High
MAIN THREAT VECTORS	Web
USER INTERACTION REQUIRED	No
DESCRIPTION	A vulnerability in some versions of Microsoft SharePoint could lead to remote code execution. The flaw lies in fails to check the source markup. Successful exploitation by a remote attacker could result in the execution of arbitrary code.
IMPORTANCE	High. On May 12, 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-May2020) Microsoft Windows Media Foundation Memory Corruption Vulnerability (CVE-2020-1028)

MTIS20-023-H

THREAT IDENTIFIER(S)	CVE-2020-1028
THREAT TYPE	Vulnerability
RISK ASSESSMENT	High

MAIN THREAT VECTORS	Web
USER INTERACTION REQUIRED	Yes
DESCRIPTION	A vulnerability in some versions of Microsoft Windows could lead to memory corruption. The flaw lies in the Media Foundation component. Successful exploitation by a remote attacker could result in security bypass and affect the integrity. The exploit requires the user to open a vulnerable website, email or document.
IMPORTANCE	High. On May 12, 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	Coverage not warranted
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-May2020) Microsoft VBScript Improperly Handles Objects in Memory Remote Code Execution (CVE-2020-1035)

MTIS20-023-I

THREAT IDENTIFIER(S)	CVE-2020-1035
THREAT TYPE	Vulnerability
RISK ASSESSMENT	High
MAIN THREAT VECTORS	Locally logged-on user
USER INTERACTION REQUIRED	Yes
DESCRIPTION	A vulnerability in some versions of Microsoft VBScript could lead to remote code execution. The flaw lies in improperly handles objects in memory. Successful exploitation by a remote attacker could result in the execution of arbitrary code. The exploit requires the user to open a vulnerable website, email or document.
IMPORTANCE	High. On May 12, Microsoft released an update to address this vulnerability
MCAFEE PRODUCT COVERAGE	
DAT FILES	The 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	Coverage not warranted
VULNERABILITY MANAGER	An upcoming FSL/MVM content release will contain coverage for this issue.
WEB GATEWAY	The package includes a vulnerability check to assess if your systems are at risk
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-May2020) Microsoft Edge Chakra Remote Code Execution (CVE-2020-1037)

MTIS20-023-J

THREAT IDENTIFIER(S)	CVE-2020-1037
THREAT TYPE	Vulnerability
RISK ASSESSMENT	Medium
MAIN THREAT VECTORS	Web
USER INTERACTION REQUIRED	Yes
DESCRIPTION	A vulnerability in some versions of Microsoft Edge could lead to remote code execution. The flaw lies in the Chakra 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 May 12, 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	Coverage not warranted
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-May2020) Microsoft Windows Print Spooler Privilege Escalation (CVE-2020-1048)

MTIS20-023-K

THREAT IDENTIFIER(S)	CVE-2020-1048
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 Spooler 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 May 12, 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-May2020) Microsoft Windows Jet Database Engine Remote Code Execution (CVE-2020-1051)

MTIS20-023-L

THREAT IDENTIFIER(S)	CVE-2020-1051
THREAT TYPE	Vulnerability
RISK ASSESSMENT	Medium
MAIN THREAT VECTORS	Locally logged-on user
USER INTERACTION REQUIRED	Yes
DESCRIPTION	A vulnerability in some versions of Microsoft Windows could lead to remote code execution. The flaw lies in the Jet Database Engine component. Successful exploitation by a remote attacker could result in the execution of arbitrary code. The exploit requires the user to open a vulnerable website, email or document.
IMPORTANCE	Medium. On May 12, 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	Coverage not warranted
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-May2020) Microsoft Windows Kernel-Mode Privilege Escalation (CVE-2020-1054)

MTIS20-023-M

THREAT IDENTIFIER(S)	CVE-2020-1054
THREAT TYPE	Vulnerability
RISK ASSESSMENT	Medium
MAIN THREAT VECTORS	Web
USER INTERACTION REQUIRED	No
DESCRIPTION	A vulnerability in some versions of Microsoft Windows could lead to privilege escalation. The flaw lies in the Kernel-Mode 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 May 12, 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	Coverage not warranted
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-May2020) Microsoft ADFS Improperly Sanitize User Inputs Spoofing (CVE-2020-1055)

MTIS20-023-N

THREAT IDENTIFIER(S)	CVE-2020-1055
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 ADFS could lead to spoofing. The flaw lies in improperly sanitize user inputs. Successful exploitation by a remote attacker could result in spoofing
IMPORTANCE	Medium. On May 12, 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-May2020) Microsoft Edge Improperly Enforce Cross-Domain Policies Privilege Escalation (CVE-2020-1056)

MTIS20-023-O

THREAT IDENTIFIER(S)	CVE-2020-1056
THREAT TYPE	Vulnerability
RISK ASSESSMENT	Medium
MAIN THREAT VECTORS	Web
USER INTERACTION REQUIRED	Yes
DESCRIPTION	A vulnerability in some versions of Microsoft Edge could lead to privilege escalation. The flaw lies in improperly enforce cross-domain policies. Successful exploitation could allow a local user to gain elevated privileges. The exploit requires the user to open a

	vulnerable website, email or document.
IMPORTANCE	Medium. On May 12, 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	Coverage not warranted
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-May2020) Microsoft VBScript Improperly Handles Objects in Memory Remote Code Execution (CVE-2020-1058)

MTIS20-023-P

THREAT IDENTIFIER(S)	CVE-2020-1058
THREAT TYPE	Vulnerability
RISK ASSESSMENT	Medium
MAIN THREAT VECTORS	Web
USER INTERACTION REQUIRED	Yes
DESCRIPTION	A vulnerability in some versions of Microsoft VBScript could lead to remote code execution. The flaw lies in improperly handles 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 May 12, Microsoft released an update to address this vulnerability
MCAFEE PRODUCT COVERAGE	
DAT FILES	The 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	Coverage not warranted
VULNERABILITY MANAGER	An upcoming FSL/MVM content release will contain coverage for this issue.
WEB GATEWAY	The package includes a vulnerability check to assess if your systems are at risk
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-May2020) Microsoft Edge Properly Parse HTTP Content Spoofing (CVE-2020-1059)

MTIS20-023-Q

THREAT IDENTIFIER(S)	CVE-2020-1059
THREAT TYPE	Vulnerability
RISK ASSESSMENT	Medium
MAIN THREAT VECTORS	Web
USER INTERACTION REQUIRED	Yes
DESCRIPTION	A vulnerability in some versions of Microsoft Edge could lead to spoofing. The flaw lies in properly parse HTTP content. 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 May 12, 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	Coverage not warranted
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-May2020) Microsoft VBScript Improperly Handles Objects in Memory Remote Code Execution (CVE-2020-1060)

MTIS20-023-R

THREAT IDENTIFIER(S)	CVE-2020-1060
THREAT TYPE	Vulnerability
RISK ASSESSMENT	Medium
MAIN THREAT VECTORS	Web
USER INTERACTION REQUIRED	Yes
DESCRIPTION	A vulnerability in some versions of Microsoft VBScript could lead to remote code execution. The flaw lies in improperly handles 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 May 12, Microsoft released an update to address this vulnerability
MCAFEE PRODUCT COVERAGE	
DAT FILES	The 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	Coverage not warranted
VULNERABILITY MANAGER	An upcoming FSL/MVM content release will contain coverage for this issue.
WEB GATEWAY	The package includes a vulnerability check to assess if your systems are at risk
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-May2020) Microsoft VBScript Improperly Handles Objects in Memory Remote Code Execution (CVE-2020-1061)

MTIS20-023-S

THREAT IDENTIFIER(S)	CVE-2020-1061
THREAT TYPE	Vulnerability
RISK ASSESSMENT	Medium
MAIN THREAT VECTORS	Web
USER INTERACTION REQUIRED	Yes
DESCRIPTION	A vulnerability in some versions of Microsoft VBScript could lead to remote code execution. The flaw lies in improperly handles 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 May 12, 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	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-May2020) Microsoft Internet Explorer Improperly Access Objects in Memory Remote Code Execution (CVE-2020-1062)

MTIS20-023-T

THREAT IDENTIFIER(S)	CVE-2020-1062
THREAT TYPE	Vulnerability
RISK ASSESSMENT	High
MAIN THREAT VECTORS	Web
USER INTERACTION REQUIRED	Yes
DESCRIPTION	A vulnerability in some versions of Microsoft Internet Explorer could lead to remote code execution. The flaw lies in improperly access objects in memory. Successful exploitation by a remote attacker could result in the execution of arbitrary code. The exploit requires the user to open a vulnerable website, email or document.
IMPORTANCE	High. On May 12, Microsoft released an update to address this vulnerability
MCAFEE PRODUCT COVERAGE	
DAT FILES	The 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	Coverage not warranted

VULNERABILITY MANAGER	An upcoming FSL/MVM content release will contain coverage for this issue.
WEB GATEWAY	The package includes a vulnerability check to assess if your systems are at risk
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-May2020) Microsoft Dynamics 365 Improperly Sanitize a Specially Crafted Web Request Spoofing (CVE-2020-1063)

MTIS20-023-U

THREAT IDENTIFIER(S)	CVE-2020-1063
THREAT TYPE	Vulnerability
RISK ASSESSMENT	Medium
MAIN THREAT VECTORS	Web
USER INTERACTION REQUIRED	No
DESCRIPTION	A vulnerability in some versions of Microsoft Dynamics 365 could lead to spoofing. The flaw lies in improperly sanitize a specially crafted web request. Successful exploitation by a remote attacker could result in spoofing
IMPORTANCE	Medium. On May 12, 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-May2020) Microsoft MSHTML Improperly Validates Input Remote Code Execution (CVE-2020-1064)

MTIS20-023-V

THREAT IDENTIFIER(S)	CVE-2020-1064
THREAT TYPE	Vulnerability
RISK ASSESSMENT	High
MAIN THREAT VECTORS	Web
USER INTERACTION REQUIRED	Yes
DESCRIPTION	A vulnerability in some versions of Microsoft MSHTML could lead to remote code execution. The flaw lies in improperly validates input. Successful exploitation by a remote attacker could result in the execution of arbitrary code. The exploit requires the user to open a vulnerable website, email or document.

IMPORTANCE	High. On May 12, 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	Coverage not warranted
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-May2020) Microsoft ChakraCore Improperly Handles Objects in Memory Remote Code Execution (CVE-2020-1065)

MTIS20-023-W

THREAT IDENTIFIER(S)	CVE-2020-1065
THREAT TYPE	Vulnerability
RISK ASSESSMENT	High
MAIN THREAT VECTORS	Web
USER INTERACTION REQUIRED	Yes
DESCRIPTION	A vulnerability in some versions of Microsoft ChakraCore could lead to remote code execution. The flaw lies in improperly handles objects in memory. Successful exploitation by a remote attacker could result in the execution of arbitrary code. The exploit requires the user to open a vulnerable website, email or document.
IMPORTANCE	High. On May 12, 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	Coverage not warranted
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-May2020) Microsoft Windows .NET Framework Privilege Escalation (CVE-2020-1066)

MTIS20-023-X

THREAT IDENTIFIER(S)	CVE-2020-1066

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 .NET Framework component. Successful exploitation could allow a local user to gain elevated privileges. The exploit requires the attacker to have valid credentials to the vulnerable system.
IMPORTANCE	Medium. On May 12, 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-May2020) Microsoft Windows Improperly Handles Objects in Memory Remote Code Execution (CVE-2020-1067)

MTIS20-023-Y

THREAT IDENTIFIER(S)	CVE-2020-1067
THREAT TYPE	Vulnerability
RISK ASSESSMENT	Medium
MAIN THREAT VECTORS	Locally logged-on user
USER INTERACTION REQUIRED	Yes
DESCRIPTION	A vulnerability in some versions of Microsoft Windows could lead to remote code execution. The flaw lies in improperly handles 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 May 12, Microsoft released an update to address this vulnerability
MCAFEE PRODUCT COVERAGE	
DAT FILES	The 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	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-May2020) Microsoft Windows Privilege Escalation (CVE-2020-1068)

MTIS20-023-Z

THREAT IDENTIFIER(S)	CVE-2020-1068
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 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 May 12, 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

For McAfee Technical Support, click here.

For Multi-National Phone Support, click here.

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

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