EXECUTIVE SUMMARY

November 12, 2019 | MTIS19-052

Since the last McAfee® Labs Security Advisory (October 16), the following noteworthy event has taken place:

- Patches are available for multiple Microsoft security updates.

NEW THREAT OVERVIEW

(MSPT-Nov2019) Microsoft Hyper-V Network Switch Denial of Service (CVE-2019-0712)

MTIS19-052-A

IMPORTANCE: Medium
COVERED PRODUCTS:
UNDER ANALYSIS:

Back to top

(MSPT-Nov2019) Microsoft Hyper-V Network Switch Remote Code Execution (CVE-2019-0719)

MTIS19-052-B

IMPORTANCE: High
COVERED PRODUCTS:
UNDER ANALYSIS:

Back to top

(MSPT-Nov2019) Microsoft Hyper-V Network Switch Remote Code Execution (CVE-2019-0721)

MTIS19-052-C

IMPORTANCE: High
COVERED PRODUCTS:
UNDER ANALYSIS:

Back to top

(MSPT-Nov2019) Microsoft Hyper-V Network Switch Denial of Service (CVE-2019-1309)

MTIS19-052-D

IMPORTANCE: Medium
COVERED PRODUCTS:
UNDER ANALYSIS:

Back to top

(MSPT-Nov2019) Microsoft Hyper-V Network Switch Denial of Service (CVE-2019-1310)

MTIS19-052-E

IMPORTANCE: Medium
COVERED PRODUCTS:
UNDER ANALYSIS:

Back to top

(MSPT-Nov2019) Microsoft TCP/IP Information Disclosure (CVE-2019-1324)

MTIS19-052-F

IMPORTANCE: Medium
COVERED PRODUCTS:
UNDER ANALYSIS:

Back to top

(MSPT-Nov2019) Microsoft Open Enclave SDK Improperly Handle Objects in Memory Information Disclosure (CVE-2019-1370)

MTIS19-052-G

IMPORTANCE: Medium
COVERED PRODUCTS:
UNDER ANALYSIS:

Back to top

(MSPT-Nov2019) Microsoft Exchange PowerShell Remote Code Execution (CVE-2019-1373)

MTIS19-052-H

IMPORTANCE: High
COVERED PRODUCTS:
UNDER ANALYSIS:

Back to top

(MSPT-Nov2019) Microsoft WER Information Disclosure (CVE-2019-1374)

MTIS19-052-I

IMPORTANCE: Medium
COVERED PRODUCTS:
UNDER ANALYSIS:

Back to top

(MSPT-Nov2019) Microsoft Data Sharing Service Privilege Escalation (CVE-2019-1379)

MTIS19-052-J

IMPORTANCE: Medium
COVERED PRODUCTS:
UNDER ANALYSIS:

Back to top

(MSPT-Nov2019) Microsoft splwow64.exe Improperly Handles Calls Privilege Escalation (CVE-2019-1380)

MTIS19-052-K

IMPORTANCE: Medium
COVERED PRODUCTS:
UNDER ANALYSIS:

Back to top

(MSPT-Nov2019) Microsoft Servicing Stack Information Disclosure (CVE-2019-1381)

MTIS19-052-L

IMPORTANCE: Medium
COVERED PRODUCTS:
UNDER ANALYSIS:

Back to top

(MSPT-Nov2019) Microsoft ActiveX Installer Improper Authenticate Files Privilege Escalation (CVE-2019-1382)
MTIS19-052-M

IMPORTANCE: Medium
COVERED PRODUCTS:
UNDER ANALYSIS:

Back to top

(MSPT-Nov2019) Microsoft Data Sharing Service Privilege Escalation (CVE-2019-1383)
MTIS19-052-N

IMPORTANCE: Medium
COVERED PRODUCTS:
UNDER ANALYSIS:

Back to top

(MSPT-Nov2019) Microsoft NETLOGON Obtain The Session Key Remote Code Execution (CVE-2019-1384)
MTIS19-052-O

IMPORTANCE: Medium
COVERED PRODUCTS:
UNDER ANALYSIS:

Back to top

(MSPT-Nov2019) Microsoft AppX Deployment Extensions Privilege Escalation (CVE-2019-1385)
MTIS19-052-P

IMPORTANCE: Medium
COVERED PRODUCTS:
UNDER ANALYSIS:

Back to top

(MSPT-Nov2019) Microsoft Windows Certificate Dialog Privilege Escalation (CVE-2019-1388)
MTIS19-052-Q

IMPORTANCE: Medium
COVERED PRODUCTS:
UNDER ANALYSIS:

Back to top

(MSPT-Nov2019) Microsoft Windows Hyper-V Remote Code Execution (CVE-2019-1389)
MTIS19-052-R

IMPORTANCE: High
COVERED PRODUCTS:
UNDER ANALYSIS:

Back to top

(MSPT-Nov2019) Microsoft VBScript Improperly Handles Objects In Memory Remote Code Execution (CVE-2019-1390)
MTIS19-052-S

IMPORTANCE: High
COVERED PRODUCTS:
UNDER ANALYSIS:

Back to top

(MSPT-Nov2019) Microsoft Windows Improperly Handles Objects In Memory Denial of Service (CVE-2019-1391)
MTIS19-052-T

IMPORTANCE: Medium

COVERED PRODUCTS:
UNDER ANALYSIS:

Back to top

(MSPT-Nov2019) Microsoft Windows Kernel Privilege Escalation (CVE-2019-1392)
MTIS19-052-U

IMPORTANCE: Medium
COVERED PRODUCTS:
UNDER ANALYSIS:

Back to top

(MSPT-Nov2019) Microsoft Windows Win32k Privilege Escalation (CVE-2019-1393)
MTIS19-052-V

IMPORTANCE: Medium
COVERED PRODUCTS:
UNDER ANALYSIS:

Back to top

(MSPT-Nov2019) Microsoft Windows Win32k Privilege Escalation (CVE-2019-1394)
MTIS19-052-W

IMPORTANCE: Medium
COVERED PRODUCTS:
UNDER ANALYSIS:

Back to top

(MSPT-Nov2019) Microsoft Windows Win32k Privilege Escalation (CVE-2019-1395)
MTIS19-052-X

IMPORTANCE: Medium
COVERED PRODUCTS:
UNDER ANALYSIS:

Back to top

(MSPT-Nov2019) Microsoft Windows Win32k Privilege Escalation (CVE-2019-1396)
MTIS19-052-Y

IMPORTANCE: Medium
COVERED PRODUCTS:
UNDER ANALYSIS:

Back to top

(MSPT-Nov2019) Microsoft Windows Hyper-V Remote Code Execution (CVE-2019-1397)
MTIS19-052-Z

IMPORTANCE: High
COVERED PRODUCTS:
UNDER ANALYSIS:

Back to top

THREAT DETAILS

(MSPT-Nov2019) Microsoft Hyper-V Network Switch Denial of Service (CVE-2019-0712)
MTIS19-052-A

THREAT IDENTIFIER(S)	CVE-2019-0712
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 Hyper-V could lead to a denial of service. The flaw lies in the Network Switch 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 November 12, Microsoft released an update to address this vulnerability
MCAFEE PRODUCT COVERAGE	
DAT FILES	No Coverage Status
VIRUS SCAN ENTERPRISE SCAN BOP	No Coverage Status
HOST IPS	No Coverage Status
NETWORK SECURITY PLATFORM	No Coverage Status
VULNERABILITY MANAGER	No Coverage Status
WEB GATEWAY	No Coverage Status
REMEDIATION MANAGER	No Coverage Status
POLICY AUDITOR	No Coverage Status
NETWORK ACCESS CONTROL	No Coverage Status
FIREWALL ENTERPRISE	No Coverage Status
APPLICATION CONTROL	No Coverage Status
DATABASE ACTIVITY MONITORING	No Coverage Status
VULNERABILITY MANAGER FOR DATABASES	No Coverage Status
ADDITIONAL INFORMATION	Microsoft: Security Update Summary

Back to top

(MSPT-Nov2019) Microsoft Hyper-V Network Switch Remote Code Execution (CVE-2019-0719)

MTIS19-052-B

THREAT IDENTIFIER(S)	CVE-2019-0719
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 Hyper-V could lead to remote code execution. The flaw lies in the Network Switch component. Successful exploitation by a remote attacker could result in the execution of arbitrary code. The exploit requires the attacker to have valid credentials to the vulnerable system.
IMPORTANCE	High. On November 12, Microsoft released an update to address this vulnerability
MCAFEE PRODUCT COVERAGE	
DAT FILES	No Coverage Status
VIRUS SCAN ENTERPRISE SCAN BOP	No Coverage Status
HOST IPS	No Coverage Status
NETWORK SECURITY PLATFORM	No Coverage Status
VULNERABILITY MANAGER	No Coverage Status
WEB GATEWAY	No Coverage Status
REMEDIATION MANAGER	No Coverage Status
POLICY AUDITOR	No Coverage Status
NETWORK ACCESS CONTROL	No Coverage Status
FIREWALL ENTERPRISE	No Coverage Status
APPLICATION CONTROL	No Coverage Status
DATABASE ACTIVITY MONITORING	No Coverage Status
VULNERABILITY MANAGER FOR DATABASES	No Coverage Status
ADDITIONAL INFORMATION	Microsoft: Security Update Summary

Back to top

(MSPT-Nov2019) Microsoft Hyper-V Network Switch Remote Code Execution (CVE-2019-0721)

MTIS19-052-C

THREAT IDENTIFIER(S)	CVE-2019-0721
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 Hyper-V could lead to remote code execution. The flaw lies in the Network Switch component. Successful exploitation by a remote attacker could result in the execution of arbitrary code. The exploit requires the attacker to have valid credentials to the vulnerable system.
IMPORTANCE	High. On November 12, Microsoft released an update to address this vulnerability
MCAFEE PRODUCT COVERAGE	
DAT FILES	No Coverage Status
VIRUS SCAN ENTERPRISE SCAN BOP	No Coverage Status
HOST IPS	No Coverage Status
NETWORK SECURITY PLATFORM	No Coverage Status
VULNERABILITY MANAGER	No Coverage Status
WEB GATEWAY	No Coverage Status
REMEDIATION MANAGER	No Coverage Status
POLICY AUDITOR	No Coverage Status
NETWORK ACCESS CONTROL	No Coverage Status
FIREWALL ENTERPRISE	No Coverage Status
APPLICATION CONTROL	No Coverage Status
DATABASE ACTIVITY MONITORING	No Coverage Status
VULNERABILITY MANAGER FOR DATABASES	No Coverage Status
ADDITIONAL INFORMATION	Microsoft: Security Update Summary

Back to top

(MSPT-Nov2019) Microsoft Hyper-V Network Switch Denial of Service (CVE-2019-1309)

MTIS19-052-D

THREAT IDENTIFIER(S)	CVE-2019-1309
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 the Network Switch 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 November 12, Microsoft released an update to address this vulnerability
MCAFEE PRODUCT COVERAGE	
DAT FILES	No Coverage Status
VIRUS SCAN ENTERPRISE SCAN BOP	No Coverage Status
HOST IPS	No Coverage Status
NETWORK SECURITY PLATFORM	No Coverage Status
VULNERABILITY MANAGER	No Coverage Status
WEB GATEWAY	No Coverage Status
REMEDIATION MANAGER	No Coverage Status
POLICY AUDITOR	No Coverage Status
NETWORK ACCESS CONTROL	No Coverage Status

FIREWALL ENTERPRISE	No Coverage Status
APPLICATION CONTROL	No Coverage Status
DATABASE ACTIVITY MONITORING	No Coverage Status
VULNERABILITY MANAGER FOR DATABASES	No Coverage Status
ADDITIONAL INFORMATION	Microsoft: Security Update Summary

Back to top

(MSPT-Nov2019) Microsoft Hyper-V Network Switch Denial of Service (CVE-2019-1310)

MTIS19-052-E

THREAT IDENTIFIER(S)	CVE-2019-1310
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 Hyper-V could lead to a denial of service. The flaw lies in the Network Switch 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 November 12, Microsoft released an update to address this vulnerability
MCAFEE PRODUCT COVERAGE	
DAT FILES	No Coverage Status
VIRUS SCAN ENTERPRISE SCAN BOP	No Coverage Status
HOST IPS	No Coverage Status
NETWORK SECURITY PLATFORM	No Coverage Status
VULNERABILITY MANAGER	No Coverage Status
WEB GATEWAY	No Coverage Status
REMEDIATION MANAGER	No Coverage Status
POLICY AUDITOR	No Coverage Status
NETWORK ACCESS CONTROL	No Coverage Status
FIREWALL ENTERPRISE	No Coverage Status
APPLICATION CONTROL	No Coverage Status
DATABASE ACTIVITY MONITORING	No Coverage Status
VULNERABILITY MANAGER FOR DATABASES	No Coverage Status
ADDITIONAL INFORMATION	Microsoft: Security Update Summary

Back to top

(MSPT-Nov2019) Microsoft TCP/IP Information Disclosure (CVE-2019-1324)

MTIS19-052-F

THREAT IDENTIFIER(S)	CVE-2019-1324
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 TCP/IP could lead to information disclosure. The flaw lies in the improper handling of fragmented IP packets. Successful exploitation by an attacker could result in the disclosure of sensitive information.
IMPORTANCE	Medium. On November 12, Microsoft released an update to address this vulnerability
MCAFEE PRODUCT COVERAGE	
DAT FILES	No Coverage Status
VIRUS SCAN ENTERPRISE SCAN BOP	No Coverage Status
HOST IPS	No Coverage Status

NETWORK SECURITY PLATFORM	No Coverage Status
VULNERABILITY MANAGER	No Coverage Status
WEB GATEWAY	No Coverage Status
REMEDIATION MANAGER	No Coverage Status
POLICY AUDITOR	No Coverage Status
NETWORK ACCESS CONTROL	No Coverage Status
FIREWALL ENTERPRISE	No Coverage Status
APPLICATION CONTROL	No Coverage Status
DATABASE ACTIVITY MONITORING	No Coverage Status
VULNERABILITY MANAGER FOR DATABASES	No Coverage Status
ADDITIONAL INFORMATION	Microsoft: Security Update Summary

Back to top

(MSPT-Nov2019) Microsoft Open Enclave SDK Improperly Handle Objects in Memory Information Disclosure (CVE-2019-1370)

MTIS19-052-G

THREAT IDENTIFIER(S)	CVE-2019-1370
THREAT TYPE	Vulnerability
RISK ASSESSMENT	Medium
MAIN THREAT VECTORS	Web
USER INTERACTION REQUIRED	Yes
DESCRIPTION	A vulnerability in some versions of Microsoft Open Enclave SDK could lead to information disclosure. The flaw lies in the improperly handle objects in 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 November 12, Microsoft released an update to address this vulnerability
MCAFEE PRODUCT COVERAGE	
DAT FILES	No Coverage Status
VIRUS SCAN ENTERPRISE SCAN BOP	No Coverage Status
HOST IPS	No Coverage Status
NETWORK SECURITY PLATFORM	No Coverage Status
VULNERABILITY MANAGER	No Coverage Status
WEB GATEWAY	No Coverage Status
REMEDIATION MANAGER	No Coverage Status
POLICY AUDITOR	No Coverage Status
NETWORK ACCESS CONTROL	No Coverage Status
FIREWALL ENTERPRISE	No Coverage Status
APPLICATION CONTROL	No Coverage Status
DATABASE ACTIVITY MONITORING	No Coverage Status
VULNERABILITY MANAGER FOR DATABASES	No Coverage Status
ADDITIONAL INFORMATION	Microsoft: Security Update Summary

Back to top

(MSPT-Nov2019) Microsoft Exchange PowerShell Remote Code Execution (CVE-2019-1373)

MTIS19-052-H

THREAT IDENTIFIER(S)	CVE-2019-1373
THREAT TYPE	Vulnerability
RISK ASSESSMENT	High
MAIN THREAT VECTORS	Web
USER INTERACTION REQUIRED	No

DESCRIPTION	A vulnerability in some versions of Microsoft Exchange could lead to remote code execution. The flaw lies in the PowerShell component. Successful exploitation by a remote attacker could result in the execution of arbitrary code.
IMPORTANCE	High. On November 12, Microsoft released an update to address this vulnerability
MCAFEE PRODUCT COVERAGE	
DAT FILES	No Coverage Status
VIRUS SCAN ENTERPRISE SCAN BOP	No Coverage Status
HOST IPS	No Coverage Status
NETWORK SECURITY PLATFORM	No Coverage Status
VULNERABILITY MANAGER	No Coverage Status
WEB GATEWAY	No Coverage Status
REMEDIATION MANAGER	No Coverage Status
POLICY AUDITOR	No Coverage Status
NETWORK ACCESS CONTROL	No Coverage Status
FIREWALL ENTERPRISE	No Coverage Status
APPLICATION CONTROL	No Coverage Status
DATABASE ACTIVITY MONITORING	No Coverage Status
VULNERABILITY MANAGER FOR DATABASES	No Coverage Status
ADDITIONAL INFORMATION	Microsoft: Security Update Summary

Back to top

(MSPT-Nov2019) Microsoft WER Information Disclosure (CVE-2019-1374)

MTIS19-052-I

THREAT IDENTIFIER(S)	CVE-2019-1374
THREAT TYPE	Vulnerability
RISK ASSESSMENT	Medium
MAIN THREAT VECTORS	Web
USER INTERACTION REQUIRED	No
DESCRIPTION	A vulnerability in some versions of Microsoft WER could lead to information disclosure. The flaw lies in the improper handling objects in memory. Successful exploitation by an attacker could result in the disclosure of sensitive information. The exploit requires the attacker to have valid credentials to the vulnerable system.
IMPORTANCE	Medium. On November 12, Microsoft released an update to address this vulnerability
MCAFEE PRODUCT COVERAGE	
DAT FILES	No Coverage Status
VIRUS SCAN ENTERPRISE SCAN BOP	No Coverage Status
HOST IPS	No Coverage Status
NETWORK SECURITY PLATFORM	No Coverage Status
VULNERABILITY MANAGER	No Coverage Status
WEB GATEWAY	No Coverage Status
REMEDIATION MANAGER	No Coverage Status
POLICY AUDITOR	No Coverage Status
NETWORK ACCESS CONTROL	No Coverage Status
FIREWALL ENTERPRISE	No Coverage Status
APPLICATION CONTROL	No Coverage Status
DATABASE ACTIVITY MONITORING	No Coverage Status
VULNERABILITY MANAGER FOR DATABASES	No Coverage Status
ADDITIONAL INFORMATION	Microsoft: Security Update Summary

Back to top

(MSPT-Nov2019) Microsoft Data Sharing Service Privilege Escalation (CVE-2019-1379)

MTIS19-052-J

THREAT IDENTIFIER(S)	CVE-2019-1379
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 Data Sharing Service could lead to privilege escalation. The flaw lies in the improper handling of file operations. 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 November 12, Microsoft released an update to address this vulnerability
MCAFEE PRODUCT COVERAGE	
DAT FILES	No Coverage Status
VIRUS SCAN ENTERPRISE SCAN BOP	No Coverage Status
HOST IPS	No Coverage Status
NETWORK SECURITY PLATFORM	No Coverage Status
VULNERABILITY MANAGER	No Coverage Status
WEB GATEWAY	No Coverage Status
REMEDIATION MANAGER	No Coverage Status
POLICY AUDITOR	No Coverage Status
NETWORK ACCESS CONTROL	No Coverage Status
FIREWALL ENTERPRISE	No Coverage Status
APPLICATION CONTROL	No Coverage Status
DATABASE ACTIVITY MONITORING	No Coverage Status
VULNERABILITY MANAGER FOR DATABASES	No Coverage Status
ADDITIONAL INFORMATION	Microsoft: Security Update Summary

Back to top

(MSPT-Nov2019) Microsoft splwow64.exe Improperly Handles Calls Privilege Escalation (CVE-2019-1380)

MTIS19-052-K

THREAT IDENTIFIER(S)	CVE-2019-1380
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 splwow64.exe could lead to privilege escalation. The flaw lies in the improperly handles calls. Successful exploitation could allow a local user to gain elevated privileges.
IMPORTANCE	Medium. On November 12, Microsoft released an update to address this vulnerability
MCAFEE PRODUCT COVERAGE	
DAT FILES	No Coverage Status
VIRUS SCAN ENTERPRISE SCAN BOP	No Coverage Status
HOST IPS	No Coverage Status
NETWORK SECURITY PLATFORM	No Coverage Status
VULNERABILITY MANAGER	No Coverage Status
WEB GATEWAY	No Coverage Status
REMEDIATION MANAGER	No Coverage Status
POLICY AUDITOR	No Coverage Status
NETWORK ACCESS CONTROL	No Coverage Status
FIREWALL ENTERPRISE	No Coverage Status
APPLICATION CONTROL	No Coverage Status
DATABASE ACTIVITY MONITORING	No Coverage Status

VULNERABILITY MANAGER FOR DATABASES	No Coverage Status
ADDITIONAL INFORMATION	Microsoft: Security Update Summary

Back to top

(MSPT-Nov2019) Microsoft Servicing Stack Information Disclosure (CVE-2019-1381)

MTIS19-052-L

THREAT IDENTIFIER(S)	CVE-2019-1381
THREAT TYPE	Vulnerability
RISK ASSESSMENT	Medium
MAIN THREAT VECTORS	Web
USER INTERACTION REQUIRED	No
DESCRIPTION	A vulnerability in some versions of Microsoft Servicing Stack could lead to information disclosure. The flaw lies in the Servicing Stack allows access to unprivileged file locations. Successful exploitation by an attacker could result in the disclosure of sensitive information. The exploit requires the attacker to have valid credentials to the vulnerable system.
IMPORTANCE	Medium. On November 12, Microsoft released an update to address this vulnerability
MCAFEE PRODUCT COVERAGE	
DAT FILES	No Coverage Status
VIRUS SCAN ENTERPRISE SCAN BOP	No Coverage Status
HOST IPS	No Coverage Status
NETWORK SECURITY PLATFORM	No Coverage Status
VULNERABILITY MANAGER	No Coverage Status
WEB GATEWAY	No Coverage Status
REMEDIATION MANAGER	No Coverage Status
POLICY AUDITOR	No Coverage Status
NETWORK ACCESS CONTROL	No Coverage Status
FIREWALL ENTERPRISE	No Coverage Status
APPLICATION CONTROL	No Coverage Status
DATABASE ACTIVITY MONITORING	No Coverage Status
VULNERABILITY MANAGER FOR DATABASES	No Coverage Status
ADDITIONAL INFORMATION	Microsoft: Security Update Summary

Back to top

(MSPT-Nov2019) Microsoft ActiveX Installer Improper Authenticate Files Privilege Escalation (CVE-2019-1382)

MTIS19-052-M

THREAT IDENTIFIER(S)	CVE-2019-1382
THREAT TYPE	Vulnerability
RISK ASSESSMENT	Medium
MAIN THREAT VECTORS	Locally logged-on user
USER INTERACTION REQUIRED	No
DESCRIPTION	A vulnerability in some versions of Microsoft ActiveX Installer could lead to privilege escalation. The flaw lies in the improper authenticate files. 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 November 12, Microsoft released an update to address this vulnerability
MCAFEE PRODUCT COVERAGE	
DAT FILES	No Coverage Status
VIRUS SCAN ENTERPRISE SCAN BOP	No Coverage Status
HOST IPS	No Coverage Status
NETWORK SECURITY PLATFORM	No Coverage Status
VULNERABILITY MANAGER	No Coverage Status

WEB GATEWAY	No Coverage Status
REMEDIATION MANAGER	No Coverage Status
POLICY AUDITOR	No Coverage Status
NETWORK ACCESS CONTROL	No Coverage Status
FIREWALL ENTERPRISE	No Coverage Status
APPLICATION CONTROL	No Coverage Status
DATABASE ACTIVITY MONITORING	No Coverage Status
VULNERABILITY MANAGER FOR DATABASES	No Coverage Status
ADDITIONAL INFORMATION	Microsoft: Security Update Summary

Back to top

(MSPT-Nov2019) Microsoft Data Sharing Service Privilege Escalation (CVE-2019-1383)

MTIS19-052-N

THREAT IDENTIFIER(S)	CVE-2019-1383
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 Data Sharing Service could lead to privilege escalation. The flaw lies in the improper handling of file operations. 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 November 12, Microsoft released an update to address this vulnerability
MCAFEE PRODUCT COVERAGE	
DAT FILES	No Coverage Status
VIRUS SCAN ENTERPRISE SCAN BOP	No Coverage Status
HOST IPS	No Coverage Status
NETWORK SECURITY PLATFORM	No Coverage Status
VULNERABILITY MANAGER	No Coverage Status
WEB GATEWAY	No Coverage Status
REMEDIATION MANAGER	No Coverage Status
POLICY AUDITOR	No Coverage Status
NETWORK ACCESS CONTROL	No Coverage Status
FIREWALL ENTERPRISE	No Coverage Status
APPLICATION CONTROL	No Coverage Status
DATABASE ACTIVITY MONITORING	No Coverage Status
VULNERABILITY MANAGER FOR DATABASES	No Coverage Status
ADDITIONAL INFORMATION	Microsoft: Security Update Summary

Back to top

(MSPT-Nov2019) Microsoft NETLOGON Obtain The Session Key Remote Code Execution (CVE-2019-1384)

MTIS19-052-O

THREAT IDENTIFIER(S)	CVE-2019-1384
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 NETLOGON could lead to remote code execution. The flaw lies in obtain the session key. 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 November 12, Microsoft released an update to address this vulnerability

MCAFEE PRODUCT COVERAGE	
DAT FILES	No Coverage Status
VIRUS SCAN ENTERPRISE SCAN BOP	No Coverage Status
HOST IPS	No Coverage Status
NETWORK SECURITY PLATFORM	No Coverage Status
VULNERABILITY MANAGER	No Coverage Status
WEB GATEWAY	No Coverage Status
REMEDIATION MANAGER	No Coverage Status
POLICY AUDITOR	No Coverage Status
NETWORK ACCESS CONTROL	No Coverage Status
FIREWALL ENTERPRISE	No Coverage Status
APPLICATION CONTROL	No Coverage Status
DATABASE ACTIVITY MONITORING	No Coverage Status
VULNERABILITY MANAGER FOR DATABASES	No Coverage Status
ADDITIONAL INFORMATION	Microsoft: Security Update Summary

Back to top

(MSPT-Nov2019) Microsoft AppX Deployment Extensions Privilege Escalation (CVE-2019-1385)

MTIS19-052-P

THREAT IDENTIFIER(S)	CVE-2019-1385
THREAT TYPE	Vulnerability
RISK ASSESSMENT	Medium
MAIN THREAT VECTORS	Web
USER INTERACTION REQUIRED	No
DESCRIPTION	A vulnerability in some versions of Microsoft AppX could lead to privilege escalation. The flaw lies in the Deployment Extensions 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 November 12, Microsoft released an update to address this vulnerability
MCAFEE PRODUCT COVERAGE	
DAT FILES	No Coverage Status
VIRUS SCAN ENTERPRISE SCAN BOP	No Coverage Status
HOST IPS	No Coverage Status
NETWORK SECURITY PLATFORM	No Coverage Status
VULNERABILITY MANAGER	No Coverage Status
WEB GATEWAY	No Coverage Status
REMEDIATION MANAGER	No Coverage Status
POLICY AUDITOR	No Coverage Status
NETWORK ACCESS CONTROL	No Coverage Status
FIREWALL ENTERPRISE	No Coverage Status
APPLICATION CONTROL	No Coverage Status
DATABASE ACTIVITY MONITORING	No Coverage Status
VULNERABILITY MANAGER FOR DATABASES	No Coverage Status
ADDITIONAL INFORMATION	Microsoft: Security Update Summary

Back to top

(MSPT-Nov2019) Microsoft Windows Certificate Dialog Privilege Escalation (CVE-2019-1388)

MTIS19-052-Q

THREAT IDENTIFIER(S)	CVE-2019-1388
THREAT TYPE	Vulnerability

RISK ASSESSMENT	Medium
MAIN THREAT VECTORS	Locally logged-on user
USER INTERACTION REQUIRED	No
DESCRIPTION	A vulnerability in some versions of Microsoft Windows could lead to privilege escalation. The flaw lies in the Certificate Dialog 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 November 12, Microsoft released an update to address this vulnerability
MCAFEE PRODUCT COVERAGE	
DAT FILES	No Coverage Status
VIRUS SCAN ENTERPRISE SCAN BOP	No Coverage Status
HOST IPS	No Coverage Status
NETWORK SECURITY PLATFORM	No Coverage Status
VULNERABILITY MANAGER	No Coverage Status
WEB GATEWAY	No Coverage Status
REMEDIATION MANAGER	No Coverage Status
POLICY AUDITOR	No Coverage Status
NETWORK ACCESS CONTROL	No Coverage Status
FIREWALL ENTERPRISE	No Coverage Status
APPLICATION CONTROL	No Coverage Status
DATABASE ACTIVITY MONITORING	No Coverage Status
VULNERABILITY MANAGER FOR DATABASES	No Coverage Status
ADDITIONAL INFORMATION	Microsoft: Security Update Summary

Back to top

(MSPT-Nov2019) Microsoft Windows Hyper-V Remote Code Execution (CVE-2019-1389)

MTIS19-052-R

THREAT IDENTIFIER(S)	CVE-2019-1389
THREAT TYPE	Vulnerability
RISK ASSESSMENT	High
MAIN THREAT VECTORS	Locally logged-on user
USER INTERACTION REQUIRED	No
DESCRIPTION	A vulnerability in some versions of Microsoft Windows could lead to remote code execution. The flaw lies in the Hyper-V component. Successful exploitation by a remote attacker could result in the execution of arbitrary code. The exploit requires the attacker to have valid credentials to the vulnerable system.
IMPORTANCE	High. On November 12, Microsoft released an update to address this vulnerability
MCAFEE PRODUCT COVERAGE	
DAT FILES	No Coverage Status
VIRUS SCAN ENTERPRISE SCAN BOP	No Coverage Status
HOST IPS	No Coverage Status
NETWORK SECURITY PLATFORM	No Coverage Status
VULNERABILITY MANAGER	No Coverage Status
WEB GATEWAY	No Coverage Status
REMEDIATION MANAGER	No Coverage Status
POLICY AUDITOR	No Coverage Status
NETWORK ACCESS CONTROL	No Coverage Status
FIREWALL ENTERPRISE	No Coverage Status
APPLICATION CONTROL	No Coverage Status
DATABASE ACTIVITY MONITORING	No Coverage Status
VULNERABILITY MANAGER FOR DATABASES	No Coverage Status
ADDITIONAL INFORMATION	Microsoft: Security Update Summary

Back to top

(MSPT-Nov2019) Microsoft VBScript Improperly Handles Objects In Memory Remote Code Execution (CVE-2019-1390)

MTIS19-052-S

THREAT IDENTIFIER(S)	CVE-2019-1390
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 the 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 November 12, Microsoft released an update to address this vulnerability
MCAFEE PRODUCT COVERAGE	
DAT FILES	No Coverage Status
VIRUS SCAN ENTERPRISE SCAN BOP	No Coverage Status
HOST IPS	No Coverage Status
NETWORK SECURITY PLATFORM	No Coverage Status
VULNERABILITY MANAGER	No Coverage Status
WEB GATEWAY	No Coverage Status
REMEDIATION MANAGER	No Coverage Status
POLICY AUDITOR	No Coverage Status
NETWORK ACCESS CONTROL	No Coverage Status
FIREWALL ENTERPRISE	No Coverage Status
APPLICATION CONTROL	No Coverage Status
DATABASE ACTIVITY MONITORING	No Coverage Status
VULNERABILITY MANAGER FOR DATABASES	No Coverage Status
ADDITIONAL INFORMATION	Microsoft: Security Update Summary

Back to top

(MSPT-Nov2019) Microsoft Windows Improperly Handles Objects In Memory Denial of Service (CVE-2019-1391)

MTIS19-052-T

THREAT IDENTIFIER(S)	CVE-2019-1391
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 a denial of service. The flaw lies in the improperly handles objects in memory. 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 November 12, Microsoft released an update to address this vulnerability
MCAFEE PRODUCT COVERAGE	
DAT FILES	No Coverage Status
VIRUS SCAN ENTERPRISE SCAN BOP	No Coverage Status
HOST IPS	No Coverage Status
NETWORK SECURITY PLATFORM	No Coverage Status
VULNERABILITY MANAGER	No Coverage Status
WEB GATEWAY	No Coverage Status
REMEDIATION MANAGER	No Coverage Status
POLICY AUDITOR	No Coverage Status

NETWORK ACCESS CONTROL	No Coverage Status
FIREWALL ENTERPRISE	No Coverage Status
APPLICATION CONTROL	No Coverage Status
DATABASE ACTIVITY MONITORING	No Coverage Status
VULNERABILITY MANAGER FOR DATABASES	No Coverage Status
ADDITIONAL INFORMATION	Microsoft: Security Update Summary

Back to top

(MSPT-Nov2019) Microsoft Windows Kernel Privilege Escalation (CVE-2019-1392)

MTIS19-052-U

THREAT IDENTIFIER(S)	CVE-2019-1392
THREAT TYPE	Vulnerability
RISK ASSESSMENT	Medium
MAIN THREAT VECTORS	Locally logged-on user
USER INTERACTION REQUIRED	No
DESCRIPTION	A vulnerability in some versions of Microsoft Windows could lead to privilege escalation. The flaw lies in the Kernel component. Successful exploitation could allow a local user to gain elevated privileges. The exploit requires the attacker to have valid credentials to the vulnerable system.
IMPORTANCE	Medium. On November 12, Microsoft released an update to address this vulnerability
MCAFEE PRODUCT COVERAGE	
DAT FILES	No Coverage Status
VIRUS SCAN ENTERPRISE SCAN BOP	No Coverage Status
HOST IPS	No Coverage Status
NETWORK SECURITY PLATFORM	No Coverage Status
VULNERABILITY MANAGER	No Coverage Status
WEB GATEWAY	No Coverage Status
REMEDIATION MANAGER	No Coverage Status
POLICY AUDITOR	No Coverage Status
NETWORK ACCESS CONTROL	No Coverage Status
FIREWALL ENTERPRISE	No Coverage Status
APPLICATION CONTROL	No Coverage Status
DATABASE ACTIVITY MONITORING	No Coverage Status
VULNERABILITY MANAGER FOR DATABASES	No Coverage Status
ADDITIONAL INFORMATION	Microsoft: Security Update Summary

Back to top

(MSPT-Nov2019) Microsoft Windows Win32k Privilege Escalation (CVE-2019-1393)

MTIS19-052-V

THREAT IDENTIFIER(S)	CVE-2019-1393
THREAT TYPE	Vulnerability
RISK ASSESSMENT	Medium
MAIN THREAT VECTORS	Locally logged-on user
USER INTERACTION REQUIRED	No
DESCRIPTION	A vulnerability in some versions of Microsoft Windows could lead to privilege escalation. The flaw lies in the Win32k 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 November 12, Microsoft released an update to address this vulnerability
MCAFEE PRODUCT COVERAGE	
DAT FILES	No Coverage Status
VIRUS SCAN ENTERPRISE SCAN BOP	No Coverage Status

HOST IPS	No Coverage Status
NETWORK SECURITY PLATFORM	No Coverage Status
VULNERABILITY MANAGER	No Coverage Status
WEB GATEWAY	No Coverage Status
REMEDIATION MANAGER	No Coverage Status
POLICY AUDITOR	No Coverage Status
NETWORK ACCESS CONTROL	No Coverage Status
FIREWALL ENTERPRISE	No Coverage Status
APPLICATION CONTROL	No Coverage Status
DATABASE ACTIVITY MONITORING	No Coverage Status
VULNERABILITY MANAGER FOR DATABASES	No Coverage Status
ADDITIONAL INFORMATION	Microsoft: Security Update Summary

Back to top

(MSPT-Nov2019) Microsoft Windows Win32k Privilege Escalation (CVE-2019-1394)

MTIS19-052-W

THREAT IDENTIFIER(S)	CVE-2019-1394
THREAT TYPE	Vulnerability
RISK ASSESSMENT	Medium
MAIN THREAT VECTORS	Locally logged-on user
USER INTERACTION REQUIRED	No
DESCRIPTION	A vulnerability in some versions of Microsoft Windows could lead to privilege escalation. The flaw lies in the Win32k 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 November 12, Microsoft released an update to address this vulnerability
MCAFEE PRODUCT COVERAGE	
DAT FILES	No Coverage Status
VIRUS SCAN ENTERPRISE SCAN BOP	No Coverage Status
HOST IPS	No Coverage Status
NETWORK SECURITY PLATFORM	No Coverage Status
VULNERABILITY MANAGER	No Coverage Status
WEB GATEWAY	No Coverage Status
REMEDIATION MANAGER	No Coverage Status
POLICY AUDITOR	No Coverage Status
NETWORK ACCESS CONTROL	No Coverage Status
FIREWALL ENTERPRISE	No Coverage Status
APPLICATION CONTROL	No Coverage Status
DATABASE ACTIVITY MONITORING	No Coverage Status
VULNERABILITY MANAGER FOR DATABASES	No Coverage Status
ADDITIONAL INFORMATION	Microsoft: Security Update Summary

Back to top

(MSPT-Nov2019) Microsoft Windows Win32k Privilege Escalation (CVE-2019-1395)

MTIS19-052-X

THREAT IDENTIFIER(S)	CVE-2019-1395
THREAT TYPE	Vulnerability
RISK ASSESSMENT	Medium
MAIN THREAT VECTORS	Locally logged-on user
USER INTERACTION REQUIRED	No

DESCRIPTION	A vulnerability in some versions of Microsoft Windows could lead to privilege escalation. The flaw lies in the Win32k 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 November 12, Microsoft released an update to address this vulnerability
MCAFEE PRODUCT COVERAGE	
DAT FILES	No Coverage Status
VIRUS SCAN ENTERPRISE SCAN BOP	No Coverage Status
HOST IPS	No Coverage Status
NETWORK SECURITY PLATFORM	No Coverage Status
VULNERABILITY MANAGER	No Coverage Status
WEB GATEWAY	No Coverage Status
REMEDIATION MANAGER	No Coverage Status
POLICY AUDITOR	No Coverage Status
NETWORK ACCESS CONTROL	No Coverage Status
FIREWALL ENTERPRISE	No Coverage Status
APPLICATION CONTROL	No Coverage Status
DATABASE ACTIVITY MONITORING	No Coverage Status
VULNERABILITY MANAGER FOR DATABASES	No Coverage Status
ADDITIONAL INFORMATION	Microsoft: Security Update Summary

Back to top

(MSPT-Nov2019) Microsoft Windows Win32k Privilege Escalation (CVE-2019-1396)

MTIS19-052-Y

THREAT IDENTIFIER(S)	CVE-2019-1396
THREAT TYPE	Vulnerability
RISK ASSESSMENT	Medium
MAIN THREAT VECTORS	Locally logged-on user
USER INTERACTION REQUIRED	No
DESCRIPTION	A vulnerability in some versions of Microsoft Windows could lead to privilege escalation. The flaw lies in the Win32k 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 November 12, Microsoft released an update to address this vulnerability
MCAFEE PRODUCT COVERAGE	
DAT FILES	No Coverage Status
VIRUS SCAN ENTERPRISE SCAN BOP	No Coverage Status
HOST IPS	No Coverage Status
NETWORK SECURITY PLATFORM	No Coverage Status
VULNERABILITY MANAGER	No Coverage Status
WEB GATEWAY	No Coverage Status
REMEDIATION MANAGER	No Coverage Status
POLICY AUDITOR	No Coverage Status
NETWORK ACCESS CONTROL	No Coverage Status
FIREWALL ENTERPRISE	No Coverage Status
APPLICATION CONTROL	No Coverage Status
DATABASE ACTIVITY MONITORING	No Coverage Status
VULNERABILITY MANAGER FOR DATABASES	No Coverage Status
ADDITIONAL INFORMATION	Microsoft: Security Update Summary

Back to top

(MSPT-Nov2019) Microsoft Windows Hyper-V Remote Code Execution (CVE-2019-1397)

MTIS19-052-Z

THREAT IDENTIFIER(S)	CVE-2019-1397
THREAT TYPE	Vulnerability
RISK ASSESSMENT	High
MAIN THREAT VECTORS	Locally logged-on user
USER INTERACTION REQUIRED	No
DESCRIPTION	A vulnerability in some versions of Microsoft Windows could lead to remote code execution. The flaw lies in the Hyper-V component. Successful exploitation by a remote attacker could result in the execution of arbitrary code. The exploit requires the attacker to have valid credentials to the vulnerable system.
IMPORTANCE	High. On November 12, Microsoft released an update to address this vulnerability
MCAFEE PRODUCT COVERAGE	
DAT FILES	No Coverage Status
VIRUS SCAN ENTERPRISE SCAN BOP	No Coverage Status
HOST IPS	No Coverage Status
NETWORK SECURITY PLATFORM	No Coverage Status
VULNERABILITY MANAGER	No Coverage Status
WEB GATEWAY	No Coverage Status
REMEDIATION MANAGER	No Coverage Status
POLICY AUDITOR	No Coverage Status
NETWORK ACCESS CONTROL	No Coverage Status
FIREWALL ENTERPRISE	No Coverage Status
APPLICATION CONTROL	No Coverage Status
DATABASE ACTIVITY MONITORING	No Coverage Status
VULNERABILITY MANAGER FOR DATABASES	No Coverage Status
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