EXECUTIVE SUMMARY

November 12, 2019 | MTIS19-054

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 DirectWrite Information Disclosure (CVE-2019-1432)

MTIS19-054-A

IMPORTANCE: Medium
COVERED PRODUCTS:
UNDER ANALYSIS:

Back to top

(MSPT-Nov2019) Microsoft Windows Graphics Privilege Escalation (CVE-2019-1433)

MTIS19-054-B

IMPORTANCE: Medium
COVERED PRODUCTS:
UNDER ANALYSIS:

Back to top

(MSPT-Nov2019) Microsoft Windows kernel-mode Privilege Escalation (CVE-2019-1434)

MTIS19-054-C

IMPORTANCE: Medium
COVERED PRODUCTS:
UNDER ANALYSIS:

Back to top

(MSPT-Nov2019) Microsoft Windows Graphics Privilege Escalation (CVE-2019-1435)

MTIS19-054-D

IMPORTANCE: Medium
COVERED PRODUCTS:
UNDER ANALYSIS:

Back to top

(MSPT-Nov2019) Microsoft Windows win32k Information Disclosure (CVE-2019-1436)

MTIS19-054-E

IMPORTANCE: Medium
COVERED PRODUCTS:
UNDER ANALYSIS:

Back to top

(MSPT-Nov2019) Microsoft Windows Graphics Privilege Escalation (CVE-2019-1437)
MTIS19-054-F

IMPORTANCE: Medium
COVERED PRODUCTS:
UNDER ANALYSIS:

Back to top

(MSPT-Nov2019) Microsoft Windows Graphics Privilege Escalation (CVE-2019-1438)
MTIS19-054-G

IMPORTANCE: Medium
COVERED PRODUCTS:
UNDER ANALYSIS:

Back to top

(MSPT-Nov2019) Microsoft Windows GDI Information Disclosure (CVE-2019-1439)
MTIS19-054-H

IMPORTANCE: Medium
COVERED PRODUCTS:
UNDER ANALYSIS:

Back to top

(MSPT-Nov2019) Microsoft Windows win32k Information Disclosure (CVE-2019-1440)
MTIS19-054-I

IMPORTANCE: Medium
COVERED PRODUCTS:
UNDER ANALYSIS:

Back to top

(MSPT-Nov2019) Microsoft Windows Font Library Remote Code Execution (CVE-2019-1441)
MTIS19-054-J

IMPORTANCE: High
COVERED PRODUCTS:
UNDER ANALYSIS:

Back to top

(MSPT-Nov2019) Microsoft Office Does Not Validate URLs Remote Code Execution (CVE-2019-1442)
MTIS19-054-K

IMPORTANCE: Medium
COVERED PRODUCTS:
UNDER ANALYSIS:

Back to top

(MSPT-Nov2019) Microsoft Windows SharePoint Information Disclosure (CVE-2019-1443)
MTIS19-054-L

IMPORTANCE: Medium
COVERED PRODUCTS:
UNDER ANALYSIS:

Back to top

(MSPT-Nov2019) Microsoft Office Online Spoofing Vulnerability (CVE-2019-1445)
MTIS19-054-M

IMPORTANCE: Medium
COVERED PRODUCTS:
UNDER ANALYSIS:

Back to top

(MSPT-Nov2019) Microsoft Excel Information Disclosure Vulnerability (CVE-2019-1446)
MTIS19-054-N

IMPORTANCE: Medium
COVERED PRODUCTS:
UNDER ANALYSIS:

Back to top

(MSPT-Nov2019) Microsoft Office Online Server Spoofing VUlnerability (CVE-2019-1447)
MTIS19-054-O

IMPORTANCE: Medium
COVERED PRODUCTS:
UNDER ANALYSIS:

Back to top

(MSPT-Nov2019) Microsoft Excel Remote Code Execution (CVE-2019-1448)
MTIS19-054-P

IMPORTANCE: Medium
COVERED PRODUCTS:
UNDER ANALYSIS:

Back to top

(MSPT-Nov2019) Microsoft Office C2R Remote Code Execution (CVE-2019-1449)
MTIS19-054-Q

IMPORTANCE: Medium
COVERED PRODUCTS:
UNDER ANALYSIS:

Back to top

(MSPT-Nov2019) Microsoft Kernel Improperly Handles Objects in Memory Information Disclosure (CVE-2018-12207)
MTIS19-054-R

IMPORTANCE: Medium
COVERED PRODUCTS:
UNDER ANALYSIS:

Back to top

(MSPT-Nov2019) Microsoft Kernel Information Disclosure (CVE-2019-11135)
MTIS19-054-S

IMPORTANCE: Medium
COVERED PRODUCTS:
UNDER ANALYSIS:

Back to top

(MSPT-Nov2019) Microsoft Azure Stack Spoofing (CVE-2019-1234)
MTIS19-054-T

IMPORTANCE: Medium
COVERED PRODUCTS:
UNDER ANALYSIS:

Back to top

(MSPT-Nov2019) Microsoft Windows Adobe Remote Code Execution (CVE-2019-1456)
MTIS19-054-U

IMPORTANCE:	Medium
COVERED PRODUCTS:	
UNDER ANALYSIS:	

Back to top

(MSPT-Nov2019) Microsoft Windows Office Remote Code Execution (CVE-2019-1457)
MTIS19-054-V

IMPORTANCE:	Medium
COVERED PRODUCTS:	
UNDER ANALYSIS:	

Back to top

THREAT DETAILS

(MSPT-Nov2019) Microsoft DirectWrite Information Disclosure (CVE-2019-1432)
MTIS19-054-A

THREAT IDENTIFIER(S)	CVE-2019-1432
THREAT TYPE	Vulnerability
RISK ASSESSMENT	Medium
MAIN THREAT VECTORS	Web
USER INTERACTION REQUIRED	Yes
DESCRIPTION	A vulnerability in some versions of Microsoft DirectWrite could lead to information disclosure. The flaw lies in the improper disclosure of contents of memory. Successful exploitation by an 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 Windows Graphics Privilege Escalation (CVE-2019-1433)
MTIS19-054-B

THREAT IDENTIFIER(S)	CVE-2019-1433
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 Graphics component. Successful exploitation could allow a local user to gain elevated privileges. The exploit requires the attacker to have valid credentials to the vulnerable system.
IMPORTANCE	Medium. On 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-mode Privilege Escalation (CVE-2019-1434)

MTIS19-054-C

THREAT IDENTIFIER(S)	CVE-2019-1434
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-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 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 Graphics Privilege Escalation (CVE-2019-1435)

MTIS19-054-D

THREAT IDENTIFIER(S)	CVE-2019-1435
THREAT TYPE	Vulnerability
RISK ASSESSMENT	Medium
MAIN THREAT VECTORS	Locally logged-on user
USER INTERACTION REQUIRED	No
DESCRIPTION	A vulnerability in some versions of Microsoft Windows could lead to privilege escalation. The flaw lies in the Graphics component. Successful exploitation could allow a local user to gain elevated privileges. The exploit requires the attacker to have valid credentials to the vulnerable system.
IMPORTANCE	Medium. On 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 Information Disclosure (CVE-2019-1436)

MTIS19-054-E

THREAT IDENTIFIER(S)	CVE-2019-1436
THREAT TYPE	Vulnerability
RISK ASSESSMENT	Medium
MAIN THREAT VECTORS	Locally logged-on user
USER INTERACTION REQUIRED	No
DESCRIPTION	A vulnerability in some versions of Microsoft Windows could lead to information disclosure. The flaw lies in the win32k component. Successful exploitation by a remote attacker could result in the disclosure of sensitive information. The exploit requires the attacker to have valid credentials to the vulnerable system.
IMPORTANCE	Medium. On 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 Graphics Privilege Escalation (CVE-2019-1437)

MTIS19-054-F

THREAT IDENTIFIER(S)	CVE-2019-1437
THREAT TYPE	Vulnerability
RISK ASSESSMENT	Medium
MAIN THREAT VECTORS	Locally logged-on user
USER INTERACTION REQUIRED	No
DESCRIPTION	A vulnerability in some versions of Microsoft Windows could lead to privilege escalation. The flaw lies in the Graphics component. Successful exploitation could allow a local user to gain elevated privileges. The exploit requires the attacker to have valid credentials to the vulnerable system.
IMPORTANCE	Medium. On 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 Graphics Privilege Escalation (CVE-2019-1438)

MTIS19-054-G

THREAT IDENTIFIER(S)	CVE-2019-1438
THREAT TYPE	Vulnerability
RISK ASSESSMENT	Medium
MAIN THREAT VECTORS	Locally logged-on user
USER INTERACTION REQUIRED	No
DESCRIPTION	A vulnerability in some versions of Microsoft Windows could lead to privilege escalation. The flaw lies in the Graphics component. Successful exploitation could allow a local user to gain elevated privileges. The exploit requires the attacker to have valid credentials to the vulnerable system.
IMPORTANCE	Medium. On 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 GDI Information Disclosure (CVE-2019-1439)

MTIS19-054-H

THREAT IDENTIFIER(S)	CVE-2019-1439
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 an 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 Windows win32k Information Disclosure (CVE-2019-1440)

MTIS19-054-I

THREAT IDENTIFIER(S)	CVE-2019-1440
THREAT TYPE	Vulnerability
RISK ASSESSMENT	Medium
MAIN THREAT VECTORS	Web
USER INTERACTION REQUIRED	No
	A vulnerability in some versions of Microsoft Windows could lead to information

DESCRIPTION	disclosure. The flaw lies in the win32k component. Successful exploitation by a remote attacker could result in the disclosure of sensitive information. The exploit requires the attacker to have valid credentials to the vulnerable system.
IMPORTANCE	Medium. On 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 Font Library Remote Code Execution (CVE-2019-1441)

MTIS19-054-J

THREAT IDENTIFIER(S)	CVE-2019-1441
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 Font Library 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 Office Does Not Validate URLs Remote Code Execution (CVE-2019-1442)

MTIS19-054-K

THREAT IDENTIFIER(S)	CVE-2019-1442
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 does not validate URLs. 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 Windows SharePoint Information Disclosure (CVE-2019-1443)

MTIS19-054-L

THREAT IDENTIFIER(S)	CVE-2019-1443
THREAT TYPE	Vulnerability
RISK ASSESSMENT	Medium
MAIN THREAT VECTORS	Web
USER INTERACTION REQUIRED	No
DESCRIPTION	A vulnerability in some versions of Microsoft Windows could lead to information disclosure. The flaw lies in the SharePoint component. Successful exploitation by a remote attacker could result in the disclosure of sensitive information. The exploit requires the attacker to have valid credentials to the vulnerable system.
IMPORTANCE	Medium. On 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 Office Online Spoofing Vulnerability (CVE-2019-1445)

MTIS19-054-M

THREAT IDENTIFIER(S)	CVE-2019-1445
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 Online could lead to spoofing. The flaw lis due to improper validation of origin in cross-origin communications handlers. 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 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 Excel Information Disclosure Vulnerability (CVE-2019-1446)

MTIS19-054-N

THREAT IDENTIFIER(S)	CVE-2019-1446
THREAT TYPE	Vulnerability
RISK ASSESSMENT	Medium
MAIN THREAT VECTORS	Web
USER INTERACTION REQUIRED	Yes
DESCRIPTION	A vulnerability in some versions of Microsoft Excel could lead to information disclosure. The flaw lies in the improper disclosure of the contents of memory. Successful exploitation by an 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 Office Online Server Spoofing VUlnerability (CVE-2019-1447)

MTIS19-054-O

THREAT IDENTIFIER(S)	CVE-2019-1447
THREAT TYPE	Vulnerability
RISK ASSESSMENT	Medium
MAIN THREAT VECTORS	Web
USER INTERACTION REQUIRED	No
DESCRIPTION	A vulnerability in some versions of Microsoft Office Online Server could lead to spoofing. The flaw lies in the improper sanitizeation of user inputs. Successful exploitation by an attacker could result in spoofing. 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 Excel Remote Code Execution (CVE-2019-1448)

MTIS19-054-P

THREAT IDENTIFIER(S)	CVE-2019-1448
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 the improper handling of objects in memory. Successful exploitation by an 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 Office C2R Remote Code Execution (CVE-2019-1449)

MTIS19-054-Q

THREAT IDENTIFIER(S)	CVE-2019-1449
THREAT TYPE	Vulnerability
RISK ASSESSMENT	Medium
MAIN THREAT VECTORS	Web
USER INTERACTION REQUIRED	No
DESCRIPTION	A vulnerability in some versions of Microsoft Office could lead to remote code execution. The flaw lies in the C2R component. Successful exploitation by a remote attacker could result in the execution of arbitrary code. The exploit requires the attacker to have valid credentials to the vulnerable system.
IMPORTANCE	Medium. On 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 Kernel Improperly Handles Objects in Memory Information Disclosure (CVE-2018-12207)

MTIS19-054-R

THREAT IDENTIFIER(S)	CVE-2018-12207
THREAT TYPE	Vulnerability
RISK ASSESSMENT	Medium

MAIN THREAT VECTORS	Web
USER INTERACTION REQUIRED	No
DESCRIPTION	A vulnerability in some versions of Microsoft Kernel could lead to information disclosure. The flaw lies in improperly handles objects in memory. Successful exploitation by a remote attacker could result in the disclosure of sensitive information. The exploit requires the attacker to have valid credentials to the vulnerable system.
IMPORTANCE	Medium. On 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 Kernel Information Disclosure (CVE-2019-11135)

MTIS19-054-S

THREAT IDENTIFIER(S)	CVE-2019-11135
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 Kernel could lead to information disclosure. The flaw lies in the improper handling of 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 Azure Stack Spoofing (CVE-2019-1234)

MTIS19-054-T

THREAT IDENTIFIER(S)	CVE-2019-1234
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 Azure could lead to spoofing. The flaw lies in the Stack component. Successful exploitation by a remote attacker could result in spoofing
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 Adobe Remote Code Execution (CVE-2019-1456)

MTIS19-054-U

THREAT IDENTIFIER(S)	CVE-2019-1456
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 Adobe 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 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 Office Remote Code Execution (CVE-2019-1457)

MTIS19-054-V

THREAT IDENTIFIER(S)	CVE-2019-1457
THREAT TYPE	Vulnerability
RISK ASSESSMENT	Medium
MAIN THREAT VECTORS	Web
USER INTERACTION REQUIRED	No
DESCRIPTION	A vulnerability in some versions of Microsoft Office could lead to remote code execution. The flaw lies in the Office component. Successful exploitation by a remote attacker could result in the execution of arbitrary code.
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

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