## EXECUTIVE SUMMARY

October 8, 2019 | MTIS19-047

Since the last McAfee® Labs Security Advisory (September 24), the following noteworthy event has taken place:

- Patches are available for multiple Microsoft security vulnerabilities

## NEW THREAT OVERVIEW

### (MSPT-Oct2019) Microsoft Windows SharePoint Privilege Escalation (CVE-2019-1330)

*MTIS19-047-A*

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

Back to top

### (MSPT-Oct2019) Microsoft Excel Remote Code Execution (CVE-2019-1331)

*MTIS19-047-B*

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

Back to top

### (MSPT-Oct2019) Microsoft Windows Remote Desktop Remote Code Execution (CVE-2019-1333)

*MTIS19-047-C*

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

Back to top

### (MSPT-Oct2019) Microsoft Kernel Improperly Handles Objects In Memory Information Disclosure (CVE-2019-1334)

*MTIS19-047-D*

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

Back to top

### (MSPT-Oct2019) Microsoft Edge Chakra Remote Code Execution (CVE-2019-1335)

*MTIS19-047-E*

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

Back to top

### (MSPT-Oct2019) Microsoft Windows Update Client Privilege Escalation (CVE-2019-1336)

*MTIS19-047-F*

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

Back to top

### (MSPT-Oct2019) Microsoft Windows Update Client Information Disclosure (CVE-2019-1337)

*MTIS19-047-G*

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

Back to top

### (MSPT-Oct2019) Microsoft Windows NTLMv2 Security Bypass (CVE-2019-1338)

*MTIS19-047-H*

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

Back to top

### (MSPT-Oct2019) Microsoft Windows Error Reporting Privilege Escalation (CVE-2019-1339)

*MTIS19-047-I*

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

Back to top

### (MSPT-Oct2019) Microsoft Windows AppX Privilege Escalation (CVE-2019-1340)

*MTIS19-047-J*

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

Back to top

### (MSPT-Oct2019) Microsoft Power Service umpo.dll Privilege Escalation (CVE-2019-1341)

*MTIS19-047-K*

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

Back to top

### (MSPT-Oct2019) Microsoft Windows Error Reporting Privilege Escalation (CVE-2019-1342)

*MTIS19-047-L*

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

Back to top

### (MSPT-Oct2019) Microsoft Windows Improperly Handles Objects In Memory Denial of Service (CVE-2019-1343)

*MTIS19-047-M*

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

Back to top

### (MSPT-Oct2019) Microsoft Windows Code Integrity Information Disclosure (CVE-2019-1344)

*MTIS19-047-N*

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

Back to top

### (MSPT-Oct2019) Microsoft Kernel Improperly Handles Objects In Memory Information Disclosure (CVE-2019-1345)

*MTIS19-047-O*

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

Back to top

(MSPT-Oct2019) Microsoft Windows Improperly Handles Objects In Memory Denial of Service (CVE-2019-1346)
*MTIS19-047-P*

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

Back to top

(MSPT-Oct2019) Microsoft Windows Improperly Handles Objects In Memory Denial of Service (CVE-2019-1347)
*MTIS19-047-Q*

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

Back to top

(MSPT-Oct2019) Microsoft Edge HTML Information Disclosure (CVE-2019-1356)
*MTIS19-047-R*

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

Back to top

(MSPT-Oct2019) Microsoft Browsers Improperly Handle Browser Cookies Spoofing (CVE-2019-1357)
*MTIS19-047-S*

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

Back to top

(MSPT-Oct2019) Microsoft Windows Jet Database Engine Remote Code Execution (CVE-2019-1358)
*MTIS19-047-T*

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

Back to top

(MSPT-Oct2019) Microsoft Windows Jet Database Engine Remote Code Execution (CVE-2019-1359)
*MTIS19-047-U*

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

Back to top

(MSPT-Oct2019) Microsoft Graphics Improperly Handle Objects In Memory Information Disclosure (CVE-2019-1361)
*MTIS19-047-V*

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

Back to top

(MSPT-Oct2019) Microsoft Windows Kernel-Mode Privilege Escalation (CVE-2019-1362)
*MTIS19-047-W*

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

Back to top

(MSPT-Oct2019) Microsoft GDI Improperly Handles Objects In Memory Information Disclosure (CVE-2019-1363)
*MTIS19-047-X*

IMPORTANCE: **Medium**

| | |
|---|---|
| COVERED PRODUCTS: | |
| UNDER ANALYSIS: | DAT \| Web Gateway \| Firewall Enterprise |

Back to top

### (MSPT-Oct2019) Microsoft Windows Kernel-mode Driver Privilege Escalation (CVE-2019-1364)

*MTIS19-047-Y*

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

Back to top

### (MSPT-Oct2019) Microsoft IIS Server Fails To Check The Length Of A Buffer Privilege Escalation (CVE-2019-1365)

*MTIS19-047-Z*

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

Back to top

## THREAT DETAILS

### (MSPT-Oct2019) Microsoft Windows SharePoint Privilege Escalation (CVE-2019-1330)

*MTIS19-047-A*

| | |
|---|---|
| **THREAT IDENTIFIER(S)** | CVE-2019-1330 |
| **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 SharePoint component. 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 October 8, Microsoft released an update to address this vulnerability |
| **MCAFEE PRODUCT COVERAGE** | |
| DAT FILES | Under analysis |
| VIRUS SCAN ENTERPRISE SCAN BOP | Out of scope |
| HOST IPS | Out of scope |
| NETWORK SECURITY PLATFORM | Coverage not warranted |
| VULNERABILITY MANAGER | An upcoming FSL/MVM content release will contain coverage for this issue. |
| WEB GATEWAY | Under analysis |
| REMEDIATION MANAGER | Not applicable |
| POLICY AUDITOR | An upcoming SCAP content release will contain coverage for this issue. |
| NETWORK ACCESS CONTROL | An upcoming SCAP content release will contain coverage for this issue. |
| FIREWALL ENTERPRISE | Under analysis |
| APPLICATION CONTROL | Out of scope |
| DATABASE ACTIVITY MONITORING | Out of scope |
| VULNERABILITY MANAGER FOR DATABASES | Out of scope |
| **ADDITIONAL INFORMATION** | Microsoft: Security Update Summary |

Back to top

### (MSPT-Oct2019) Microsoft Excel Remote Code Execution (CVE-2019-1331)

*MTIS19-047-B*

| | |
|---|---|
| **THREAT IDENTIFIER(S)** | CVE-2019-1331 |
| **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 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 October 8, Microsoft released an update to address this vulnerability |
| **MCAFEE PRODUCT COVERAGE** | |
| DAT FILES | Under analysis |
| VIRUS SCAN ENTERPRISE SCAN BOP | Out of scope |
| HOST IPS | Out of scope |
| NETWORK SECURITY PLATFORM | Coverage not warranted |
| VULNERABILITY MANAGER | An upcoming FSL/MVM content release will contain coverage for this issue. |
| WEB GATEWAY | Under analysis |
| REMEDIATION MANAGER | Not applicable |
| POLICY AUDITOR | An upcoming SCAP content release will contain coverage for this issue. |
| NETWORK ACCESS CONTROL | An upcoming SCAP content release will contain coverage for this issue. |
| FIREWALL ENTERPRISE | Under analysis |
| APPLICATION CONTROL | Out of scope |
| DATABASE ACTIVITY MONITORING | Out of scope |
| VULNERABILITY MANAGER FOR DATABASES | Out of scope |
| **ADDITIONAL INFORMATION** | Microsoft: Security Update Summary |

Back to top

## (MSPT-Oct2019) Microsoft Windows Remote Desktop Remote Code Execution (CVE-2019-1333)

*MTIS19-047-C*

| | |
|---|---|
| **THREAT IDENTIFIER(S)** | CVE-2019-1333 |
| **THREAT TYPE** | Vulnerability |
| **RISK ASSESSMENT** | High |
| **MAIN THREAT VECTORS** | Web |
| **USER INTERACTION REQUIRED** | No |
| **DESCRIPTION** | A vulnerability in some versions of Microsoft Windows could lead to remote code execution. The flaw lies in the Remote Desktop component. Successful exploitation by a remote attacker could result in the execution of arbitrary code. |
| **IMPORTANCE** | High. On October 8, Microsoft released an update to address this vulnerability |
| **MCAFEE PRODUCT COVERAGE** | |
| DAT FILES | Under analysis |
| VIRUS SCAN ENTERPRISE SCAN BOP | Out of scope |
| HOST IPS | Out of scope |
| NETWORK SECURITY PLATFORM | Coverage not warranted |
| VULNERABILITY MANAGER | An upcoming FSL/MVM content release will contain coverage for this issue. |
| WEB GATEWAY | Under analysis |
| REMEDIATION MANAGER | Not applicable |
| POLICY AUDITOR | An upcoming SCAP content release will contain coverage for this issue. |
| NETWORK ACCESS CONTROL | An upcoming SCAP content release will contain coverage for this issue. |
| FIREWALL ENTERPRISE | Under analysis |
| APPLICATION CONTROL | Out of scope |
| DATABASE ACTIVITY MONITORING | Out of scope |
| VULNERABILITY MANAGER FOR DATABASES | Out of scope |
| **ADDITIONAL INFORMATION** | Microsoft: Security Update Summary |

Back to top

## (MSPT-Oct2019) Microsoft Kernel Improperly Handles Objects In Memory Information Disclosure (CVE-2019-1334)

*MTIS19-047-D*

| | |
|---|---|
| **THREAT IDENTIFIER(S)** | CVE-2019-1334 |
| **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 the 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 October 8, Microsoft released an update to address this vulnerability |
| **MCAFEE PRODUCT COVERAGE** | |
| DAT FILES | Under analysis |
| VIRUS SCAN ENTERPRISE SCAN BOP | Out of scope |
| HOST IPS | Out of scope |
| NETWORK SECURITY PLATFORM | Coverage not warranted |
| VULNERABILITY MANAGER | An upcoming FSL/MVM content release will contain coverage for this issue. |
| WEB GATEWAY | Under analysis |
| REMEDIATION MANAGER | Not applicable |
| POLICY AUDITOR | An upcoming SCAP content release will contain coverage for this issue. |
| NETWORK ACCESS CONTROL | An upcoming SCAP content release will contain coverage for this issue. |
| FIREWALL ENTERPRISE | Under analysis |
| APPLICATION CONTROL | Out of scope |
| DATABASE ACTIVITY MONITORING | Out of scope |
| VULNERABILITY MANAGER FOR DATABASES | Out of scope |
| **ADDITIONAL INFORMATION** | Microsoft: Security Update Summary |

Back to top

## (MSPT-Oct2019) Microsoft Edge Chakra Remote Code Execution (CVE-2019-1335)

*MTIS19-047-E*

| | |
|---|---|
| **THREAT IDENTIFIER(S)** | CVE-2019-1335 |
| **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 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** | High. On October 8, Microsoft released an update to address this vulnerability |
| **MCAFEE PRODUCT COVERAGE** | |
| DAT FILES | Under analysis |
| VIRUS SCAN ENTERPRISE SCAN BOP | Out of scope |
| HOST IPS | Out of scope |
| NETWORK SECURITY PLATFORM | Coverage not warranted |
| VULNERABILITY MANAGER | An upcoming FSL/MVM content release will contain coverage for this issue. |
| WEB GATEWAY | Under analysis |
| REMEDIATION MANAGER | Not applicable |
| POLICY AUDITOR | An upcoming SCAP content release will contain coverage for this issue. |
| NETWORK ACCESS CONTROL | An upcoming SCAP content release will contain coverage for this issue. |
| FIREWALL ENTERPRISE | Under analysis |
| APPLICATION CONTROL | Out of scope |
| DATABASE ACTIVITY MONITORING | Out of scope |
| VULNERABILITY MANAGER FOR DATABASES | Out of scope |
| **ADDITIONAL INFORMATION** | Microsoft: Security Update Summary |

Back to top

## (MSPT-Oct2019) Microsoft Windows Update Client Privilege Escalation (CVE-2019-1336)

*MTIS19-047-F*

| | |
|---|---|
| **THREAT IDENTIFIER(S)** | CVE-2019-1336 |
| **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 Update Client 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 October 8, Microsoft released an update to address this vulnerability |
| **MCAFEE PRODUCT COVERAGE** | |
| DAT FILES | Under analysis |
| VIRUS SCAN ENTERPRISE SCAN BOP | Out of scope |
| HOST IPS | Out of scope |
| NETWORK SECURITY PLATFORM | Coverage not warranted |
| VULNERABILITY MANAGER | An upcoming FSL/MVM content release will contain coverage for this issue. |
| WEB GATEWAY | Under analysis |
| REMEDIATION MANAGER | Not applicable |
| POLICY AUDITOR | An upcoming SCAP content release will contain coverage for this issue. |
| NETWORK ACCESS CONTROL | An upcoming SCAP content release will contain coverage for this issue. |
| FIREWALL ENTERPRISE | Under analysis |
| APPLICATION CONTROL | Out of scope |
| DATABASE ACTIVITY MONITORING | Out of scope |
| VULNERABILITY MANAGER FOR DATABASES | Out of scope |
| **ADDITIONAL INFORMATION** | Microsoft: Security Update Summary |

Back to top

## (MSPT-Oct2019) Microsoft Windows Update Client Information Disclosure (CVE-2019-1337)

*MTIS19-047-G*

| | |
|---|---|
| **THREAT IDENTIFIER(S)** | CVE-2019-1337 |
| **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 Update Client 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 October 8, Microsoft released an update to address this vulnerability |
| **MCAFEE PRODUCT COVERAGE** | |
| DAT FILES | Under analysis |
| VIRUS SCAN ENTERPRISE SCAN BOP | Out of scope |
| HOST IPS | Out of scope |
| NETWORK SECURITY PLATFORM | Coverage not warranted |
| VULNERABILITY MANAGER | An upcoming FSL/MVM content release will contain coverage for this issue. |
| WEB GATEWAY | Under analysis |
| REMEDIATION MANAGER | Not applicable |
| POLICY AUDITOR | An upcoming SCAP content release will contain coverage for this issue. |
| NETWORK ACCESS CONTROL | An upcoming SCAP content release will contain coverage for this issue. |
| FIREWALL ENTERPRISE | Under analysis |
| APPLICATION CONTROL | Out of scope |
| DATABASE ACTIVITY MONITORING | Out of scope |
| VULNERABILITY MANAGER FOR DATABASES | Out of scope |
| **ADDITIONAL INFORMATION** | Microsoft: Security Update Summary |

Back to top

## (MSPT-Oct2019) Microsoft Windows NTLMv2 Security Bypass (CVE-2019-1338)

*MTIS19-047-H*

| | |
|---|---|
| **THREAT IDENTIFIER(S)** | CVE-2019-1338 |
| **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 security bypass. The flaw lies in the NTLMv2 component. Successful exploitation by a remote attacker could result in the bypass of intended access restrictions. |
| **IMPORTANCE** | Medium. On October 8, Microsoft released an update to address this vulnerability |
| **MCAFEE PRODUCT COVERAGE** | |
| DAT FILES | Under analysis |
| VIRUS SCAN ENTERPRISE SCAN BOP | Out of scope |
| HOST IPS | Out of scope |
| NETWORK SECURITY PLATFORM | Coverage not warranted |
| VULNERABILITY MANAGER | An upcoming FSL/MVM content release will contain coverage for this issue. |
| WEB GATEWAY | Under analysis |
| REMEDIATION MANAGER | Not applicable |
| POLICY AUDITOR | An upcoming SCAP content release will contain coverage for this issue. |
| NETWORK ACCESS CONTROL | An upcoming SCAP content release will contain coverage for this issue. |
| FIREWALL ENTERPRISE | Under analysis |
| APPLICATION CONTROL | Out of scope |
| DATABASE ACTIVITY MONITORING | Out of scope |
| VULNERABILITY MANAGER FOR DATABASES | Out of scope |
| **ADDITIONAL INFORMATION** | Microsoft: Security Update Summary |

Back to top

## (MSPT-Oct2019) Microsoft Windows Error Reporting Privilege Escalation (CVE-2019-1339)

*MTIS19-047-I*

| | |
|---|---|
| **THREAT IDENTIFIER(S)** | CVE-2019-1339 |
| **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 Error Reporting 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 October 8, Microsoft released an update to address this vulnerability |
| **MCAFEE PRODUCT COVERAGE** | |
| DAT FILES | Under analysis |
| VIRUS SCAN ENTERPRISE SCAN BOP | Out of scope |
| HOST IPS | Out of scope |
| NETWORK SECURITY PLATFORM | Coverage not warranted |
| VULNERABILITY MANAGER | An upcoming FSL/MVM content release will contain coverage for this issue. |
| WEB GATEWAY | Under analysis |
| REMEDIATION MANAGER | Not applicable |
| POLICY AUDITOR | An upcoming SCAP content release will contain coverage for this issue. |
| NETWORK ACCESS CONTROL | An upcoming SCAP content release will contain coverage for this issue. |
| FIREWALL ENTERPRISE | Under analysis |
| APPLICATION CONTROL | Out of scope |
| DATABASE ACTIVITY MONITORING | Out of scope |
| VULNERABILITY MANAGER FOR DATABASES | Out of scope |
| **ADDITIONAL INFORMATION** | Microsoft: Security Update Summary |

Back to top

## (MSPT-Oct2019) Microsoft Windows AppX Privilege Escalation (CVE-2019-1340)

*MTIS19-047-J*

| | |
|---|---|
| **THREAT IDENTIFIER(S)** | CVE-2019-1340 |
| **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 AppX 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 October 8, Microsoft released an update to address this vulnerability |
| **MCAFEE PRODUCT COVERAGE** | |
| DAT FILES | Under analysis |
| VIRUS SCAN ENTERPRISE SCAN BOP | Out of scope |
| HOST IPS | Out of scope |
| NETWORK SECURITY PLATFORM | Coverage not warranted |
| VULNERABILITY MANAGER | An upcoming FSL/MVM content release will contain coverage for this issue. |
| WEB GATEWAY | Under analysis |
| REMEDIATION MANAGER | Not applicable |
| POLICY AUDITOR | An upcoming SCAP content release will contain coverage for this issue. |
| NETWORK ACCESS CONTROL | An upcoming SCAP content release will contain coverage for this issue. |
| FIREWALL ENTERPRISE | Under analysis |
| APPLICATION CONTROL | Out of scope |
| DATABASE ACTIVITY MONITORING | Out of scope |
| VULNERABILITY MANAGER FOR DATABASES | Out of scope |
| **ADDITIONAL INFORMATION** | Microsoft: Security Update Summary |

Back to top

## (MSPT-Oct2019) Microsoft Power Service umpo.dll Privilege Escalation (CVE-2019-1341)

*MTIS19-047-K*

| | |
|---|---|
| **THREAT IDENTIFIER(S)** | CVE-2019-1341 |
| **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 Power Service could lead to privilege escalation. The flaw lies in the umpo.dll 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 October 8, Microsoft released an update to address this vulnerability |
| **MCAFEE PRODUCT COVERAGE** | |
| DAT FILES | Under analysis |
| VIRUS SCAN ENTERPRISE SCAN BOP | Out of scope |
| HOST IPS | Out of scope |
| NETWORK SECURITY PLATFORM | Coverage not warranted |
| VULNERABILITY MANAGER | An upcoming FSL/MVM content release will contain coverage for this issue. |
| WEB GATEWAY | Under analysis |
| REMEDIATION MANAGER | Not applicable |
| POLICY AUDITOR | An upcoming SCAP content release will contain coverage for this issue. |
| NETWORK ACCESS CONTROL | An upcoming SCAP content release will contain coverage for this issue. |
| FIREWALL ENTERPRISE | Under analysis |
| APPLICATION CONTROL | Out of scope |
| DATABASE ACTIVITY MONITORING | Out of scope |
| VULNERABILITY MANAGER FOR DATABASES | Out of scope |
| **ADDITIONAL INFORMATION** | Microsoft: Security Update Summary |

Back to top

## (MSPT-Oct2019) Microsoft Windows Error Reporting Privilege Escalation (CVE-2019-1342)

*MTIS19-047-L*

| | |
|---|---|
| **THREAT IDENTIFIER(S)** | CVE-2019-1342 |
| **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 Error Reporting 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 October 8, Microsoft released an update to address this vulnerability |
| **MCAFEE PRODUCT COVERAGE** | |
| DAT FILES | Under analysis |
| VIRUS SCAN ENTERPRISE SCAN BOP | Out of scope |
| HOST IPS | Out of scope |
| NETWORK SECURITY PLATFORM | Coverage not warranted |
| VULNERABILITY MANAGER | An upcoming FSL/MVM content release will contain coverage for this issue. |
| WEB GATEWAY | Under analysis |
| REMEDIATION MANAGER | Not applicable |
| POLICY AUDITOR | An upcoming SCAP content release will contain coverage for this issue. |
| NETWORK ACCESS CONTROL | An upcoming SCAP content release will contain coverage for this issue. |
| FIREWALL ENTERPRISE | Under analysis |
| APPLICATION CONTROL | Out of scope |
| DATABASE ACTIVITY MONITORING | Out of scope |
| VULNERABILITY MANAGER FOR DATABASES | Out of scope |
| **ADDITIONAL INFORMATION** | Microsoft: Security Update Summary |

Back to top

## (MSPT-Oct2019) Microsoft Windows Improperly Handles Objects In Memory Denial of Service (CVE-2019-1343)

*MTIS19-047-M*

| | |
|---|---|
| **THREAT IDENTIFIER(S)** | CVE-2019-1343 |
| **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 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 October 8, Microsoft released an update to address this vulnerability |
| **MCAFEE PRODUCT COVERAGE** | |
| DAT FILES | Under analysis |
| VIRUS SCAN ENTERPRISE SCAN BOP | Out of scope |
| HOST IPS | Out of scope |
| NETWORK SECURITY PLATFORM | Coverage not warranted |
| VULNERABILITY MANAGER | An upcoming FSL/MVM content release will contain coverage for this issue. |
| WEB GATEWAY | Under analysis |
| REMEDIATION MANAGER | Not applicable |
| POLICY AUDITOR | An upcoming SCAP content release will contain coverage for this issue. |
| NETWORK ACCESS CONTROL | An upcoming SCAP content release will contain coverage for this issue. |
| FIREWALL ENTERPRISE | Under analysis |
| APPLICATION CONTROL | Out of scope |
| DATABASE ACTIVITY MONITORING | Out of scope |
| VULNERABILITY MANAGER FOR DATABASES | Out of scope |
| **ADDITIONAL INFORMATION** | Microsoft: Security Update Summary |

Back to top

## (MSPT-Oct2019) Microsoft Windows Code Integrity Information Disclosure (CVE-2019-1344)

*MTIS19-047-N*

| | |
|---|---|
| **THREAT IDENTIFIER(S)** | CVE-2019-1344 |
| **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 Code Integrity 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 October 8, Microsoft released an update to address this vulnerability |
| **MCAFEE PRODUCT COVERAGE** | |
| DAT FILES | Under analysis |
| VIRUS SCAN ENTERPRISE SCAN BOP | Out of scope |
| HOST IPS | Out of scope |
| NETWORK SECURITY PLATFORM | Coverage not warranted |
| VULNERABILITY MANAGER | An upcoming FSL/MVM content release will contain coverage for this issue. |
| WEB GATEWAY | Under analysis |
| REMEDIATION MANAGER | Not applicable |
| POLICY AUDITOR | An upcoming SCAP content release will contain coverage for this issue. |
| NETWORK ACCESS CONTROL | An upcoming SCAP content release will contain coverage for this issue. |
| FIREWALL ENTERPRISE | Under analysis |
| APPLICATION CONTROL | Out of scope |
| DATABASE ACTIVITY MONITORING | Out of scope |
| VULNERABILITY MANAGER FOR DATABASES | Out of scope |
| **ADDITIONAL INFORMATION** | Microsoft: Security Update Summary |

Back to top

## (MSPT-Oct2019) Microsoft Kernel Improperly Handles Objects In Memory Information Disclosure (CVE-2019-1345)

*MTIS19-047-O*

| | |
|---|---|
| **THREAT IDENTIFIER(S)** | CVE-2019-1345 |
| **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 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 October 8, Microsoft released an update to address this vulnerability |
| **MCAFEE PRODUCT COVERAGE** | |
| DAT FILES | Under analysis |
| VIRUS SCAN ENTERPRISE SCAN BOP | Out of scope |
| HOST IPS | Out of scope |
| NETWORK SECURITY PLATFORM | Coverage not warranted |
| VULNERABILITY MANAGER | An upcoming FSL/MVM content release will contain coverage for this issue. |
| WEB GATEWAY | Under analysis |
| REMEDIATION MANAGER | Not applicable |
| POLICY AUDITOR | An upcoming SCAP content release will contain coverage for this issue. |
| NETWORK ACCESS CONTROL | An upcoming SCAP content release will contain coverage for this issue. |
| FIREWALL ENTERPRISE | Under analysis |
| APPLICATION CONTROL | Out of scope |
| DATABASE ACTIVITY MONITORING | Out of scope |

| | |
|---|---|
| VULNERABILITY MANAGER FOR DATABASES | Out of scope |
| **ADDITIONAL INFORMATION** | Microsoft: Security Update Summary |

Back to top

## (MSPT-Oct2019) Microsoft Windows Improperly Handles Objects In Memory Denial of Service (CVE-2019-1346)

*MTIS19-047-P*

| | |
|---|---|
| **THREAT IDENTIFIER(S)** | CVE-2019-1346 |
| **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 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 October 8, Microsoft released an update to address this vulnerability |
| **MCAFEE PRODUCT COVERAGE** | |
| DAT FILES | Under analysis |
| VIRUS SCAN ENTERPRISE SCAN BOP | Out of scope |
| HOST IPS | Out of scope |
| NETWORK SECURITY PLATFORM | Coverage not warranted |
| VULNERABILITY MANAGER | An upcoming FSL/MVM content release will contain coverage for this issue. |
| WEB GATEWAY | Under analysis |
| REMEDIATION MANAGER | Not applicable |
| POLICY AUDITOR | An upcoming SCAP content release will contain coverage for this issue. |
| NETWORK ACCESS CONTROL | An upcoming SCAP content release will contain coverage for this issue. |
| FIREWALL ENTERPRISE | Under analysis |
| APPLICATION CONTROL | Out of scope |
| DATABASE ACTIVITY MONITORING | Out of scope |
| VULNERABILITY MANAGER FOR DATABASES | Out of scope |
| **ADDITIONAL INFORMATION** | Microsoft: Security Update Summary |

Back to top

## (MSPT-Oct2019) Microsoft Windows Improperly Handles Objects In Memory Denial of Service (CVE-2019-1347)

*MTIS19-047-Q*

| | |
|---|---|
| **THREAT IDENTIFIER(S)** | CVE-2019-1347 |
| **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 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 October 8, Microsoft released an update to address this vulnerability |
| **MCAFEE PRODUCT COVERAGE** | |
| DAT FILES | Under analysis |
| VIRUS SCAN ENTERPRISE SCAN BOP | Out of scope |
| HOST IPS | Out of scope |
| NETWORK SECURITY PLATFORM | Coverage not warranted |
| VULNERABILITY MANAGER | An upcoming FSL/MVM content release will contain coverage for this issue. |
| WEB GATEWAY | Under analysis |
| REMEDIATION MANAGER | Not applicable |
| POLICY AUDITOR | An upcoming SCAP content release will contain coverage for this issue. |
| NETWORK ACCESS CONTROL | An upcoming SCAP content release will contain coverage for this issue. |
| FIREWALL ENTERPRISE | Under analysis |
| APPLICATION CONTROL | Out of scope |

| | |
|---|---|
| DATABASE ACTIVITY MONITORING | Out of scope |
| VULNERABILITY MANAGER FOR DATABASES | Out of scope |
| **ADDITIONAL INFORMATION** | Microsoft: Security Update Summary |

Back to top

## (MSPT-Oct2019) Microsoft Edge HTML Information Disclosure (CVE-2019-1356)

*MTIS19-047-R*

| | |
|---|---|
| **THREAT IDENTIFIER(S)** | CVE-2019-1356 |
| **THREAT TYPE** | Vulnerability |
| **RISK ASSESSMENT** | Medium |
| **MAIN THREAT VECTORS** | Locally logged-on user |
| **USER INTERACTION REQUIRED** | Yes |
| **DESCRIPTION** | A vulnerability in some versions of Microsoft Edge could lead to information disclosure. The flaw lies in the HTML 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 October 8, Microsoft released an update to address this vulnerability |
| **MCAFEE PRODUCT COVERAGE** | |
| DAT FILES | Under analysis |
| VIRUS SCAN ENTERPRISE SCAN BOP | Out of scope |
| HOST IPS | Out of scope |
| NETWORK SECURITY PLATFORM | Coverage not warranted |
| VULNERABILITY MANAGER | An upcoming FSL/MVM content release will contain coverage for this issue. |
| WEB GATEWAY | Under analysis |
| REMEDIATION MANAGER | Not applicable |
| POLICY AUDITOR | An upcoming SCAP content release will contain coverage for this issue. |
| NETWORK ACCESS CONTROL | An upcoming SCAP content release will contain coverage for this issue. |
| FIREWALL ENTERPRISE | Under analysis |
| APPLICATION CONTROL | Out of scope |
| DATABASE ACTIVITY MONITORING | Out of scope |
| VULNERABILITY MANAGER FOR DATABASES | Out of scope |
| **ADDITIONAL INFORMATION** | Microsoft: Security Update Summary |

Back to top

## (MSPT-Oct2019) Microsoft Browsers Improperly Handle Browser Cookies Spoofing (CVE-2019-1357)

*MTIS19-047-S*

| | |
|---|---|
| **THREAT IDENTIFIER(S)** | CVE-2019-1357 |
| **THREAT TYPE** | Vulnerability |
| **RISK ASSESSMENT** | Medium |
| **MAIN THREAT VECTORS** | Web |
| **USER INTERACTION REQUIRED** | Yes |
| **DESCRIPTION** | A vulnerability in some versions of Microsoft Browsers could lead to spoofing. The flaw lies in the improperly handle browser cookies. 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 October 8, Microsoft released an update to address this vulnerability |
| **MCAFEE PRODUCT COVERAGE** | |
| DAT FILES | Under analysis |
| VIRUS SCAN ENTERPRISE SCAN BOP | Out of scope |
| HOST IPS | Out of scope |
| NETWORK SECURITY PLATFORM | Coverage not warranted |
| VULNERABILITY MANAGER | An upcoming FSL/MVM content release will contain coverage for this issue. |
| WEB GATEWAY | Under analysis |
| REMEDIATION MANAGER | Not applicable |
| POLICY AUDITOR | An upcoming SCAP content release will contain coverage for this issue. |
| NETWORK ACCESS CONTROL | An upcoming SCAP content release will contain coverage for this issue. |

| | |
|---|---|
| FIREWALL ENTERPRISE | Under analysis |
| APPLICATION CONTROL | Out of scope |
| DATABASE ACTIVITY MONITORING | Out of scope |
| VULNERABILITY MANAGER FOR DATABASES | Out of scope |
| **ADDITIONAL INFORMATION** | Microsoft: Security Update Summary |

Back to top

## (MSPT-Oct2019) Microsoft Windows Jet Database Engine Remote Code Execution (CVE-2019-1358)

*MTIS19-047-T*

| | |
|---|---|
| **THREAT IDENTIFIER(S)** | CVE-2019-1358 |
| **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 Jet Database Engine. 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 October 8, Microsoft released an update to address this vulnerability |
| **MCAFEE PRODUCT COVERAGE** | |
| DAT FILES | Under analysis |
| VIRUS SCAN ENTERPRISE SCAN BOP | Out of scope |
| HOST IPS | Out of scope |
| NETWORK SECURITY PLATFORM | Coverage not warranted |
| VULNERABILITY MANAGER | An upcoming FSL/MVM content release will contain coverage for this issue. |
| WEB GATEWAY | Under analysis |
| REMEDIATION MANAGER | Not applicable |
| POLICY AUDITOR | An upcoming SCAP content release will contain coverage for this issue. |
| NETWORK ACCESS CONTROL | An upcoming SCAP content release will contain coverage for this issue. |
| FIREWALL ENTERPRISE | Under analysis |
| APPLICATION CONTROL | Out of scope |
| DATABASE ACTIVITY MONITORING | Out of scope |
| VULNERABILITY MANAGER FOR DATABASES | Out of scope |
| **ADDITIONAL INFORMATION** | Microsoft: Security Update Summary |

Back to top

## (MSPT-Oct2019) Microsoft Windows Jet Database Engine Remote Code Execution (CVE-2019-1359)

*MTIS19-047-U*

| | |
|---|---|
| **THREAT IDENTIFIER(S)** | CVE-2019-1359 |
| **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 Jet Database Engine component. 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 October 8, Microsoft released an update to address this vulnerability |
| **MCAFEE PRODUCT COVERAGE** | |
| DAT FILES | Under analysis |
| VIRUS SCAN ENTERPRISE SCAN BOP | Out of scope |
| HOST IPS | Out of scope |
| NETWORK SECURITY PLATFORM | Coverage not warranted |
| VULNERABILITY MANAGER | An upcoming FSL/MVM content release will contain coverage for this issue. |
| WEB GATEWAY | Under analysis |
| REMEDIATION MANAGER | Not applicable |

| | |
|---|---|
| POLICY AUDITOR | An upcoming SCAP content release will contain coverage for this issue. |
| NETWORK ACCESS CONTROL | An upcoming SCAP content release will contain coverage for this issue. |
| FIREWALL ENTERPRISE | Under analysis |
| APPLICATION CONTROL | Out of scope |
| DATABASE ACTIVITY MONITORING | Out of scope |
| VULNERABILITY MANAGER FOR DATABASES | Out of scope |
| **ADDITIONAL INFORMATION** | Microsoft: Security Update Summary |

Back to top

## (MSPT-Oct2019) Microsoft Graphics Improperly Handle Objects In Memory Information Disclosure (CVE-2019-1361)

*MTIS19-047-V*

| | |
|---|---|
| **THREAT IDENTIFIER(S)** | CVE-2019-1361 |
| **THREAT TYPE** | Vulnerability |
| **RISK ASSESSMENT** | Medium |
| **MAIN THREAT VECTORS** | Web |
| **USER INTERACTION REQUIRED** | Yes |
| **DESCRIPTION** | A vulnerability in some versions of Microsoft Graphics 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 October 8, Microsoft released an update to address this vulnerability |
| **MCAFEE PRODUCT COVERAGE** | |
| DAT FILES | Under analysis |
| VIRUS SCAN ENTERPRISE SCAN BOP | Out of scope |
| HOST IPS | Out of scope |
| NETWORK SECURITY PLATFORM | Coverage not warranted |
| VULNERABILITY MANAGER | An upcoming FSL/MVM content release will contain coverage for this issue. |
| WEB GATEWAY | Under analysis |
| REMEDIATION MANAGER | Not applicable |
| POLICY AUDITOR | An upcoming SCAP content release will contain coverage for this issue. |
| NETWORK ACCESS CONTROL | An upcoming SCAP content release will contain coverage for this issue. |
| FIREWALL ENTERPRISE | Under analysis |
| APPLICATION CONTROL | Out of scope |
| DATABASE ACTIVITY MONITORING | Out of scope |
| VULNERABILITY MANAGER FOR DATABASES | Out of scope |
| **ADDITIONAL INFORMATION** | Microsoft: Security Update Summary |

Back to top

## (MSPT-Oct2019) Microsoft Windows Kernel-Mode Privilege Escalation (CVE-2019-1362)

*MTIS19-047-W*

| | |
|---|---|
| **THREAT IDENTIFIER(S)** | CVE-2019-1362 |
| **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 October 8, Microsoft released an update to address this vulnerability |
| **MCAFEE PRODUCT COVERAGE** | |
| DAT FILES | Under analysis |
| VIRUS SCAN ENTERPRISE SCAN BOP | Out of scope |
| HOST IPS | Out of scope |
| NETWORK SECURITY PLATFORM | Coverage not warranted |
| VULNERABILITY MANAGER | An upcoming FSL/MVM content release will contain coverage for this issue. |

| | |
|---|---|
| WEB GATEWAY | Under analysis |
| REMEDIATION MANAGER | Not applicable |
| POLICY AUDITOR | An upcoming SCAP content release will contain coverage for this issue. |
| NETWORK ACCESS CONTROL | An upcoming SCAP content release will contain coverage for this issue. |
| FIREWALL ENTERPRISE | Under analysis |
| APPLICATION CONTROL | Out of scope |
| DATABASE ACTIVITY MONITORING | Out of scope |
| VULNERABILITY MANAGER FOR DATABASES | Out of scope |
| **ADDITIONAL INFORMATION** | Microsoft: Security Update Summary |

Back to top

## (MSPT-Oct2019) Microsoft GDI Improperly Handles Objects In Memory Information Disclosure (CVE-2019-1363)

*MTIS19-047-X*

| | |
|---|---|
| **THREAT IDENTIFIER(S)** | CVE-2019-1363 |
| **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 GDI could lead to information disclosure. The flaw lies in the 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 October 8, Microsoft released an update to address this vulnerability |
| **MCAFEE PRODUCT COVERAGE** | |
| DAT FILES | Under analysis |
| VIRUS SCAN ENTERPRISE SCAN BOP | Out of scope |
| HOST IPS | Out of scope |
| NETWORK SECURITY PLATFORM | Coverage not warranted |
| VULNERABILITY MANAGER | An upcoming FSL/MVM content release will contain coverage for this issue. |
| WEB GATEWAY | Under analysis |
| REMEDIATION MANAGER | Not applicable |
| POLICY AUDITOR | An upcoming SCAP content release will contain coverage for this issue. |
| NETWORK ACCESS CONTROL | An upcoming SCAP content release will contain coverage for this issue. |
| FIREWALL ENTERPRISE | Under analysis |
| APPLICATION CONTROL | Out of scope |
| DATABASE ACTIVITY MONITORING | Out of scope |
| VULNERABILITY MANAGER FOR DATABASES | Out of scope |
| **ADDITIONAL INFORMATION** | Microsoft: Security Update Summary |

Back to top

## (MSPT-Oct2019) Microsoft Windows Kernel-mode Driver Privilege Escalation (CVE-2019-1364)

*MTIS19-047-Y*

| | |
|---|---|
| **THREAT IDENTIFIER(S)** | CVE-2019-1364 |
| **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 Driver 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 October 8, Microsoft released an update to address this vulnerability |
| **MCAFEE PRODUCT COVERAGE** | |
| DAT FILES | Under analysis |
| VIRUS SCAN ENTERPRISE SCAN BOP | Out of scope |
| HOST IPS | Out of scope |
| NETWORK SECURITY PLATFORM | Coverage not warranted |

| | |
|---|---|
| VULNERABILITY MANAGER | An upcoming FSL/MVM content release will contain coverage for this issue. |
| WEB GATEWAY | Under analysis |
| REMEDIATION MANAGER | Not applicable |
| POLICY AUDITOR | An upcoming SCAP content release will contain coverage for this issue. |
| NETWORK ACCESS CONTROL | An upcoming SCAP content release will contain coverage for this issue. |
| FIREWALL ENTERPRISE | Under analysis |
| APPLICATION CONTROL | Out of scope |
| DATABASE ACTIVITY MONITORING | Out of scope |
| VULNERABILITY MANAGER FOR DATABASES | Out of scope |
| **ADDITIONAL INFORMATION** | Microsoft: Security Update Summary |

Back to top

## (MSPT-Oct2019) Microsoft IIS Server Fails To Check The Length Of A Buffer Privilege Escalation (CVE-2019-1365)

*MTIS19-047-Z*

| | |
|---|---|
| **THREAT IDENTIFIER(S)** | CVE-2019-1365 |
| **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 IIS Server could lead to privilege escalation. The flaw lies in the fails to check the length of a buffer. Successful exploitation could allow a local user to gain elevated privileges. |
| **IMPORTANCE** | Medium. On October 8, Microsoft released an update to address this vulnerability |
| **MCAFEE PRODUCT COVERAGE** | |
| DAT FILES | Under analysis |
| VIRUS SCAN ENTERPRISE SCAN BOP | Out of scope |
| HOST IPS | Out of scope |
| NETWORK SECURITY PLATFORM | Coverage not warranted |
| VULNERABILITY MANAGER | An upcoming FSL/MVM content release will contain coverage for this issue. |
| WEB GATEWAY | Under analysis |
| REMEDIATION MANAGER | Not applicable |
| POLICY AUDITOR | An upcoming SCAP content release will contain coverage for this issue. |
| NETWORK ACCESS CONTROL | An upcoming SCAP content release will contain coverage for this issue. |
| FIREWALL ENTERPRISE | Under analysis |
| APPLICATION CONTROL | Out of scope |
| DATABASE ACTIVITY MONITORING | Out of scope |
| VULNERABILITY MANAGER FOR DATABASES | Out of scope |
| **ADDITIONAL INFORMATION** | Microsoft: Security Update Summary |

Back to top

---