EXECUTIVE SUMMARY
December 8, 2020 | MTIS20-060

Since the last McAfee® Labs Security Advisory (December 8), the following noteworthy event has taken place:
1. Patches are available for multiple Microsoft security vulnerabilities

NEW THREAT OVERVIEW

| (MSPT-Dec2020) Microsoft Windows Backup Engine Privilege Escalation (CVE-2020-16958) MTIS20-060-A |
| IMPORTANCE: Medium |
| COVERED PRODUCTS: Firewall Enterprise |

Back to top

| (MSPT-Dec2020) Microsoft Windows Backup Engine Privilege Escalation (CVE-2020-16959) MTIS20-060-B |
| IMPORTANCE: Medium |
| COVERED PRODUCTS: Firewall Enterprise |

Back to top

| (MSPT-Dec2020) Microsoft Windows Backup Engine Privilege Escalation (CVE-2020-16960) MTIS20-060-C |
| IMPORTANCE: Medium |
| COVERED PRODUCTS: Firewall Enterprise |

Back to top

| (MSPT-Dec2020) Microsoft Windows Backup Engine Privilege Escalation (CVE-2020-16961) MTIS20-060-D |
| IMPORTANCE: Medium |
| COVERED PRODUCTS: Firewall Enterprise |

Back to top

| IMPORTANCE: Medium |
| COVERED PRODUCTS: Firewall Enterprise |

Back to top
(MSPT-Dec2020) Microsoft Windows Backup Engine Privilege Escalation (CVE-2020-16963)

* MTIS20-060-F

**IMPORTANCE:** Medium

**COVERED PRODUCTS:** Firewall Enterprise

---

(MSPT-Dec2020) Microsoft Windows Backup Engine Privilege Escalation (CVE-2020-16964)

* MTIS20-060-G

**IMPORTANCE:** Medium

**COVERED PRODUCTS:** Firewall Enterprise

---

(MSPT-Dec2020) Microsoft Azure SDK Privilege Escalation (CVE-2020-16971)

* MTIS20-060-H

**IMPORTANCE:** Medium

**COVERED PRODUCTS:** Firewall Enterprise

---


* MTIS20-060-I

**IMPORTANCE:** Medium

**COVERED PRODUCTS:** Firewall Enterprise

---

(MSPT-Dec2020) Microsoft Azure SDK Privilege Escalation (CVE-2020-17002)

* MTIS20-060-J

**IMPORTANCE:** Medium

**COVERED PRODUCTS:** Firewall Enterprise

---

(MSPT-Dec2020) Microsoft Office SharePoint Privilege Escalation (CVE-2020-17089)

* MTIS20-060-K

**IMPORTANCE:** Medium

**COVERED PRODUCTS:** Firewall Enterprise

---

(MSPT-Dec2020) Microsoft Windows Network Connections Privilege Escalation (CVE-2020-17092)

* MTIS20-060-L

**IMPORTANCE:** Medium

**COVERED PRODUCTS:** Firewall Enterprise

---

(MSPT-Dec2020) Microsoft Windows Error Reporting Information Disclosure (CVE-2020-17094)

* MTIS20-060-M

**IMPORTANCE:** Medium

**COVERED PRODUCTS:** Firewall Enterprise
MTIS20-060-N
IMPORTANCE: High
COVERED PRODUCTS: Firewall Enterprise
UNDER ANALYSIS:

Back to top

(MSPT-Dec2020) Microsoft Windows NTFS Remote Code Execution (CVE-2020-17096)
MTIS20-060-O
IMPORTANCE: Medium
COVERED PRODUCTS: Firewall Enterprise
UNDER ANALYSIS: DAT | Web Gateway | Firewall Enterprise

Back to top

(MSPT-Dec2020) Microsoft Windows Media Privilege Escalation (CVE-2020-17097)
MTIS20-060-P
IMPORTANCE: Medium
COVERED PRODUCTS: Firewall Enterprise
UNDER ANALYSIS: DAT | Web Gateway | Firewall Enterprise

Back to top

MTIS20-060-Q
IMPORTANCE: Medium
COVERED PRODUCTS: Firewall Enterprise
UNDER ANALYSIS: DAT | Web Gateway | Firewall Enterprise

Back to top

(MSPT-Dec2020) Microsoft Windows Lock Screen Remote Code Execution (CVE-2020-17099)
MTIS20-060-R
IMPORTANCE: Medium
COVERED PRODUCTS: Firewall Enterprise
UNDER ANALYSIS: DAT | Web Gateway | Firewall Enterprise

Back to top

(MSPT-Dec2020) Microsoft Windows Cloud Files Mini Filter Driver Privilege Escalation (CVE-2020-17103)
MTIS20-060-S
IMPORTANCE: Medium
COVERED PRODUCTS: Firewall Enterprise
UNDER ANALYSIS: DAT | Web Gateway | Firewall Enterprise

Back to top

(MSPT-Dec2020) Microsoft Office SharePoint Spoofing Vulnerability (CVE-2020-17115)
MTIS20-060-T
IMPORTANCE: Low
COVERED PRODUCTS: Firewall Enterprise
UNDER ANALYSIS: DAT | Web Gateway | Firewall Enterprise

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

(September 2020) Microsoft Office SharePoint Remote Code Execution (CVE-2020-17118)

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

(September 2020) Microsoft Office Outlook Information Disclosure (CVE-2020-17119)

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

(September 2020) Microsoft Office SharePoint Information Disclosure (CVE-2020-17120)

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

(September 2020) Microsoft Office SharePoint Remote Code Execution (CVE-2020-17121)

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

(September 2020) Microsoft Office Excel Remote Code Execution (CVE-2020-17122)

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

---

**THREAT DETAILS**

(September 2020) Microsoft Windows Backup Engine Privilege Escalation (CVE-2020-16958)

**THREAT IDENTIFIER(S):** CVE-2020-16958
**THREAT TYPE:** Vulnerability
**RISK ASSESSMENT:** Medium
**MAIN THREAT VECTORS:** Locally logged-on user
**USER INTERACTION REQUIRED:** No
A vulnerability in some versions of Microsoft Windows could lead to privilege escalation. The flaw lies in the Backup Engine component. Successful exploitation could allow a local user to gain elevated privileges.

**IMPORTANCE**
Medium. On December 8, Microsoft released an update to address this vulnerability

**MCAFEE PRODUCT COVERAGE**
- **DAT FILES**: Out of scope
- **VIRUS SCAN ENTERPRISE SCAN BOP**: Out of scope
- **HOST IPS**: Out of scope
- **NETWORK SECURITY PLATFORM**: Coverage not warranted
- **VULNERABILITY MANAGER**: An upcoming FSL/MVM content release will contain coverage for this issue.
- **WEB GATEWAY**: Out of scope
- **REMEDIATION MANAGER**: Not applicable
- **POLICY AUDITOR**: An upcoming SCAP content release will contain coverage for this issue.
- **NETWORK ACCESS CONTROL**: An upcoming SCAP content release will contain coverage for this issue.
- **FIREWALL ENTERPRISE**: Under analysis
- **APPLICATION CONTROL**: Out of scope
- **DATABASE ACTIVITY MONITORING**: Out of scope
- **VULNERABILITY MANAGER FOR DATABASES**: Out of scope

**ADDITIONAL INFORMATION**
Microsoft: Security Update Summary
A vulnerability in some versions of Microsoft Windows could lead to privilege escalation. The flaw lies in the Backup Engine component. Successful exploitation could allow a local user to gain elevated privileges.

Microsoft: Security Update Summary
### (MSPT-Dec2020) Microsoft Windows Backup Engine Privilege Escalation (CVE-2020-16962)

**THREAT IDENTIFIER(S)**
- CVE-2020-16962

**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 Backup Engine component. Successful exploitation could allow a local user to gain elevated privileges.

**IMPORTANCE**

Medium. On December 8, Microsoft released an update to address this vulnerability

**MCAFEE PRODUCT COVERAGE**

<table>
<thead>
<tr>
<th>Component</th>
<th>Coverage</th>
</tr>
</thead>
<tbody>
<tr>
<td>DAT FILES</td>
<td>Out of scope</td>
</tr>
<tr>
<td>VIRUS SCAN ENTERPRISE SCAN BOP</td>
<td>Out of scope</td>
</tr>
<tr>
<td>HOST IPS</td>
<td>Out of scope</td>
</tr>
<tr>
<td>NETWORK SECURITY PLATFORM</td>
<td>Coverage not warranted</td>
</tr>
<tr>
<td>VULNERABILITY MANAGER</td>
<td>An upcoming FSL/MVM content release will contain coverage for this issue.</td>
</tr>
<tr>
<td>WEB GATEWAY</td>
<td>Out of scope</td>
</tr>
<tr>
<td>REMEDIATION MANAGER</td>
<td>Not applicable</td>
</tr>
<tr>
<td>POLICY AUDITOR</td>
<td>An upcoming SCAP content release will contain coverage for this issue.</td>
</tr>
<tr>
<td>NETWORK ACCESS CONTROL</td>
<td>An upcoming SCAP content release will contain coverage for this issue.</td>
</tr>
<tr>
<td>FIREWALL ENTERPRISE</td>
<td>Under analysis</td>
</tr>
<tr>
<td>APPLICATION CONTROL</td>
<td>Out of scope</td>
</tr>
<tr>
<td>DATABASE ACTIVITY MONITORING</td>
<td>Out of scope</td>
</tr>
<tr>
<td>VULNERABILITY MANAGER FOR DATABASES</td>
<td>Out of scope</td>
</tr>
</tbody>
</table>

### (MSPT-Dec2020) Microsoft Windows Backup Engine Privilege Escalation (CVE-2020-16963)

**THREAT IDENTIFIER(S)**
- CVE-2020-16963

**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 Backup Engine component. Successful exploitation could allow a local user to gain elevated privileges.

**IMPORTANCE**

Medium. On December 8, Microsoft released an update to address this vulnerability

**MCAFEE PRODUCT COVERAGE**

<table>
<thead>
<tr>
<th>Component</th>
<th>Coverage</th>
</tr>
</thead>
<tbody>
<tr>
<td>DAT FILES</td>
<td>Out of scope</td>
</tr>
<tr>
<td>VIRUS SCAN ENTERPRISE SCAN BOP</td>
<td>Out of scope</td>
</tr>
<tr>
<td>HOST IPS</td>
<td>Out of scope</td>
</tr>
<tr>
<td>NETWORK SECURITY PLATFORM</td>
<td>Coverage not warranted</td>
</tr>
<tr>
<td>VULNERABILITY MANAGER</td>
<td>An upcoming FSL/MVM content release will contain coverage for this issue.</td>
</tr>
<tr>
<td>WEB GATEWAY</td>
<td>Out of scope</td>
</tr>
<tr>
<td>REMEDIATION MANAGER</td>
<td>Not applicable</td>
</tr>
<tr>
<td>POLICY AUDITOR</td>
<td>An upcoming SCAP content release will contain coverage for this issue.</td>
</tr>
</tbody>
</table>
An upcoming SCAP content release will contain coverage for this issue.

Under analysis

Out of scope

Out of scope

Out of scope

Microsoft: Security Update Summary

(MSPT-Dec2020) Microsoft Windows Backup Engine Privilege Escalation (CVE-2020-16964)

MTIS20-060-G

THREAT IDENTIFIER(S) CVE-2020-16964

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 Backup Engine component. Successful exploitation could allow a local user to gain elevated privileges.

IMPORTANCE Medium. On December 8, Microsoft released an update to address this vulnerability

MCAFEE PRODUCT COVERAGE

DAT FILES Out of scope

VIRUS SCAN ENTERPRISE SCAN BOP Out of scope

HOST IPS Out of scope

NETWORK SECURITY PLATFORM Coverage not warranted

VULNERABILITY MANAGER An upcoming FSL/MVM content release will contain coverage for this issue.

WEB GATEWAY Out of scope

REMEDICATION 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

(MSPT-Dec2020) Microsoft Azure SDK Privilege Escalation (CVE-2020-16971)

MTIS20-060-H

THREAT IDENTIFIER(S) CVE-2020-16971

THREAT TYPE Vulnerability

RISK ASSESSMENT Medium

MAIN THREAT VECTORS Web

USER INTERACTION REQUIRED No

DESCRIPTION A vulnerability in some versions of Microsoft Azure could lead to privilege escalation. The flaw lies in the SDK component. Successful exploitation could allow a local user to gain elevated privileges.

IMPORTANCE Medium. On December 8, Microsoft released an update to address this vulnerability

MCAFEE PRODUCT COVERAGE

DAT FILES Out of scope

VIRUS SCAN ENTERPRISE SCAN BOP Out of scope

HOST IPS Out of scope
### (MSPT-Dec2020) Microsoft Windows Kerberos Remote Code Execution (CVE-2020-16996)

**Threat Identifier(s):** CVE-2020-16996  
**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 remote code execution. The flaw lies in the Kerberos component. Successful exploitation by a remote attacker could result in the execution of arbitrary code.

**Importance:** Medium. On December 8, Microsoft released an update to address this vulnerability.
<table>
<thead>
<tr>
<th><strong>VULNERABILITY MANAGER</strong></th>
<th>An upcoming FSL/MVM content release will contain coverage for this issue.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>WEB GATEWAY</strong></td>
<td>Out of scope</td>
</tr>
<tr>
<td><strong>REMEDICATION MANAGER</strong></td>
<td>Not applicable</td>
</tr>
<tr>
<td><strong>POLICY AUDITOR</strong></td>
<td>An upcoming SCAP content release will contain coverage for this issue.</td>
</tr>
<tr>
<td><strong>NETWORK ACCESS CONTROL</strong></td>
<td>An upcoming SCAP content release will contain coverage for this issue.</td>
</tr>
<tr>
<td><strong>FIREWALL ENTERPRISE</strong></td>
<td>Under analysis</td>
</tr>
<tr>
<td><strong>APPLICATION CONTROL</strong></td>
<td>Out of scope</td>
</tr>
<tr>
<td><strong>DATABASE ACTIVITY MONITORING</strong></td>
<td>Out of scope</td>
</tr>
<tr>
<td><strong>VULNERABILITY MANAGER FOR DATABASES</strong></td>
<td>Out of scope</td>
</tr>
</tbody>
</table>

**ADDITIONAL INFORMATION**

Microsoft: Security Update Summary
A vulnerability in some versions of Microsoft Windows could lead to privilege escalation. The flaw lies in the Network Connections component. Successful exploitation could allow a local user to gain elevated privileges.

**Importance**
Medium. On December 8, Microsoft released an update to address this vulnerability.

**MCAFEE PRODUCT COVERAGE**
- DAT FILES: Out of scope
- VIRUS SCAN ENTERPRISE SCAN BOP: Out of scope
- HOST IPS: Out of scope
- NETWORK SECURITY PLATFORM: Coverage not warranted
- VULNERABILITY MANAGER: An upcoming FSL/MVM content release will contain coverage for this issue.
- WEB GATEWAY: Out of scope
- REMEDIATION MANAGER: Not applicable
- POLICY AUDITOR: An upcoming SCAP content release will contain coverage for this issue.
- NETWORK ACCESS CONTROL: An upcoming SCAP content release will contain coverage for this issue.
- FIREWALL ENTERPRISE: Under analysis
- APPLICATION CONTROL: Out of scope
- DATABASE ACTIVITY MONITORING: Out of scope
- VULNERABILITY MANAGER FOR DATABASES: Out of scope

**ADDITIONAL INFORMATION**
Microsoft: Security Update Summary

---

A vulnerability in some versions of Microsoft Windows could lead to information disclosure. The flaw lies in the Error Reporting component. Successful exploitation by an attacker could result in the disclosure of sensitive information.

**Importance**
Medium. On December 8, Microsoft released an update to address this vulnerability.

**MCAFEE PRODUCT COVERAGE**
- DAT FILES: Out of scope
- VIRUS SCAN ENTERPRISE SCAN BOP: Out of scope
- HOST IPS: Out of scope
- NETWORK SECURITY PLATFORM: Coverage not warranted
- VULNERABILITY MANAGER: An upcoming FSL/MVM content release will contain coverage for this issue.
- WEB GATEWAY: Out of scope
- REMEDIATION MANAGER: Not applicable
- POLICY AUDITOR: An upcoming SCAP content release will contain coverage for this issue.
- NETWORK ACCESS CONTROL: An upcoming SCAP content release will contain coverage for this issue.
- FIREWALL ENTERPRISE: Under analysis
- APPLICATION CONTROL: Out of scope
- DATABASE ACTIVITY MONITORING: Out of scope
- VULNERABILITY MANAGER FOR DATABASES: Out of scope

**ADDITIONAL INFORMATION**
Microsoft: Security Update Summary
### (MSPT-Dec2020) Microsoft Windows Hyper-V Remote Code Execution (CVE-2020-17095)

**MTIS20-060-N**

<table>
<thead>
<tr>
<th><strong>THREAT IDENTIFIER(S)</strong></th>
<th>CVE-2020-17095</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>THREAT TYPE</strong></td>
<td>Vulnerability</td>
</tr>
<tr>
<td><strong>RISK ASSESSMENT</strong></td>
<td>High</td>
</tr>
<tr>
<td><strong>MAIN THREAT VECTORS</strong></td>
<td>Web</td>
</tr>
<tr>
<td><strong>USER INTERACTION REQUIRED</strong></td>
<td>No</td>
</tr>
</tbody>
</table>

**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.

**IMPORTANCE**

High. On December 8, Microsoft released an update to address this vulnerability.

**MCAFEE PRODUCT COVERAGE**

<table>
<thead>
<tr>
<th>DAT FILES</th>
<th>Out of scope</th>
</tr>
</thead>
<tbody>
<tr>
<td>VIRUS SCAN ENTERPRISE SCAN BOP</td>
<td>Out of scope</td>
</tr>
<tr>
<td>HOST IPS</td>
<td>Out of scope</td>
</tr>
<tr>
<td>NETWORK SECURITY PLATFORM</td>
<td>Coverage not warranted</td>
</tr>
<tr>
<td>VULNERABILITY MANAGER</td>
<td>An upcoming FSL/MVM content release will contain coverage for this issue.</td>
</tr>
<tr>
<td>WEB GATEWAY</td>
<td>Out of scope</td>
</tr>
<tr>
<td>REMEDIATION MANAGER</td>
<td>Not applicable</td>
</tr>
<tr>
<td>POLICY AUDITOR</td>
<td>An upcoming SCAP content release will contain coverage for this issue.</td>
</tr>
<tr>
<td>NETWORK ACCESS CONTROL</td>
<td>An upcoming SCAP content release will contain coverage for this issue.</td>
</tr>
<tr>
<td>FIREWALL ENTERPRISE</td>
<td>Under analysis</td>
</tr>
<tr>
<td>APPLICATION CONTROL</td>
<td>Out of scope</td>
</tr>
<tr>
<td>DATABASE ACTIVITY MONITORING</td>
<td>Out of scope</td>
</tr>
<tr>
<td>VULNERABILITY MANAGER FOR DATABASES</td>
<td>Out of scope</td>
</tr>
</tbody>
</table>

**ADDITIONAL INFORMATION**

Microsoft: Security Update Summary

### (MSPT-Dec2020) Microsoft Windows NTFS Remote Code Execution (CVE-2020-17096)

**MTIS20-060-O**

<table>
<thead>
<tr>
<th><strong>THREAT IDENTIFIER(S)</strong></th>
<th>CVE-2020-17096</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>THREAT TYPE</strong></td>
<td>Vulnerability</td>
</tr>
<tr>
<td><strong>RISK ASSESSMENT</strong></td>
<td>Medium</td>
</tr>
<tr>
<td><strong>MAIN THREAT VECTORS</strong></td>
<td>Web</td>
</tr>
<tr>
<td><strong>USER INTERACTION REQUIRED</strong></td>
<td>No</td>
</tr>
</tbody>
</table>

**DESCRIPTION**

A vulnerability in some versions of Microsoft Windows could lead to remote code execution. The flaw lies in the NTFS component. Successful exploitation by a remote attacker could result in the execution of arbitrary code.

**IMPORTANCE**

Medium. On December 8, Microsoft released an update to address this vulnerability.

**MCAFEE PRODUCT COVERAGE**

<table>
<thead>
<tr>
<th>DAT FILES</th>
<th>Under analysis</th>
</tr>
</thead>
<tbody>
<tr>
<td>VIRUS SCAN ENTERPRISE SCAN BOP</td>
<td>Out of scope</td>
</tr>
<tr>
<td>HOST IPS</td>
<td>Out of scope</td>
</tr>
<tr>
<td>NETWORK SECURITY PLATFORM</td>
<td>Coverage not warranted</td>
</tr>
<tr>
<td>VULNERABILITY MANAGER</td>
<td>An upcoming FSL/MVM content release will contain coverage for this issue.</td>
</tr>
<tr>
<td>WEB GATEWAY</td>
<td>Under analysis</td>
</tr>
<tr>
<td>REMEDIATION MANAGER</td>
<td>Not applicable</td>
</tr>
<tr>
<td>POLICY AUDITOR</td>
<td>An upcoming SCAP content release will contain coverage for this issue.</td>
</tr>
<tr>
<td>NETWORK ACCESS CONTROL</td>
<td>An upcoming SCAP content release will contain coverage for this issue.</td>
</tr>
<tr>
<td>FIREWALL ENTERPRISE</td>
<td>Under analysis</td>
</tr>
</tbody>
</table>
(MSPT-Dec2020) Microsoft Windows Media Privilege Escalation (CVE-2020-17097)

**THREAT IDENTIFIER(S)**
CVE-2020-17097

**THREAT TYPE**
Vulnerability

**RISK ASSESSMENT**
Medium

**MAIN THREAT VECTORS**
Web

**USER INTERACTION REQUIRED**
No

**DESCRIPTION**
A vulnerability in some versions of Microsoft Windows could lead to privilege escalation. The flaw lies in the Media component. Successful exploitation could allow a local user to gain elevated privileges.

**IMPORTANCE**
Medium. On December 8, Microsoft released an update to address this vulnerability

**MCAFEE PRODUCT COVERAGE**

<table>
<thead>
<tr>
<th>DAT FILES</th>
<th>Under analysis</th>
</tr>
</thead>
<tbody>
<tr>
<td>VIRUS SCAN ENTERPRISE SCAN BOP</td>
<td>Out of scope</td>
</tr>
<tr>
<td>HOST IPS</td>
<td>Out of scope</td>
</tr>
<tr>
<td>NETWORK SECURITY PLATFORM</td>
<td>Coverage not warranted</td>
</tr>
<tr>
<td>VULNERABILITY MANAGER</td>
<td>An upcoming FSL/MVM content release will contain coverage for this issue.</td>
</tr>
<tr>
<td>WEB GATEWAY</td>
<td>Under analysis</td>
</tr>
<tr>
<td>REMEDIATION MANAGER</td>
<td>Not applicable</td>
</tr>
<tr>
<td>POLICY AUDITOR</td>
<td>An upcoming SCAP content release will contain coverage for this issue.</td>
</tr>
<tr>
<td>NETWORK ACCESS CONTROL</td>
<td>An upcoming SCAP content release will contain coverage for this issue.</td>
</tr>
<tr>
<td>FIREWALL ENTERPRISE</td>
<td>Under analysis</td>
</tr>
<tr>
<td>APPLICATION CONTROL</td>
<td>Out of scope</td>
</tr>
<tr>
<td>DATABASE ACTIVITY MONITORING</td>
<td>Out of scope</td>
</tr>
<tr>
<td>VULNERABILITY MANAGER FOR DATABASES</td>
<td>Out of scope</td>
</tr>
</tbody>
</table>

**ADDITIONAL INFORMATION**
Microsoft: Security Update Summary

---


**THREAT IDENTIFIER(S)**
CVE-2020-17098

**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 Graphics component. Successful exploitation by a remote attacker could result in the disclosure of sensitive information.

**IMPORTANCE**
Medium. On December 8, Microsoft released an update to address this vulnerability

**MCAFEE PRODUCT COVERAGE**

<table>
<thead>
<tr>
<th>DAT FILES</th>
<th>Under analysis</th>
</tr>
</thead>
<tbody>
<tr>
<td>VIRUS SCAN ENTERPRISE SCAN BOP</td>
<td>Out of scope</td>
</tr>
<tr>
<td>HOST IPS</td>
<td>Out of scope</td>
</tr>
<tr>
<td>NETWORK SECURITY PLATFORM</td>
<td>Coverage not warranted</td>
</tr>
<tr>
<td>VULNERABILITY MANAGER</td>
<td>An upcoming FSL/MVM content release will contain coverage for this issue.</td>
</tr>
</tbody>
</table>

**ADDITIONAL INFORMATION**
Microsoft: Security Update Summary
(MSPT-Dec2020) Microsoft Windows Lock Screen Remote Code Execution (CVE-2020-17099)

**MTIS20-060-R**

**THREAT IDENTIFIER(S)**
CVE-2020-17099

**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 remote code execution. The flaw lies in the Lock Screen component. Successful exploitation by a remote attacker could result in the execution of arbitrary code.

**IMPORTANCE**
Medium. On December 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
- **REMEDICATION 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-Dec2020) Microsoft Windows Cloud Files Mini Filter Driver Privilege Escalation (CVE-2020-17103)

**MTIS20-060-S**

**THREAT IDENTIFIER(S)**
CVE-2020-17103

**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 Cloud Files Mini Filter Driver component. Successful exploitation could allow a local user to gain elevated privileges.

**IMPORTANCE**
Medium. On December 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
- **REMEDICATION 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-Dec2020) Microsoft Office SharePoint Spoofing Vulnerability (CVE-2020-17115)

**THREAT IDENTIFIER(S)**
CVE-2020-17115

**THREAT TYPE**
Vulnerability

**RISK ASSESSMENT**
Low

**MAIN THREAT VECTORS**
Web

**USER INTERACTION REQUIRED**
No

**DESCRIPTION**
A vulnerability in some versions of Microsoft Office could lead to spoofing. The flaw lies in the SharePoint component. Successful exploitation by a remote attacker could result in the spoofing vulnerability.

**IMPORTANCE**
Low. On December 8, Microsoft released an update to address this vulnerability.


**THREAT IDENTIFIER(S)**
CVE-2020-17117

**THREAT TYPE**
Vulnerability

**RISK ASSESSMENT**
High

**MAIN THREAT VECTORS**
Web
A vulnerability in some versions of Microsoft Windows could lead to remote code execution. The flaw lies in the Exchange Server component. Successful exploitation by a remote attacker could result in the execution of arbitrary code.

High. On December 8, Microsoft released an update to address this vulnerability

Microsoft: Security Update Summary
A vulnerability in some versions of Microsoft Office could lead to information disclosure. The flaw lies in the Outlook component. Successful exploitation by a remote attacker could result in the disclosure of sensitive information.

Importance: Medium. On December 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-Dec2020) Microsoft Office SharePoint Information Disclosure (CVE-2020-17120)

THREAT IDENTIFIER(S): CVE-2020-17120
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 information disclosure. The flaw lies in the SharePoint component. Successful exploitation by a remote attacker could result in the disclosure of sensitive information.
IMPORTANCE: Medium. On December 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
(MSPT-Dec2020) Microsoft Office SharePoint Remote Code Execution (CVE-2020-17121)

**THREAT IDENTIFIER(S)**
CVE-2020-17121

**THREAT TYPE**
Vulnerability

**RISK ASSESSMENT**
High

**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 SharePoint component. Successful exploitation by a remote attacker could result in the execution of arbitrary code.

**IMPORTANCE**
High. On December 8, Microsoft released an update to address this vulnerability

**MCAFEE PRODUCT COVERAGE**

<table>
<thead>
<tr>
<th>Component</th>
<th>Coverage</th>
</tr>
</thead>
<tbody>
<tr>
<td>DAT FILES</td>
<td>Under analysis</td>
</tr>
<tr>
<td>VIRUS SCAN ENTERPRISE SCAN BOP</td>
<td>Out of scope</td>
</tr>
<tr>
<td>HOST IPS</td>
<td>Out of scope</td>
</tr>
<tr>
<td>NETWORK SECURITY PLATFORM</td>
<td>Coverage not warranted</td>
</tr>
<tr>
<td>VULNERABILITY MANAGER</td>
<td>An upcoming FSL/MVM content release will contain coverage for this issue.</td>
</tr>
<tr>
<td>WEB GATEWAY</td>
<td>Under analysis</td>
</tr>
<tr>
<td>REMEDIATION MANAGER</td>
<td>Not applicable</td>
</tr>
<tr>
<td>POLICY AUDITOR</td>
<td>An upcoming SCAP content release will contain coverage for this issue.</td>
</tr>
<tr>
<td>NETWORK ACCESS CONTROL</td>
<td>An upcoming SCAP content release will contain coverage for this issue.</td>
</tr>
<tr>
<td>FIREWALL ENTERPRISE</td>
<td>Under analysis</td>
</tr>
<tr>
<td>APPLICATION CONTROL</td>
<td>Out of scope</td>
</tr>
<tr>
<td>DATABASE ACTIVITY MONITORING</td>
<td>Out of scope</td>
</tr>
<tr>
<td>VULNERABILITY MANAGER FOR DATABASES</td>
<td>Out of scope</td>
</tr>
</tbody>
</table>

**ADDITIONAL INFORMATION**
Microsoft: Security Update Summary
An upcoming SCAP content release will contain coverage for this issue.

Under analysis

Out of scope

Out of scope

Out of scope

Microsoft: Security Update Summary