EXECUTIVE SUMMARY
December 8, 2020 | MTIS20-061

Since the last McAfee® Labs Security Advisory (December 8), the following noteworthy event has taken place:

- Patches are available for multiple Microsoft security vulnerabilities

NEW THREAT OVERVIEW

(MSPT-Dec2020) Microsoft Office Excel Remote Code Execution (CVE-2020-17123)
MTIS20-061-A
IMPORTANCE: Medium
COVERED PRODUCTS: DAT | Web Gateway | Firewall Enterprise
UNDER ANALYSIS: DAT | Web Gateway | Firewall Enterprise

Back to top

(MSPT-Dec2020) Microsoft Office PowerPoint Remote Code Execution (CVE-2020-17124)
MTIS20-061-B
IMPORTANCE: Medium
COVERED PRODUCTS: DAT | Web Gateway | Firewall Enterprise
UNDER ANALYSIS: DAT | Web Gateway | Firewall Enterprise

Back to top

(MSPT-Dec2020) Microsoft Office Excel Remote Code Execution (CVE-2020-17125)
MTIS20-061-C
IMPORTANCE: Medium
COVERED PRODUCTS: Firewall Enterprise
UNDER ANALYSIS: Firewall Enterprise

Back to top

(MSPT-Dec2020) Microsoft Office Excel Information Disclosure (CVE-2020-17126)
MTIS20-061-D
IMPORTANCE: Medium
COVERED PRODUCTS: Firewall Enterprise
UNDER ANALYSIS: Firewall Enterprise

Back to top

(MSPT-Dec2020) Microsoft Office Excel Remote Code Execution (CVE-2020-17127)
MTIS20-061-E
IMPORTANCE: Medium
COVERED PRODUCTS: Firewall Enterprise
UNDER ANALYSIS: Firewall Enterprise
(MSPT-Dec2020) Microsoft Office Excel Remote Code Execution (CVE-2020-17128)

MTIS20-061-F

IMPORTANCE: Medium
COVERED PRODUCTS: Firewall Enterprise
UNDER ANALYSIS:

Back to top

(MSPT-Dec2020) Microsoft Office Excel Remote Code Execution (CVE-2020-17129)

MTIS20-061-G

IMPORTANCE: Medium
COVERED PRODUCTS: Firewall Enterprise
UNDER ANALYSIS:

Back to top

(MSPT-Dec2020) Microsoft Office Excel Remote Code Execution (CVE-2020-17130)

MTIS20-061-H

IMPORTANCE: Medium
COVERED PRODUCTS: Firewall Enterprise
UNDER ANALYSIS:

Back to top

(MSPT-Dec2020) Microsoft Edge Chakra Scripting Engine Remote Code Execution (CVE-2020-17131)

MTIS20-061-I

IMPORTANCE: High
COVERED PRODUCTS: Firewall Enterprise
UNDER ANALYSIS:

Back to top


MTIS20-061-J

IMPORTANCE: High
COVERED PRODUCTS: Firewall Enterprise
UNDER ANALYSIS:

Back to top

(MSPT-Dec2020) Microsoft Dynamics Business Central/NAV Information Disclosure (CVE-2020-17133)

MTIS20-061-K

IMPORTANCE: Medium
COVERED PRODUCTS: Firewall Enterprise
UNDER ANALYSIS:

Back to top

(MSPT-Dec2020) Microsoft Windows Overlay Filter Security Feature Privilege Escalation (CVE-2020-17134)

MTIS20-061-L

IMPORTANCE: Medium
COVERED PRODUCTS: Firewall Enterprise
UNDER ANALYSIS:

Back to top

(MSPT-Dec2020) Microsoft Azure DevOps Server Spoofing (CVE-2020-17135)

MTIS20-061-M
(MSPT-Dec2020) Microsoft Windows Cloud Files Mini Filter Driver Privilege Escalation (CVE-2020-17136)  
IMPORTANCE: Medium  
COVERED PRODUCTS: Firewall Enterprise  
UNDER ANALYSIS:  

Back to top

(MSPT-Dec2020) Microsoft DirectX Graphics Kernel Privilege Escalation (CVE-2020-17137)  
IMPORTANCE: Medium  
COVERED PRODUCTS: Firewall Enterprise  
UNDER ANALYSIS:  

Back to top

(MSPT-Dec2020) Microsoft Windows Error Reporting Information Disclosure (CVE-2020-17138)  
IMPORTANCE: Medium  
COVERED PRODUCTS: Firewall Enterprise  
UNDER ANALYSIS:  

Back to top

IMPORTANCE: Medium  
COVERED PRODUCTS: Firewall Enterprise  
UNDER ANALYSIS:  

Back to top

(MSPT-Dec2020) Microsoft Windows SMB Information Disclosure (CVE-2020-17140)  
IMPORTANCE: Medium  
COVERED PRODUCTS: DAT | Web Gateway | Firewall Enterprise  
UNDER ANALYSIS:  

Back to top

IMPORTANCE: Medium  
COVERED PRODUCTS: Firewall Enterprise  
UNDER ANALYSIS:  

Back to top

IMPORTANCE: High  
COVERED PRODUCTS: Firewall Enterprise  
UNDER ANALYSIS:  

Back to top
(MSPT-Dec2020) Microsoft Windows Exchange Server Information Disclosure (CVE-2020-17143)

IMPORTANCE: Medium
COVERED PRODUCTS: Firewall Enterprise


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

(MSPT-Dec2020) Microsoft Azure DevOps Server and Team Foundation Services Spoofing (CVE-2020-17145)

IMPORTANCE: Medium
COVERED PRODUCTS: Firewall Enterprise

(MSPT-Dec2020) Microsoft Dynamics CRM Webclient Spoofing (CVE-2020-17147)

IMPORTANCE: Medium
COVERED PRODUCTS: Firewall Enterprise


IMPORTANCE: Medium
COVERED PRODUCTS: Firewall Enterprise


IMPORTANCE: Medium
COVERED PRODUCTS: Firewall Enterprise

THREAT DETAILS

(MSPT-Dec2020) Microsoft Office Excel Remote Code Execution (CVE-2020-17123)

THREAT IDENTIFIER(S) CVE-2020-17123
THREAT TYPE Vulnerability
RISK ASSESSMENT Medium
MAIN THREAT VECTORS Web
USER INTERACTION REQUIRED No
A vulnerability in some versions of Microsoft Office could lead to remote code execution. The flaw lies in the Excel component. Successful exploitation by an 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
- **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

---


**THREAT IDENTIFIER(S)**
CVE-2020-17124

**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 PowerPoint component. Successful exploitation by an 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
- **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

---


**MTIS20-061-C**
## Threat Identifier(s)
- CVE-2020-17125

## 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 Excel component. Successful exploitation by an 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>Category</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>

### Additional Information
- Microsoft: Security Update Summary

---

(MSPT-Dec2020) Microsoft Office Excel Information Disclosure (CVE-2020-17126)

### Threat Identifier(s)
- CVE-2020-17126

### 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 Excel 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.
### (MSPT-Dec2020) Microsoft Office Excel Remote Code Execution (CVE-2020-17127)

**Threat Identifier(s):** CVE-2020-17127  
**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 Excel component. Successful exploitation by an 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>Product</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>

**Additional Information:**

Microsoft: Security Update Summary

---

### (MSPT-Dec2020) Microsoft Office Excel Remote Code Execution (CVE-2020-17128)

**Threat Identifier(s):** CVE-2020-17128  
**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 Excel component. Successful exploitation by an 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>Product</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>

**Additional Information:**

Microsoft: Security Update Summary
**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**

(\textit{MSPT-Dec2020}) Microsoft Office Excel Remote Code Execution (CVE-2020-17129)

\textit{MTIS20-061-G}

**THREAT IDENTIFIER(S)**
CVE-2020-17129

**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 Excel component. Successful exploitation by an 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>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

---

**Back to top**

(\textit{MSPT-Dec2020}) Microsoft Office Excel Remote Code Execution (CVE-2020-17130)

\textit{MTIS20-061-H}

**THREAT IDENTIFIER(S)**
CVE-2020-17130

**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 Excel component. Successful exploitation by an 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>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>
</tbody>
</table>

---

Security Advisory MTIS20-061 - Page 8 of 19
Back to top

(MSPT-Dec2020) Microsoft Edge Chakra Scripting Engine Remote Code Execution (CVE-2020-17131)

MTIS20-061-I

THREAT IDENTIFIER(S)  CVE-2020-17131
THREAT TYPE  Vulnerability
RISK ASSESSMENT  High
MAIN THREAT VECTORS  Web
USER INTERACTION REQUIRED  No
DESCRIPTION  A vulnerability in some versions of Microsoft Edge could lead to remote code execution. The flaw lies in the Chakra Scripting Engine 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

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

Back to top


MTIS20-061-J

THREAT IDENTIFIER(S)  CVE-2020-17132
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 Exchange Server component. Successful exploitation by a remote attacker could result in the execution of arbitrary code.
### (MSPT-Dec2020) Microsoft Dynamics Business Central/NAV Information Disclosure (CVE-2020-17133)

**THREAT IDENTIFIER(S)**  
CVE-2020-17133

**THREAT TYPE**  
Vulnerability

**RISK ASSESSMENT**  
Medium

**MAIN THREAT VECTORS**  
Web

**USER INTERACTION REQUIRED**  
No

**DESCRIPTION**  
A vulnerability in some versions of Microsoft Dynamics could lead to information disclosure. The flaw lies in the Business Central/NAV 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>Feature</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>

### ADDITIONAL INFORMATION

Microsoft: Security Update Summary

---

### (MSPT-Dec2020) Microsoft Windows Overlay Filter Security Feature Privilege Escalation (CVE-2020-17134)

**THREAT IDENTIFIER(S)**  
CVE-2020-17134

---

Security Advisory MTIS20-061 - Page 10 of 19
### A vulnerability in some versions of Microsoft Windows could lead to privilege escalation. The flaw lies in the Overlay Filter Security Feature 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 Azure could lead to spoofing. The flaw lies in the DevOps Server component. Successful exploitation by a remote attacker could result in spoofing.**

**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

---

**THREAT IDENTIFIER(S)**
CVE-2020-17135

**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 spoofing. The flaw lies in the DevOps Server component. Successful exploitation by a remote attacker could result in spoofing.

**ADDITIONAL INFORMATION**
Microsoft: Security Update Summary

---

**Back to top**
Microsoft Windows Cloud Files Mini Filter Driver Privilege Escalation (CVE-2020-17136)

THREAT IDENTIFIER(S) | CVE-2020-17136
---|---
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 | 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 | 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

Microsoft DirectX Graphics Kernel Privilege Escalation (CVE-2020-17137)

THREAT IDENTIFIER(S) | CVE-2020-17137
---|---
THREAT TYPE | Vulnerability
RISK ASSESSMENT | Medium
MAIN THREAT VECTORS | Web
USER INTERACTION REQUIRED | No
DESCRIPTION | A vulnerability in some versions of Microsoft DirectX could lead to privilege escalation. The flaw lies in the Graphics Kernel 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
### (MSPT-Dec2020) Microsoft Windows Error Reporting Information Disclosure (CVE-2020-17138)

**THREAT IDENTIFIER(S)**
CVE-2020-17138

**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 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**

<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

**THREAT IDENTIFIER(S)**
CVE-2020-17140

**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 SMB 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**
  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

MTIS20-061-T

**THREAT IDENTIFIER(S)**
CVE-2020-17142

**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 Exchange Server 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

---

(MSPT-Dec2020) Microsoft Windows Exchange Server Information Disclosure (CVE-2020-17143)

MTIS20-061-U

**THREAT IDENTIFIER(S)**
CVE-2020-17143

**THREAT TYPE**
Vulnerability

**RISK ASSESSMENT**
Medium

**MAIN THREAT VECTORS**
Web
A vulnerability in some versions of Microsoft Windows could lead to information disclosure. The flaw lies in the Exchange Server 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>Category</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>

**ADDITIONAL INFORMATION**
Microsoft: Security Update Summary

---

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.

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

**MCAFEE PRODUCT COVERAGE**

<table>
<thead>
<tr>
<th>Category</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
### THREAT IDENTIFIER(S)
CVE-2020-17145

### 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 spoofing. The flaw lies in the DevOps Server and Team Foundation Services component. Successful exploitation by a remote attacker could result in spoofing.

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

### MCAFEE PRODUCT COVERAGE

<table>
<thead>
<tr>
<th>Category</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>

### ADDITIONAL INFORMATION
Microsoft: Security Update Summary

---

### THREAT IDENTIFIER(S)
CVE-2020-17147

### THREAT TYPE
Vulnerability

### RISK ASSESSMENT
Medium

### MAIN THREAT VECTORS
Web

### USER INTERACTION REQUIRED
No

### DESCRIPTION
A vulnerability in some versions of Microsoft Dynamics could lead to spoofing. The flaw lies in the CRM Webclient component. Successful exploitation by a remote attacker could result in spoofing.

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

### MCAFEE PRODUCT COVERAGE

<table>
<thead>
<tr>
<th>Category</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>
</tbody>
</table>

**THREAT IDENTIFIER(S)**
CVE-2020-17148

**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 Visual Studio 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**
  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

---


**THREAT IDENTIFIER(S)**
CVE-2020-17149

**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 Visual Studio 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**
  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
For McAfee Technical Support, click here.

For Multi-National Phone Support, click here.

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

*The information provided is only for the use and convenience of McAfee’s customers in connection with their McAfee products, and applies only to the threats described herein. McAfee product coverage statements are limited to known attack vectors and should not be considered comprehensive. THE INFORMATION PROVIDED HEREIN IS PROVIDED “AS IS” AND IS SUBJECT TO CHANGE WITHOUT NOTICE.

The information contained herein is the property of McAfee, LLC and may not be reproduced or disseminated without the expressed written consent of McAfee, LLC.

McAfee and the McAfee logo are trademarks or registered trademarks of McAfee, LLC or its subsidiaries in the US and other countries. Other marks and brands may be claimed as the property of others.

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

© 2018 McAfee, LLC. All rights reserved.