NEW CHECKS

26675 - (MSPT-Jun2020) Microsoft Outlook Information Disclosure (CVE-2020-1229)
Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)
Risk Level: High
CVE: CVE-2020-1229

Description
A vulnerability in some versions of Microsoft Outlook could lead to Security Feature Bypass.

Observation
A vulnerability in some versions of Microsoft Outlook could lead to Security Feature Bypass.

The flaw lies in improperly enforce security settings configured. Successful exploitation by an attacker could result in the security feature bypass. The exploit requires the user to open a vulnerable website, email or document.

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)
Risk Level: High
CVE: CVE-2020-1248

Description
A vulnerability in some versions of Microsoft Windows could lead to remote code execution.

Observation
A vulnerability in some versions of Microsoft Windows could lead to remote code execution.

The flaw lies in the GDI 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.

26647 - (MSPT-Jun2020) Microsoft Store Runtime Privilege Escalation (CVE-2020-1222)
Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)
Risk Level: High
CVE: CVE-2020-1222

Description
A vulnerability in some versions of Microsoft Store Runtime could lead to privilege escalation.
Observation
A vulnerability in some versions of Microsoft Store Runtime could lead to privilege escalation.

The flaw lies in improperly handles objects in memory. Successful exploitation could allow a local user to gain elevated privileges. The exploit requires the attacker to have valid credentials to the vulnerable system.


Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)
Risk Level: High
CVE: CVE-2020-1225

Description
A vulnerability in some versions of Microsoft Excel could lead to remote code execution.

Observation
A vulnerability in some versions of Microsoft Excel could lead to remote code execution.

The flaw lies in improperly handle 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.


Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)
Risk Level: High
CVE: CVE-2020-1226

Description
A vulnerability in some versions of Microsoft Excel could lead to remote code execution.

Observation
A vulnerability in some versions of Microsoft Excel could lead to remote code execution.

The flaw lies in improperly handle 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.

26678 - (MSPT-Jun2020) Microsoft Team Foundation Server HTML Injection (CVE-2020-1327)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)
Risk Level: High
CVE: CVE-2020-1327

Description
A vulnerability in some versions of Microsoft Team Foundation Server could lead to HTML Injection.

Observation
A vulnerability in some versions of Microsoft Team Foundation Server could lead to HTML Injection.

The flaw lies in improperly handle web requests. Successful exploitation by a remote attacker could result in HTML Injection. The exploit requires the user to open a vulnerable website, email or document.
**26681 - (MSPT-Jun2020) Microsoft SharePoint Server Spoofing (CVE-2020-1148)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High  
CVE: CVE-2020-1148

**Description**
A vulnerability in some versions of Microsoft SharePoint Server could lead to spoofing.

**Observation**
A vulnerability in some versions of Microsoft SharePoint Server could lead to spoofing.

The flaw lies in the properly sanitize a crafted web request. Successful exploitation by a remote attacker could result in spoofing. The exploit requires the user to open a vulnerable website, email or document.

**26682 - (MSPT-Jun2020) Microsoft SharePoint Server Cross Site Scripting (CVE-2020-1177)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High  
CVE: CVE-2020-1177

**Description**
A vulnerability in some versions of Microsoft SharePoint Server could lead to cross site scripting.

**Observation**
A vulnerability in some versions of Microsoft SharePoint Server could lead to cross site scripting.

The flaw lies in improperly sanitize a crafted web request. 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.

**26685 - (MSPT-Jun2020) Microsoft SharePoint Server Cross Site Scripting (CVE-2020-1183)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High  
CVE: CVE-2020-1183

**Description**
A vulnerability in some versions of Microsoft SharePoint Server could lead to cross site scripting.

**Observation**
A vulnerability in some versions of Microsoft SharePoint Server could lead to cross site scripting.

The flaw lies in improperly sanitize a crafted web request. 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.

**26688 - (MSPT-Jun2020) Microsoft SharePoint Server Cross Site Scripting (CVE-2020-1297)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)
Description
A vulnerability in some versions of Microsoft SharePoint Server could lead to cross site scripting.

Observation
A vulnerability in some versions of Microsoft SharePoint Server could lead to cross site scripting.

The flaw lies in improperly sanitize crafted Web request. Successful exploitation by a remote attacker could affect the integrity of the target.

26690 - (MSPT-Jun2020) Microsoft SharePoint Server Cross Site Scripting (CVE-2020-1318)
Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)
Risk Level: High
CVE: CVE-2020-1318

Description
A vulnerability in some versions of Microsoft SharePoint Server could lead to cross site scripting.

Observation
A vulnerability in some versions of Microsoft SharePoint Server could lead to cross site scripting.

The flaw lies in improperly sanitize a crafted web request. Successful exploitation by a remote attacker could affect the integrity of the target.

26691 - (MSPT-Jun2020) Microsoft SharePoint Server Cross Site Scripting (CVE-2020-1320)
Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)
Risk Level: High
CVE: CVE-2020-1320

Description
A vulnerability in some versions of Microsoft SharePoint Server could lead to cross site scripting.

Observation
A vulnerability in some versions of Microsoft SharePoint Server could lead to cross site scripting.

The flaw lies in improperly sanitize a crafted web request. Successful exploitation by a remote attacker could affect the integrity of the target.

26692 - (MSPT-Jun2020) Microsoft Windows SharePoint Open Redirect (CVE-2020-1323)
Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)
Risk Level: High
CVE: CVE-2020-1323

Description
A vulnerability in some versions of Microsoft Windows could lead to spoofing.
Observation
A vulnerability in some versions of Microsoft Windows could lead to spoofing.

The flaw lies in the SharePoint component. Successful exploitation could allow a local user to disclose sensitive information. The exploit requires the user to open a vulnerable website, email or document.

26693 - (APSB20-30) Vulnerability In Adobe Flash Player

Category: Windows Host Assessment -> Adobe Patches Only
(CATEGORY REQUIRES CREDENTIALS)
Risk Level: High
CVE: CVE-2020-9633

Description
A vulnerability in some versions of Adobe Flash Player could lead to remote code execution.

Observation
A vulnerability in some versions of Adobe Flash Player could lead to remote code execution.

The flaw lies in an unknown component. Successful exploitation by a remote attacker could result in the execution of arbitrary code.

26649 - (MSPT-Jun2020) Microsoft Windows onnected User Experiences and Telemetry Service Denial of Service (CVE-2020-1244)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)
Risk Level: Medium
CVE: CVE-2020-1244

Description
A vulnerability in some versions of Microsoft Windows could lead to a denial of service.

Observation
A vulnerability in some versions of Microsoft Windows could lead to a denial of service.

The flaw lies in the onnected User Experiences and Telemetry Service component. Successful exploitation by an attacker could result in a denial of service condition. The exploit requires the attacker to have valid credentials to the vulnerable system.


Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)
Risk Level: Medium
CVE: CVE-2020-1181

Description
A vulnerability in some versions of Microsoft SharePoint Server could lead to remote code execution.

Observation
A vulnerability in some versions of Microsoft SharePoint Server could lead to remote code execution.
The flaw lies in fails to properly identify and filter unsafe ASP.Net web controls. 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.

26689 - (MSPT-Jun2020) Microsoft SharePoint Server Cross Site Scripting (CVE-2020-1298)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)
Risk Level: Medium
CVE: CVE-2020-1298

Description
A vulnerability in some versions of Microsoft SharePoint Server could lead to cross site scripting.

Observation
A vulnerability in some versions of Microsoft SharePoint Server could lead to cross site scripting.

The flaw lies in improperly sanitize crafted Web request. Successful exploitation by a remote attacker could affect the integrity of the target.


Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)
Risk Level: Medium
CVE: CVE-2020-1348

Description
A vulnerability in some versions of Microsoft Windows could lead to information disclosure.

Observation
A vulnerability in some versions of Microsoft Windows could lead to information disclosure.

The flaw lies in the GDI component. Successful exploitation by an attacker could result in the disclosure of sensitive information. The exploit requires the user to open a vulnerable website, email or document.

26567 - (MSPT-Jun2020) Microsoft Windows Kernel Privilege Escalation (CVE-2020-1262)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)
Risk Level: Medium
CVE: CVE-2020-1262

Description
A vulnerability in some versions of Microsoft Windows could lead to privilege escalation.

Observation
A vulnerability in some versions of Microsoft Windows could lead to privilege escalation.

The flaw lies in the Kernel component. Successful exploitation could allow a local user to gain elevated privileges. The exploit requires the attacker to have valid credentials to the vulnerable system.

26568 - (MSPT-Jun2020) Microsoft Windows Kernel Privilege Escalation (CVE-2020-1265)
Description
A vulnerability in some versions of Microsoft Windows could lead to privilege escalation.

Observation
A vulnerability in some versions of Microsoft Windows could lead to privilege escalation.

The flaw lies in the Kernel component. Successful exploitation could allow a local user to gain elevated privileges. The exploit requires the attacker to have valid credentials to the vulnerable system.

26569 - (MSPT-Jun2020) Microsoft Windows Kernel Privilege Escalation (CVE-2020-1266)

Description
A vulnerability in some versions of Microsoft Windows could lead to privilege escalation.

Observation
A vulnerability in some versions of Microsoft Windows could lead to privilege escalation.

The flaw lies in the Kernel component. Successful exploitation could allow a local user to gain elevated privileges. The exploit requires the attacker to have valid credentials to the vulnerable system.


Description
A vulnerability in some versions of Microsoft Windows could lead to information disclosure.

Observation
A vulnerability in some versions of Microsoft Windows could lead to information disclosure.

The flaw lies in the Kernel 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.


Description
A vulnerability in some versions of Microsoft Windows could lead to privilege escalation.

Observation
A vulnerability in some versions of Microsoft Windows could lead to privilege escalation.

The flaw lies in the Kernel component. Successful exploitation could allow a remote attacker to gain elevated privileges. The exploit requires the attacker to have valid credentials to the vulnerable system.
A vulnerability in some versions of Microsoft Windows could lead to privilege escalation.

The flaw lies in the Kernel component. Successful exploitation could allow a local user to gain elevated privileges. The exploit requires the attacker to have valid credentials to the vulnerable system.
A vulnerability in some versions of Microsoft Windows could lead to privilege escalation.

The flaw lies in the Kernel component. Successful exploitation could allow a local user to gain elevated privileges. The exploit requires the attacker to have valid credentials to the vulnerable system.


Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)  
Risk Level: Medium  
CVE: CVE-2020-1276

**Description**

A vulnerability in some versions of Microsoft Windows could lead to privilege escalation.

**Observation**

A vulnerability in some versions of Microsoft Windows could lead to privilege escalation.

The flaw lies in the Kernel component. Successful exploitation could allow a local user to gain elevated privileges. The exploit requires the attacker to have valid credentials to the vulnerable system.


Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)  
Risk Level: Medium  
CVE: CVE-2020-1280

**Description**

A vulnerability in some versions of Microsoft Windows could lead to privilege escalation.

**Observation**

A vulnerability in some versions of Microsoft Windows could lead to privilege escalation.

The flaw lies in the Kernel component. Successful exploitation could allow a local user to gain elevated privileges. The exploit requires the attacker to have valid credentials to the vulnerable system.


Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)  
Risk Level: Medium  
CVE: CVE-2020-1287

**Description**

A vulnerability in some versions of Microsoft Windows could lead to privilege escalation.

**Observation**

A vulnerability in some versions of Microsoft Windows could lead to privilege escalation.

The flaw lies in the Kernel component. Successful exploitation could allow a local user to gain elevated privileges. The exploit requires the attacker to have valid credentials to the vulnerable system.
Description
A vulnerability in some versions of Microsoft Windows could lead to privilege escalation.

Observation
A vulnerability in some versions of Microsoft Windows could lead to privilege escalation.

The flaw lies in the Kernel component. Successful exploitation could allow a local user to gain elevated privileges. The exploit requires the attacker to have valid credentials to the vulnerable system.

Description
A vulnerability in some versions of Microsoft Windows could lead to privilege escalation.

Observation
A vulnerability in some versions of Microsoft Windows could lead to privilege escalation.

The flaw lies in the Kernel component. Successful exploitation could allow a local user to gain elevated privileges. The exploit requires the attacker to have valid credentials to the vulnerable system.

Description
A vulnerability in some versions of Microsoft Windows could lead to privilege escalation.

Observation
A vulnerability in some versions of Microsoft Windows could lead to privilege escalation.

The flaw lies in the Kernel component. Successful exploitation could allow a local user to gain elevated privileges. The exploit requires the attacker to have valid credentials to the vulnerable system.
A vulnerability in some versions of Microsoft Windows could lead to privilege escalation.

The flaw lies in the Kernel component. Successful exploitation could allow a local user to gain elevated privileges. The exploit requires the attacker to have valid credentials to the vulnerable system.

Category: Windows Host Assessment -> Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2020-1264

Description
A vulnerability in some versions of Microsoft Windows could lead to privilege escalation.

Observation
A vulnerability in some versions of Microsoft Windows could lead to privilege escalation.

The flaw lies in the Kernel component. Successful exploitation by a remote attacker could result in the execution of arbitrary code. The exploit requires the attacker to have valid credentials to the vulnerable system.
A vulnerability in some versions of Microsoft Windows could lead to privilege escalation.

The flaw lies in the Kernel component. Successful exploitation could allow a local user to gain elevated privileges. The exploit requires the attacker to have valid credentials to the vulnerable system.


Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)
Risk Level: Medium
CVE: CVE-2020-1307

Description
A vulnerability in some versions of Microsoft Windows could lead to privilege escalation.

The flaw lies in the Kernel component. Successful exploitation could allow a local user to gain elevated privileges. The exploit requires the attacker to have valid credentials to the vulnerable system.


Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)
Risk Level: Medium
CVE: CVE-2020-1281

Description
A vulnerability in some versions of Microsoft Windows could lead to remote code execution.

The flaw lies in the OLE 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.

**26587 - (MSPT-Jun2020) Microsoft Windows Runtime Privilege Escalation (CVE-2020-1231)**

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)
Risk Level: Medium
CVE: CVE-2020-1231

Description
A vulnerability in some versions of Microsoft Windows could lead to privilege escalation.

The flaw lies in the Runtime 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.
26588 - (MSPT-Jun2020) Microsoft Windows Runtime Privilege Escalation (CVE-2020-1233)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)
Risk Level: Medium
CVE: CVE-2020-1233

Description
A vulnerability in some versions of Microsoft Windows could lead to privilege escalation.

Observation
A vulnerability in some versions of Microsoft Windows could lead to privilege escalation.

The flaw lies in the Runtime 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.

26589 - (MSPT-Jun2020) Microsoft Windows Runtime Privilege Escalation (CVE-2020-1235)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)
Risk Level: Medium
CVE: CVE-2020-1235

Description
A vulnerability in some versions of Microsoft Windows could lead to privilege escalation.

Observation
A vulnerability in some versions of Microsoft Windows could lead to privilege escalation.

The flaw lies in the Runtime 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.

26590 - (MSPT-Jun2020) Microsoft Windows Runtime Privilege Escalation (CVE-2020-1306)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)
Risk Level: Medium
CVE: CVE-2020-1306

Description
A vulnerability in some versions of Microsoft Windows could lead to privilege escalation.

Observation
A vulnerability in some versions of Microsoft Windows could lead to privilege escalation.

The flaw lies in the Runtime 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.

26591 - (MSPT-Jun2020) Microsoft Windows OLE Automation Privilege Escalation (CVE-2020-1212)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)
Risk Level: Medium  
CVE: CVE-2020-1212

Description
A vulnerability in some versions of Microsoft Windows could lead to privilege escalation.

Observation
A vulnerability in some versions of Microsoft Windows could lead to privilege escalation.

The flaw lies in the OLE Automation 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.


Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)
Risk Level: Medium  
CVE: CVE-2020-1299

Description
A vulnerability in some versions of Microsoft Windows could lead to remote code execution.

Observation
A vulnerability in some versions of Microsoft Windows could lead to remote code execution.

The flaw lies in the .LNK File Parser 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.


Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)
Risk Level: Medium  
CVE: CVE-2020-1286

Description
A vulnerability in some versions of Microsoft Windows could lead to remote code execution.

Observation
A vulnerability in some versions of Microsoft Windows could lead to remote code execution.

The flaw lies in the Shell 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.

26594 - (MSPT-Jun2020) Microsoft Windows Backup Service Privilege Escalation (CVE-2020-1271)

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)
Risk Level: Medium  
CVE: CVE-2020-1271

Description
A vulnerability in some versions of Microsoft Windows could lead to privilege escalation.
**Observation**

A vulnerability in some versions of Microsoft Windows could lead to privilege escalation.

The flaw lies in the Backup Service 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.

**26595 - (MSPT-Jun2020) Microsoft Cortana Retrieves Data Without Consideration For Status Privilege Escalation (CVE-2020-1279)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)  
Risk Level: Medium  
CVE: CVE-2020-1279

**Description**

A vulnerability in some versions of Microsoft Cortana could lead to privilege escalation.

**Observation**

A vulnerability in some versions of Microsoft Cortana could lead to privilege escalation.

The flaw lies in retrieves data without consideration for status. Successful exploitation could allow a local user to gain elevated privileges. The exploit requires the attacker to have valid credentials to the vulnerable system.


Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)  
Risk Level: Medium  
CVE: CVE-2020-1296

**Description**

A vulnerability in some versions of Microsoft Windows could lead to information disclosure.

**Observation**

A vulnerability in some versions of Microsoft Windows could lead to information disclosure.

The flaw lies in the Diagnostics 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.

**26597 - (MSPT-Jun2020) Microsoft Windows Improperly Handles Objects in Memory Denial of Service (CVE-2020-1283)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)  
Risk Level: Medium  
CVE: CVE-2020-1283

**Description**

A vulnerability in some versions of Microsoft Windows could lead to a denial of service.

**Observation**

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.

26599 - (MSPT-Jun2020) Microsoft Windows Registry Denial of Service (CVE-2020-1194)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)
Risk Level: Medium
CVE: CVE-2020-1194

Description
A vulnerability in some versions of Microsoft Windows could lead to a denial of service.

Observation
A vulnerability in some versions of Microsoft Windows could lead to a denial of service.

The flaw lies in the Registry component. Successful exploitation by a remote attacker could result in a denial of service condition. The exploit requires the attacker to have valid credentials to the vulnerable system.

26600 - (MSPT-Jun2020) Microsoft Windows Now Playing Session Manager Privilege Escalation (CVE-2020-1201)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)
Risk Level: Medium
CVE: CVE-2020-1201

Description
A vulnerability in some versions of Microsoft Windows could lead to privilege escalation.

Observation
A vulnerability in some versions of Microsoft Windows could lead to privilege escalation.

The flaw lies in the Now Playing Session Manager 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.


Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)
Risk Level: Medium
CVE: CVE-2020-1317

Description
A vulnerability in some versions of Microsoft Group Policy could lead to privilege escalation.

Observation
A vulnerability in some versions of Microsoft Group Policy could lead to privilege escalation.

The flaw lies in improperly checks access. Successful exploitation could allow a local user to gain elevated privileges. The exploit requires the attacker to have valid credentials to the vulnerable system.

26602 - (MSPT-Jun2020) Microsoft Windows WalletService Privilege Escalation (CVE-2020-1294)
Description
A vulnerability in some versions of Microsoft Windows could lead to privilege escalation.

Observation
A vulnerability in some versions of Microsoft Windows could lead to privilege escalation.

The flaw lies in the WalletService 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.

---


Description
A vulnerability in some versions of Microsoft Windows could lead to remote code execution.

Observation
A vulnerability in some versions of Microsoft Windows could lead to remote code execution.

The flaw lies in the Improperly Handle Cabinet Files 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.

---


Description
A vulnerability in some versions of Microsoft Windows could lead to privilege escalation.

Observation
A vulnerability in some versions of Microsoft Windows could lead to privilege escalation.

The flaw lies in the Host Guardian Service 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.

---

26605 - (MSPT-Jun2020) Microsoft No Title Remote Code Execution (CVE-2020-1196)

Description
A vulnerability in some versions of Microsoft Windows could lead to privilege escalation.

Observation
A vulnerability in some versions of Microsoft Windows could lead to privilege escalation.

The flaw lies in the Host Guardian Service 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.
A vulnerability in some versions of Microsoft Windows could lead to privilege escalation.

**Description**

The flaw lies in the printconfig.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.

<table>
<thead>
<tr>
<th>Vulnerability</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>26606</td>
<td>(MSPT-Jun2020) Microsoft No Title Remote Code Execution (CVE-2020-1291)</td>
</tr>
<tr>
<td>Category:</td>
<td>Windows Host Assessment -&gt; Patches and Hotfixes</td>
</tr>
<tr>
<td></td>
<td>(CATEGORY REQUIRES CREDENTIALS)</td>
</tr>
<tr>
<td>Risk Level:</td>
<td>Medium</td>
</tr>
<tr>
<td>CVE:</td>
<td>CVE-2020-1291</td>
</tr>
</tbody>
</table>

**Description**

The flaw lies in the Network Connections Service 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.

<table>
<thead>
<tr>
<th>Vulnerability</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>26607</td>
<td>(MSPT-Jun2020) Microsoft No Title Remote Code Execution (CVE-2020-1316)</td>
</tr>
<tr>
<td>Category:</td>
<td>Windows Host Assessment -&gt; Patches and Hotfixes</td>
</tr>
<tr>
<td></td>
<td>(CATEGORY REQUIRES CREDENTIALS)</td>
</tr>
<tr>
<td>Risk Level:</td>
<td>Medium</td>
</tr>
<tr>
<td>CVE:</td>
<td>CVE-2020-1316</td>
</tr>
</tbody>
</table>

**Description**

The flaw lies in the kernel component. Successful exploitation could allow a local user to gain elevated privileges. The exploit requires the attacker to have valid credentials to the vulnerable system.

<table>
<thead>
<tr>
<th>Vulnerability</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>26609</td>
<td>(MSPT-Jun2020) Microsoft Windows Media Foundation Privilege Escalation (CVE-2020-1238)</td>
</tr>
<tr>
<td>Category:</td>
<td>Windows Host Assessment -&gt; Patches and Hotfixes</td>
</tr>
<tr>
<td></td>
<td>(CATEGORY REQUIRES CREDENTIALS)</td>
</tr>
<tr>
<td>Risk Level:</td>
<td>Medium</td>
</tr>
<tr>
<td>CVE:</td>
<td>CVE-2020-1238</td>
</tr>
</tbody>
</table>
A vulnerability in some versions of Microsoft Windows could lead to privilege escalation.

The flaw lies in the Media Foundation 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.

### 26610 - (MSPT-Jun2020) Microsoft Media Foundation Improperly Handles Objects in Memory Information Disclosure (CVE-2020-1232)

**Category:** Windows Host Assessment -> Patches and Hotfixes  
**Risk Level:** Medium  
**CVE:** CVE-2020-1232

**Description**
A vulnerability in some versions of Microsoft Media Foundation could lead to information disclosure.

**Observation**
A vulnerability in some versions of Microsoft Media Foundation could lead to information disclosure.

The flaw lies in improperly handles objects in memory. Successful exploitation by a remote attacker could result in the disclosure of sensitive information. The exploit requires the attacker to have valid credentials to the vulnerable system.

### 26611 - (MSPT-Jun2020) Microsoft Windows Media Foundation Privilege Escalation (CVE-2020-1239)

**Category:** Windows Host Assessment -> Patches and Hotfixes  
**Risk Level:** Medium  
**CVE:** CVE-2020-1239

**Description**
A vulnerability in some versions of Microsoft Windows could lead to privilege escalation.

**Observation**
A vulnerability in some versions of Microsoft Windows could lead to privilege escalation.

The flaw lies in the Media Foundation 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.

### 26612 - (MSPT-Jun2020) Microsoft Windows Runtime Privilege Escalation (CVE-2020-1304)

**Category:** Windows Host Assessment -> Patches and Hotfixes  
**Risk Level:** Medium  
**CVE:** CVE-2020-1304

**Description**
A vulnerability in some versions of Microsoft Windows could lead to privilege escalation.

**Observation**
A vulnerability in some versions of Microsoft Windows could lead to privilege escalation.

The flaw lies in the Runtime 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.
26613 - (MSPT-Jun2020) Microsoft Windows SMB Denial of Service (CVE-2020-1284)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)
Risk Level: Medium
CVE: CVE-2020-1284

Description
A vulnerability in some versions of Microsoft Windows could lead to a denial of service.

Observation
A vulnerability in some versions of Microsoft Windows could lead to a denial of service.

The flaw lies in the SMB component. Successful exploitation by a remote attacker could result in a denial of service condition.

26615 - (MSPT-Jun2020) Microsoft No Title Remote Code Execution (CVE-2020-1206)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)
Risk Level: Medium
CVE: CVE-2020-1206

Description
A vulnerability in some versions of Microsoft Windows could lead to information disclosure.

Observation
A vulnerability in some versions of Microsoft Windows could lead to information disclosure.

The flaw lies in the SMBv3 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.

26616 - (MSPT-Jun2020) Microsoft Server Message Block 1.0 Improperly Handles Certain Requests Remote Code Execution (CVE-2020-1301)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)
Risk Level: Medium
CVE: CVE-2020-1301

Description
A vulnerability in some versions of Microsoft Server Message Block 1.0 could lead to remote code execution.

Observation
A vulnerability in some versions of Microsoft Server Message Block 1.0 could lead to remote code execution.

The flaw lies in improperly handles certain requests. Successful exploitation by a remote attacker could result in the execution of arbitrary code.


Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)
A vulnerability in some versions of Microsoft Diagnostics Hub Standard Collector Service could lead to privilege escalation. The flaw lies in improperly handles file operations. Successful exploitation could allow a local user to gain elevated privileges. The exploit requires the attacker to have valid credentials to the vulnerable system.

Description
A vulnerability in some versions of Microsoft Windows could lead to privilege escalation.

Observation
A vulnerability in some versions of Microsoft Windows could lead to privilege escalation.

The flaw lies in the Diagnostics Hub Standard Collector or the Visual Studio Standard Collector 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.
A vulnerability in some versions of Microsoft Windows could lead to privilege escalation.

The flaw lies in the Diagnostics Hub Standard Collector Service 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.


Category: Windows Host Assessment -> Patches and Hotfixes (CATEGORY REQUIRES CREDENTIALS)
Risk Level: Medium
CVE: CVE-2020-1293

A vulnerability in some versions of Microsoft Diagnostics Hub Standard Collector Service could lead to privilege escalation.

The flaw lies in improperly handles file operations. Successful exploitation could allow a local user to gain elevated privileges. The exploit requires the attacker to have valid credentials to the vulnerable system.


Category: Windows Host Assessment -> Patches and Hotfixes (CATEGORY REQUIRES CREDENTIALS)
Risk Level: Medium
CVE: CVE-2020-1334

A vulnerability in some versions of Microsoft Windows could lead to privilege escalation.

The flaw lies in the Runtime 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.


Category: Windows Host Assessment -> Patches and Hotfixes (CATEGORY REQUIRES CREDENTIALS)
Risk Level: Medium
CVE: CVE-2020-1255

A vulnerability in some versions of Microsoft Windows could lead to privilege escalation.

The flaw lies in the BITS 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.
A vulnerability in some versions of Microsoft Windows could lead to privilege escalation.

Observation
A vulnerability in some versions of Microsoft Windows could lead to privilege escalation.

The flaw lies in the BITS 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.

26626 - (MSPT-Jun2020) Microsoft Windows Kernel Spoofing (CVE-2020-1311)
Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)
Risk Level: Medium
CVE: CVE-2020-1311

Description
A vulnerability in some versions of Microsoft Windows could lead to spoofing.

Observation
A vulnerability in some versions of Microsoft Windows could lead to spoofing.

The flaw lies in the Kernel component. Successful exploitation by a remote attacker could result in spoofing The exploit requires the user to open a vulnerable website, email or document.

26627 - (MSPT-Jun2020) Microsoft Wlansvc.dll Improperly Handles Objects in Memory Privilege Escalation (CVE-2020-1270)
Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)
Risk Level: Medium
CVE: CVE-2020-1270

Description
A vulnerability in some versions of Microsoft Wlansvc.dll could lead to privilege escalation.

Observation
A vulnerability in some versions of Microsoft Wlansvc.dll could lead to privilege escalation.

The flaw lies in improperly handles objects in memory. Successful exploitation could allow a local user to gain elevated privileges. The exploit requires the attacker to have valid credentials to the vulnerable system.

26628 - (MSPT-Jun2020) Microsoft Windows Security Health Service Privilege Escalation (CVE-2020-1162)
Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)
Risk Level: Medium
CVE: CVE-2020-1162

Description
A vulnerability in some versions of Microsoft Windows could lead to privilege escalation.

Observation
A vulnerability in some versions of Microsoft Windows could lead to privilege escalation.
The flaw lies in the Security Health Service 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.

**26629 - (MSPT-Jun2020) Microsoft Windows GDI Privilege Escalation (CVE-2020-0915)**

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)
Risk Level: Medium
CVE: CVE-2020-0915

**Description**
A vulnerability in some versions of Microsoft Windows could lead to privilege escalation.

**Observation**
A vulnerability in some versions of Microsoft Windows could lead to privilege escalation.

The flaw lies in the GDI 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.

**26630 - (MSPT-Jun2020) Microsoft Windows GDI Privilege Escalation (CVE-2020-0916)**

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)
Risk Level: Medium
CVE: CVE-2020-0916

**Description**
A vulnerability in some versions of Microsoft Windows could lead to privilege escalation.

**Observation**
A vulnerability in some versions of Microsoft Windows could lead to privilege escalation.

The flaw lies in the GDI 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.


Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)
Risk Level: Medium
CVE: CVE-2020-1160

**Description**
A vulnerability in some versions of Microsoft Windows could lead to information disclosure.

**Observation**
A vulnerability in some versions of Microsoft Windows could lead to information disclosure.

The flaw lies in the Graphics component. Successful exploitation by an attacker could result in the disclosure of sensitive information. The exploit requires the attacker to have valid credentials to the vulnerable system.
26632 - (MSPT-Jun2020) Microsoft Windows Error Reporting Privilege Escalation (CVE-2020-1197)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)
Risk Level: Medium
CVE: CVE-2020-1197

Description
A vulnerability in some versions of Microsoft Windows could lead to privilege escalation.

Observation
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.

26633 - (MSPT-Jun2020) Microsoft Windows Error Reporting Privilege Escalation (CVE-2020-1234)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)
Risk Level: Medium
CVE: CVE-2020-1234

Description
A vulnerability in some versions of Microsoft Windows could lead to privilege escalation.

Observation
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.

26635 - (MSPT-Jun2020) Microsoft Windows Installer Privilege Escalation (CVE-2020-1254)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)
Risk Level: Medium
CVE: CVE-2020-1254

Description
A vulnerability in some versions of Microsoft Windows could lead to privilege escalation.

Observation
A vulnerability in some versions of Microsoft Windows could lead to privilege escalation.

The flaw lies in the Installer 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.


Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)
Risk Level: Medium
CVE: CVE-2020-1261

Description
A vulnerability in some versions of Microsoft Windows could lead to information disclosure.

Observation
A vulnerability in some versions of Microsoft Windows could lead to information disclosure.

The flaw lies in the WER component. Successful exploitation by an attacker could result in the disclosure of sensitive information. The exploit requires the attacker to have valid credentials to the vulnerable system.


Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)
Risk Level: Medium
CVE: CVE-2020-1263

Description
A vulnerability in some versions of Microsoft Windows could lead to information disclosure.

Observation
A vulnerability in some versions of Microsoft Windows could lead to information disclosure.

The flaw lies in the WER component. Successful exploitation by an attacker could result in the disclosure of sensitive information. The exploit requires the attacker to have valid credentials to the vulnerable system.

26638 - (MSPT-Jun2020) Microsoft Windows Installer Privilege Escalation (CVE-2020-1272)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)
Risk Level: Medium
CVE: CVE-2020-1272

Description
A vulnerability in some versions of Microsoft Windows could lead to privilege escalation.

Observation
A vulnerability in some versions of Microsoft Windows could lead to privilege escalation.

The flaw lies in the Installer 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.

26639 - (MSPT-Jun2020) Microsoft Windows Installer Privilege Escalation (CVE-2020-1277)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)
Risk Level: Medium
CVE: CVE-2020-1277

Description
A vulnerability in some versions of Microsoft Windows could lead to privilege escalation.
Observation
A vulnerability in some versions of Microsoft Windows could lead to privilege escalation.

The flaw lies in the Installer 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.

26640 - (MSPT-Jun2020) Microsoft Windows Installer Privilege Escalation (CVE-2020-1302)
Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)
Risk Level: Medium
CVE: CVE-2020-1302

Description
A vulnerability in some versions of Microsoft Windows could lead to privilege escalation.

Observation
A vulnerability in some versions of Microsoft Windows could lead to privilege escalation.

The flaw lies in the Installer 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.

26641 - (MSPT-Jun2020) Microsoft Windows Installer Privilege Escalation (CVE-2020-1312)
Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)
Risk Level: Medium
CVE: CVE-2020-1312

Description
A vulnerability in some versions of Microsoft Windows could lead to privilege escalation.

Observation
A vulnerability in some versions of Microsoft Windows could lead to privilege escalation.

The flaw lies in the Installer 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.

26643 - (MSPT-Jun2020) Microsoft Windows Connected User Experiences and Telemetry Service Denial of Service (CVE-2020-1120)
Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)
Risk Level: Medium
CVE: CVE-2020-1120

Description
A vulnerability in some versions of Microsoft Windows could lead to a denial of service.

Observation
A vulnerability in some versions of Microsoft Windows could lead to a denial of service.

The flaw lies in the Connected User Experiences and Telemetry Service component. Successful exploitation by a remote attacker
could result in a denial of service condition. The exploit requires the attacker to have valid credentials to the vulnerable system.

**26644 - (MSPT-Jun2020) Microsoft Windows MDM Diagnostics Privilege Escalation (CVE-2020-1204)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)
Risk Level: Medium  
CVE: CVE-2020-1204

**Description**
A vulnerability in some versions of Microsoft Windows could lead to privilege escalation.

**Observation**
A vulnerability in some versions of Microsoft Windows could lead to privilege escalation.

The flaw lies in the MDM Diagnostics 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.


Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)
Risk Level: Medium  
CVE: CVE-2020-1208

**Description**
A vulnerability in some versions of Microsoft Windows could lead to remote code execution.

**Observation**
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.

**26646 - (MSPT-Jun2020) Microsoft Windows Network List Service Privilege Escalation (CVE-2020-1209)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)
Risk Level: Medium  
CVE: CVE-2020-1209

**Description**
A vulnerability in some versions of Microsoft Windows could lead to privilege escalation.

**Observation**
A vulnerability in some versions of Microsoft Windows could lead to privilege escalation.

The flaw lies in the Network List Service 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.


Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)
Risk Level: Medium
CVE: CVE-2020-1236

Description
A vulnerability in some versions of Microsoft Windows could lead to remote code execution.

Observation
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.


Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)
Risk Level: Medium
CVE: CVE-2020-1290

Description
A vulnerability in some versions of Microsoft Windows could lead to information disclosure.

Observation
A vulnerability in some versions of Microsoft Windows could lead to information disclosure.

The flaw lies in the win32k component. Successful exploitation by an attacker could result in the disclosure of sensitive information. The exploit requires the attacker to have valid credentials to the vulnerable system.

26651 - (MSPT-Jun2020) Microsoft Windows OpenSSH Privilege Escalation (CVE-2020-1292)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)
Risk Level: Medium
CVE: CVE-2020-1292

Description
A vulnerability in some versions of Microsoft Windows could lead to privilege escalation.

Observation
A vulnerability in some versions of Microsoft Windows could lead to privilege escalation.

The flaw lies in the OpenSSH 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.

26652 - (MSPT-Jun2020) Microsoft Windows State Repository Service Privilege Escalation (CVE-2020-1305)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)
Risk Level: Medium
CVE: CVE-2020-1305

Description
A vulnerability in some versions of Microsoft Windows could lead to privilege escalation.

Observation
A vulnerability in some versions of Microsoft Windows could lead to privilege escalation.

The flaw lies in the State Repository Service 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.

**26653 - (MSPT-Jun2020) Microsoft Store Runtime Privilege Escalation (CVE-2020-1309)**

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)
Risk Level: Medium
CVE: CVE-2020-1309

Description
A vulnerability in some versions of Microsoft Store Runtime could lead to privilege escalation.

Observation
A vulnerability in some versions of Microsoft Store Runtime could lead to privilege escalation.

The flaw lies in the Improperly Handles Memory 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.


Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)
Risk Level: Medium
CVE: CVE-2020-1313

Description
A vulnerability in some versions of Microsoft Windows could lead to privilege escalation.

Observation
A vulnerability in some versions of Microsoft Windows could lead to privilege escalation.

The flaw lies in the Update Orchestrator Service 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.


Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)
Risk Level: Medium
CVE: CVE-2020-1207

Description
A vulnerability in some versions of Microsoft Windows could lead to privilege escalation.

Observation
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.


Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)
Risk Level: Medium
CVE: CVE-2020-1251

Description
A vulnerability in some versions of Microsoft Windows could lead to privilege escalation.

Observation
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.


Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)
Risk Level: Medium
CVE: CVE-2020-1253

Description
A vulnerability in some versions of Microsoft Windows could lead to privilege escalation.

Observation
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.


Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)
Risk Level: Medium
CVE: CVE-2020-1258

Description
A vulnerability in some versions of Microsoft Windows could lead to privilege escalation.

Observation
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.

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.


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.

26661 - (MSPT-Jun2020) Microsoft Windows Win32k Privilege Escalation (CVE-2020-1314)

A vulnerability in some versions of Microsoft Windows could lead to privilege escalation.

The flaw lies in the Win32k component. Successful exploitation could allow a local user to gain elevated privileges. The exploit requires the attacker to have valid credentials to the vulnerable system.

26662 - (MSPT-Jun2020) Microsoft VBScript Improperly Handles Objects in Memory Remote Code Execution (CVE-2020-1213)

A vulnerability in some versions of Microsoft Windows could lead to privilege escalation.
CVE: CVE-2020-1213

Description
A vulnerability in some versions of Microsoft VBScript could lead to remote code execution.

Observation
A vulnerability in some versions of Microsoft VBScript could lead to remote code execution.

The flaw lies in improperly handles objects in memory. Successful exploitation by a remote attacker could result in the execution of arbitrary code. The exploit requires the user to open a vulnerable website, email or document.

26663 - (MSPT-Jun2020) Microsoft Edge (Chromium-based) IE Mode Spoofing (CVE-2020-1220)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)
Risk Level: Medium
CVE: CVE-2020-1220

Description
A vulnerability in some versions of Microsoft Edge (Chromium-based) could lead to spoofing.

Observation
A vulnerability in some versions of Microsoft Edge (Chromium-based) could lead to spoofing.

The flaw lies in the IE Mode component. Successful exploitation by a remote attacker could result in spoofing. The exploit requires the user to open a vulnerable website, email or document.

26664 - (MSPT-Jun2020) Microsoft Internet Explorer Improperly Handles Objects in Memory Information Disclosure (CVE-2020-1315)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)
Risk Level: Medium
CVE: CVE-2020-1315

Description
A vulnerability in some versions of Microsoft Internet Explorer could lead to information disclosure.

Observation
A vulnerability in some versions of Microsoft Internet Explorer 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 user to open a vulnerable website, email or document.


Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)
Risk Level: Medium
CVE: CVE-2020-1242

Description
A vulnerability in some versions of Microsoft Edge could lead to information disclosure.

Observation
A vulnerability in some versions of Microsoft Edge could lead to information disclosure.

The flaw lies in improperly handles cross-origin requests. 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.

**26666 - (MSPT-Jun2020) Microsoft ChakraCore Improperly Handles Objects in Memory Remote Code Execution (CVE-2020-1073)**

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)
Risk Level: Medium
CVE: CVE-2020-1073

Description
A vulnerability in some versions of Microsoft ChakraCore could lead to remote code execution.

Observation
A vulnerability in some versions of Microsoft ChakraCore could lead to remote code execution.

The flaw lies in improperly handles objects in memory. Successful exploitation by a remote attacker could result in the execution of arbitrary code. The exploit requires the user to open a vulnerable website, email or document.


Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)
Risk Level: Medium
CVE: CVE-2020-1214

Description
A vulnerability in some versions of Microsoft VBScript could lead to remote code execution.

Observation
A vulnerability in some versions of Microsoft VBScript could lead to remote code execution.

The flaw lies in improperly handles objects in memory. Successful exploitation by a remote attacker could result in the execution of arbitrary code. The exploit requires the user to open a vulnerable website, email or document.

**26668 - (MSPT-Jun2020) Microsoft VBScript Improperly Handles Objects in Memory Remote Code Execution (CVE-2020-1215)**

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)
Risk Level: Medium
CVE: CVE-2020-1215

Description
A vulnerability in some versions of Microsoft VBScript could lead to remote code execution.
A vulnerability in some versions of Microsoft VBScript could lead to remote code execution.

The flaw lies in improperly handling objects in memory. Successful exploitation by a remote attacker could result in the execution of arbitrary code. The exploit requires the user to open a vulnerable website, email or document.


Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)  
Risk Level: Medium  
CVE: CVE-2020-1216

**Description**  
A vulnerability in some versions of Microsoft VBScript could lead to remote code execution.

**Observation**  
A vulnerability in some versions of Microsoft VBScript could lead to remote code execution.

The flaw lies in improperly handling objects in memory. Successful exploitation by a remote attacker could result in the execution of arbitrary code. The exploit requires the user to open a vulnerable website, email or document.


Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)  
Risk Level: Medium  
CVE: CVE-2020-1219

**Description**  
A vulnerability in some versions of Microsoft Browsers could lead to remote code execution.

**Observation**  
A vulnerability in some versions of Microsoft Browsers could lead to remote code execution.

The flaw lies in the Access Objects in Memory 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.


Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)  
Risk Level: Medium  
CVE: CVE-2020-1230

**Description**  
A vulnerability in some versions of Microsoft VBScript could lead to remote code execution.

**Observation**  
A vulnerability in some versions of Microsoft VBScript could lead to remote code execution.
The flaw lies in improperly handles objects in memory. Successful exploitation by a remote attacker could result in the execution of arbitrary code. The exploit requires the user to open a vulnerable website, email or document.


Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)
Risk Level: Medium
CVE: CVE-2020-1260

**Description**
A vulnerability in some versions of Microsoft VBScript could lead to remote code execution.

**Observation**
A vulnerability in some versions of Microsoft VBScript could lead to remote code execution.

The flaw lies in the improperly handles objects in memory. Successful exploitation by a remote attacker could result in the execution of arbitrary code. The exploit requires the user to open a vulnerable website, email or document.


Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)
Risk Level: Medium
CVE: CVE-2020-1217

**Description**
A vulnerability in some versions of Microsoft Windows could lead to information disclosure.

**Observation**
A vulnerability in some versions of Microsoft Windows could lead to information disclosure.

The flaw lies in the Runtime 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.

**26683 - (MSPT-Jun2020) Microsoft SharePoint Server Privilege Escalation (CVE-2020-1178)**

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)
Risk Level: Medium
CVE: CVE-2020-1178

**Description**
A vulnerability in some versions of Microsoft SharePoint Server could lead to privilege escalation.

**Observation**
A vulnerability in some versions of Microsoft SharePoint Server could lead to privilege escalation.

The flaw lies in improperly sanitize a crafted web request. Successful exploitation could allow a local user to gain elevated privileges. The exploit requires the attacker to have valid credentials to the vulnerable system.

**26686 - (MSPT-Jun2020) Microsoft SharePoint Server Spoofing (CVE-2020-1289)**
Description
A vulnerability in some versions of Microsoft SharePoint Server could lead to spoofing.

Observation
A vulnerability in some versions of Microsoft SharePoint Server could lead to spoofing.

The flaw lies in improperly sanitize a crafted web request. Successful exploitation by a remote attacker could result in spoofing.

26687 - (MSPT-Jun2020) Microsoft Windows SharePoint Privilege Escalation (CVE-2020-1295)

Description
A vulnerability in some versions of Microsoft Windows could lead to privilege escalation.

Observation
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 attacker to have valid credentials to the vulnerable system.

26695 - (MSPT-Jun2020) Microsoft Windows Defender Privilege Escalation (CVE-2020-1163)

Description
A vulnerability in some versions of Microsoft Windows could lead to privilege escalation.

Observation
A vulnerability in some versions of Microsoft Windows could lead to privilege escalation.

The flaw lies in the Defender 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.


Description
A vulnerability in some versions of Microsoft Windows could lead to privilege escalation.

Observation
A vulnerability in some versions of Microsoft Windows could lead to privilege escalation.

The flaw lies in the Defender 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.
Description
A vulnerability in some versions of Microsoft Windows could lead to privilege escalation.

Observation
A vulnerability in some versions of Microsoft Windows could lead to privilege escalation.

The flaw lies in the Defender 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.


Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)
Risk Level: Medium
CVE: CVE-2020-1324

Description
A vulnerability in some versions of Microsoft Windows could lead to privilege escalation.

Observation
A vulnerability in some versions of Microsoft Windows could lead to privilege escalation.

The flaw lies in the Security Health Service 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.


Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)
Risk Level: Medium
CVE: CVE-2020-1199

Description
A vulnerability in some versions of Microsoft Windows could lead to privilege escalation.

Observation
A vulnerability in some versions of Microsoft Windows could lead to privilege escalation.

The flaw lies in the Feedback Hub for HoloLens 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.

**ENHANCED CHECKS**

The following checks have been updated. Enhancements may include optimizations, changes that reflect new information on a vulnerability and anything else that improves upon an existing FSL check.

**70014 - netbios-helpers.fasl3.inc**

Category: General Vulnerability Assessment -> NonIntrusive -> Invalid Category
Risk Level: Informational
CVE: CVE-MAP-NOMATCH

**Update Details**
FS1000 APPLIANCE customers should follow the instructions for Enterprise/Professional customers, below. In addition, we strongly urge all appliance customers to authorize and install any Windows Update critical patches. The appliance will auto-download any critical updates but will wait for your explicit authorization before installing.

FOUNDSTONE ENTERPRISE and PROFESSIONAL customers may obtain these new scripts using the FSUpdate Utility by selecting "FoundScan Update" on the help menu. Make sure that you have a valid FSUpdate username and password. The new vulnerability scripts will be automatically included in your scans if you have selected that option by right-clicking the selected vulnerability category and checking the "Run New Checks" checkbox.

MANAGED SERVICE CUSTOMERS already have the newest update applied to their environment. The new vulnerability scripts will be automatically included when your scans are next scheduled, provided the Run New Scripts option has been turned on.

**MCAFEE TECHNICAL SUPPORT**

ServicePortal: https://mysupport.mcafee.com

Multi-National Phone Support available here:

http://www.mcafee.com/us/about/contact/index.html

Non-US customers - Select your country from the list of Worldwide Offices.

This email may contain confidential and privileged material for the sole use of the intended recipient. Any review or distribution by others is strictly prohibited. If you are not the intended recipient please contact the sender and delete all copies.

Copyright 2020 McAfee, Inc.
McAfee is a registered trademark of McAfee, Inc. and/or its affiliates