Nach der Installation des Sicherheitsupdates 896358 oder des Sicherheitsupdates 896358 funktionieren bestimmte HTML-Hilfefunktionen in einigen Websites nicht

Dieser Artikel ist eine Übersetzung des folgenden englischsprachigen Artikels der Microsoft Knowledge Base:
892675 Certain Web sites and HTML Help features may not work after you install security update 896358 or security update 890175

Wichtig: Dieser Artikel enthält Informationen zum Bearbeiten der Registrierung. Sie sollten eine Sicherungskopie der Registrierung erstellen, bevor Sie die Registrierung bearbeiten. Sie müssen wissen, wie die Registrierung wiederhergestellt werden kann, wenn ein Problem auftritt. Weitere Informationen zum Erstellen einer Sicherungskopie, zum Wiederherstellen und Bearbeiten der Registrierung finden Sie in folgendem Artikel der Microsoft Knowledge Base:

256986 Beschreibung der Microsoft Windows-Registrierung

Problembeschreibung

Nachdem Sie das Sicherheitsupdate 896358 oder 890175 installiert haben, treten möglicherweise eines oder mehrere der folgenden Symptome auf:

- Bestimmte webbasierte Programme funktionieren nicht ordnungsgemäß. Zum Beispiel kann ein Inhaltsverzeichnis in der HTML-Hilfe nicht mehr angezeigt werden.
- Bestimmte Funktionen der HTML-Hilfe funktionieren möglicherweise nicht mehr, wenn Sie eine CHM-Datei

von einem Remotestandort aus öffnen. Das Feature "Verwandte Themen" funktioniert möglicherweise nicht.

Hinweis: Dieser Artikel enthält Informationen, die zusätzlich zu den Informationen in den folgenden Artikeln der Microsoft Knowledge Base bereitgestellt werden:

896358 MS05-026: Sicherheitsanfälligkeit in HTML-Hilfe kann Remotecodeausführung ermöglichen

890175 MS05-001: Sicherheitsanfälligkeit in HTML-Hilfe kann Codeausführung ermöglichen

Ursache

Dieses Problem tritt auf, da die Sicherheitsupdates 896358 und 890175 verhindern, dass HTML-Inhalt außerhalb der lokalen Zone eine Instanz des ActiveX-Steuerelements für die HTML-Hilfe erstellt. Diese Änderung sollen Sicherheitsanfälligkeiten in der HTML-Hilfe reduzieren.

Lösung

Achtung: Bei der Installation der Sicherheitsupdates sind diese Symptome erwartet und erwünscht. Dieser Abschnitt bietet Beispiele für Administratoren, die das ActiveX-Steuerelement für die HTML-Hilfe für besonders wichtige Unternehmensanwendungen erneut aktivieren müssen. Die Workarounds können jedoch zur Folge haben, dass der Computer angreifbarer gegenüber den zugrunde liegenden Sicherheitsbedrohungen ist. Die sicherste Methode ist, die Registrierungs-Workarounds anzuwenden. Wenn Sie nicht auf die Workarounds verzichten können, legen Sie die Registrierungswerte mit einer möglichst starken Einschränkung fest.

Warnung: Durch die falsche Bearbeitung der Registrierung mithilfe des Registrierungs-Editors oder einer anderen Methode können schwerwiegende Probleme verursacht werden. Diese Probleme können eine Neuinstallation des Betriebssystems erforderlich machen. Microsoft kann nicht dafür garantieren, dass Probleme, die von einer falschen Verwendung des Registrierung-Editors herrühren, behoben werden können. Änderungen in der Registrierung geschehen auf eigene Verantwortung.

Das erste der folgenden Beispiele bietet die stärkste Einschränkung. Das nächste Beispiel weist die zweitstärkste Einschränkung auf.

Beispiel 1: Verwenden des Wertes "URLAllowList", um bestimmte URLs zu aktivieren

Achtung: Nehmen Sie nur URLs in die Liste auf, denen Sie vertrauen können.

Die .reg-Datei in diesem Beispiel ermöglicht das Hosting des ActiveX-Steuerelements für HTML-Hilfe im folgenden Rahmen:

- Alle CHM-Dateien, die sich im Ordner "\\productmanuals\helpfiles" befinden
- Eine Web-Applikation unter "http://www.wingtiptoys.com/help".

Fügen Sie folgenden Text in einen Texteditor (beispielsweise Editor) ein. Anschließend können Sie die Datei speichern, die die REG-Dateinamenerweiterung verwendet.

```
REGEDIT4 [HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft
```

Sie können in der URL-Zeichenfolge einer Site, die zu dem Registrierungsschlüssel "UrlAllowList" hinzugefügt wird, keine Platzhalterzeichen verwenden. Sie können beispielsweise nicht den folgenden URL-String verwenden:

"UrlAllowList"="http://*.wingtiptoys.com"

Alternativ können Sie folgenden URL-String verwenden:

"UrlAllowList"="http://help.wingtiptoys.com"

Diese Zeichenfolge ermöglicht das Hosten des ActiveX-Steuerelements für die HTML-Hilfe durch folgende Sites:

- http://help.wingtiptoys.com/research
- http://help.wingtiptoys.com/sales

Beispiel 2: Verwenden Sie den Eintrag "MaxAllowedZone", um eine Sicherheitszone freizugeben

Achtung: Der Eintrag "MaxAllowedZone" gibt alle Sites einer bestimmten Zone frei. Es ist möglicherweise sicherer, den Eintrag "UrlAllowList" zu verwenden. Falls Sie den Eintrag "MaxAllowedZone" verwenden müssen, setzen Sie dessen Wert so niedrig wie möglich. Falls Sie den Wert von MaxAllowedZone auf "3" oder höher setzen, sind Ihre Systeme vor Internetattacken nur mangelhaft geschützt.

Hinweis: Standardmäßig ist der Wert MaxAllowedZone auf "0" (Null) eingestellt. Die folgende Tabelle fasst zusammen, wie verschiedene Einträge vom Wert MaxAllowedZone interpretiert werden.

MaxAllowedZone	Lokale Zone	Zone "Lokales Intranet"	Zone "Vertrauenswürdige Sites"	Internetzone	Zone "Eingeschränkte Sites"
0	Zugelassen	Gesperrt	Gesperrt	Gesperrt	Gesperrt
1	Zugelassen	Zugelassen	Gesperrt	Gesperrt	Gesperrt

2	Zugelassen	Zugelassen	Zugelassen	Gesperrt	Gesperrt
3	Zugelassen	Zugelassen	Zugelassen	Zugelassen	Gesperrt
4	Zugelassen	Zugelassen	Zugelassen	Zugelassen	Zugelassen

Fügen Sie folgenden Text in einen Texteditor (beispielsweise Editor) ein: Anschließend können Sie die Datei speichern, die die REG-Dateinamenerweiterung verwendet. Die folgende REG-Datei lässt das Hosten des ActiveX-Steuerelements für die HTML-Hilfe durch sämtlichen Inhalt in der Intranetzone zu.

```
REGEDIT4 [HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft
```

Beispiel 3: Verwenden Sie die Einträge "URLAllowList" und "MaxAllowedZone"

Achtung: Der Eintrag "MaxAllowedZone" gibt alle Sites einer bestimmten Zone frei. Es ist möglicherweise sicherer, den Eintrag "UrlAllowList" zu verwenden. Falls Sie den Eintrag "MaxAllowedZone" verwenden müssen, setzen Sie dessen Wert so niedrig wie möglich. Falls Sie den Wert von MaxAllowedZone auf "3" oder höher setzen, sind Ihre Systeme vor Internetattacken nur mangelhaft geschützt.

Fügen Sie folgenden Text in einen Texteditor (beispielsweise Editor) ein: Anschließend können Sie die Datei speichern, die die REG-Dateinamenerweiterung verwendet. Die folgende REG-Datei lässt das Hosten des ActiveX-Steuerelements für die HTML-Hilfe durch sämtlichen Inhalt in der Intranetzone zu. Diese REG-Datei lässt das Hosten des Steuerelements durch zwei Internetsites zu.

```
REGEDIT4 [HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft
```

Bereitstellen der Registrierungsschlüssel in einer Domäne

Es wird empfohlen, die Einstellungen in den zuvor in diesem Artikel beschriebenen Beispielen mithilfe von Gruppenrichtlinien als Startskripts bereitzustellen. Sie können diese Einstellungen auch als Anmeldeskripts bereitstellen. Erstere Methode ist dieser Methode jedoch aufgrund von Berechtigungseinschränkungen vorzuziehen.

Mit den folgenden Schritten können Sie die Einstellungen aus Beispiel 1 über eine Gruppenrichtlinie als Startskript implementieren.

1. Fügen Sie folgenden Text in einen Texteditor (beispielsweise Editor) ein:

   ```
   REGEDIT4
   [HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\HTMLH
   [HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\HTMLH
   "UrlAllowList"="http://myintranetapplicatior
   ```

2. Speichern Sie die Datei als REG-Datei (.reg). Nennen Sie die Datei "AllowTrustedSites.reg".

3. Fügen Sie folgenden Text in einen Texteditor (beispielsweise Editor) ein:

   ```
   REGEDIT.EXE /S AllowTrustedSites.reg
   ```

4. Speichern Sie die Datei als Batchdatei. Nennen Sie die Datei "AllowTrustedSites.bat".

5. Importieren Sie die Batchdatei in das Gruppenrichtlinienobjekt. Gehen Sie hierzu folgendermaßen vor:
   1. Fügen Sie die Batchdatei, die Sie in Schritt 4 erstellt haben, und die REG-Datei, die Sie in Schritt 2 erstellt haben, in den Ordner "*Domänenname*\SysVol*Domänenname*\Policies*GUID des gewählten Gruppenrichtlinienobjekts*\Machine\Scripts\Startup" ein.
   2. Klicken Sie auf dem Computer, auf dem Sie das Gruppenrichtlinienobjekt ausführen möchten, auf **Start** und auf **Ausführen**, geben Sie dsa.msc ein, und klicken Sie anschließend auf **OK**.
   3. Klicken Sie mit der rechten Maustaste auf Ihre Domäne, und klicken Sie anschließend auf **Eigenschaften**.
   4. Klicken Sie auf **Gruppenrichtlinie** und danach auf **Neu**.
   5. Geben Sie den gewünschten Namen für diese Richtlinie ein, und drücken Sie dann die [EINGABETASTE].
   6. Klicken Sie auf **Bearbeiten**.
   7. Erweitern Sie **Computerkonfiguration**, erweitern Sie **Windows-Einstellungen**, und klicken Sie auf **Skripts (Start/Herunterfahren)**.
   8. Doppelklicken Sie im rechten Fensterbereich auf **Start**, und klicken Sie anschließend auf **Hinzufügen**.
   9. Gehen Sie zu der Batchdatei, die Sie in Schritt 4 erstellt haben, und markieren Sie diese.
   10. Klicken Sie auf **Hinzufügen**.
   11. Klicken Sie auf **OK**, auf **Ja** und zweimal auf **OK**.

Weitere Informationen

Überblick und Beispiele für Systemadministratoren

Weitere Informationen über das Sicherheitsupdate 896358 und dazu, wie Sie von diesem Update betroffene

Webanwendungen erneut aktivieren können, finden Sie in folgendem Artikel der Microsoft Knowledge Base:

896358 MS05-026: Sicherheitsanfälligkeit in HTML-Hilfe kann Remotecodeausführung ermöglichen

Internet Explorer-Sicherheitszonen

Weitere Informationen zur Verwendung von Sicherheitszonen in Internet Explorer finden Sie in folgendem Artikel der Microsoft Knowledge Base:

174360 Sicherheitszonen in Internet Explorer verwenden

Gruppenrichtlinie

Weitere Informationen über Gruppenrichtlinien finden Sie auf folgenden Websites von Microsoft:

- Auflistung von Gruppenrichtlinien

  http://technet2.microsoft.com/WindowsServer/en/Library/6d7cb788-b31d-4d17-9f1e-b5ddaa6deecd1033.mspx

- Was ist der Gruppenrichtlinienobjekt-Editor?

  http://technet2.microsoft.com/WindowsServer/en/Library/47ba1311-6cca-414f-98c9-2d7f99fca8a31033.mspx

- Die wichtigsten Gruppenrichtlinien-Tools und -Einstellungen

  http://technet2.microsoft.com/WindowsServer/en/Library/e926577a-5619-4912-b5d9-e73d4bdc94911033.mspx

Technischer Support für x64-Versionen von Microsoft Windows

Falls Sie Microsoft Windows in einer x64-Version verwenden, sollten Sie die Anweisungen aus dem Abschnitt "Abhilfe" entsprechend anpassen. Sie müssen beispielsweise einen anderen Teil der Registrierung bearbeiten, wenn Sie die 32-Bit bzw. 64-Bit-Funktionalität anpassen möchten.Weitere Informationen finden Sie in folgendem Artikel der Microsoft Knowledge Base:

896459 Registrierungsänderungen in von mal 64-based Versionen Windows Server 2003 und Windows XP Professional x 64 Version

Ihr Hardwarehersteller bietet technischen Support und

Unterstützung für x64-Versionen von Microsoft Windows. Da eine x64-Version von Windows zusammen mit Ihrer Hardware geliefert wurde, ist der Hersteller der Hardware für den technischen Support zuständig. Möglicherweise hat der Hersteller der Hardware die x64-Version von Windows durch einzelne Komponenten verändert. Dazu gehören beispielsweise bestimmte Gerätetreiber oder optionale Einstellungen zur Leistungsoptimierung der Hardware. Wenn Sie technische Hilfe zu Ihrer x64-Version von Windows benötigen, bietet Microsoft in diesem Fall Unterstützung in angemessenem Rahmen. Sie müssen sich jedoch möglicherweise direkt an den Hersteller wenden. Der Hersteller kann Ihnen den besten Support für die von ihm auf der Hardware installierten Software bieten.

Produktinformationen zu Microsoft Windows XP Professional x64 Edition finden Sie auf der folgenden Website von Microsoft:

http://www.microsoft.com/germany/windowsxp/64bit/default.mspx

Weitere Produktinformationen zu den x64-Versionen von Windows Server 2003 finden Sie auf folgender Microsoft-Website:

http://www.microsoft.com/germany/windowsserver2003/editionen/64bit/default.mspx

---

Letzte Aktualisierung: 07.01.2017