

Help and Support

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

Dieser Artikel ist eine Übersetzung des folgenden englischsprachigen Artikels der Microsoft Knowledge Base:
[896358](http://support.microsoft.com/kb/896358/EN-US/) (<http://support.microsoft.com/kb/896358/EN-US/>) MS05-026: A vulnerability in HTML Help could allow remote code execution

Artikel-ID : 896358
Geändert am : Montag, 2. April 2007
Version : 6.2

Bitte beachten Sie: Bei diesem Artikel handelt es sich um eine Übersetzung aus dem Englischen. Es ist möglich, dass nachträgliche Änderungen bzw. Ergänzungen im englischen Originalartikel in dieser Übersetzung nicht berücksichtigt sind. Die in diesem Artikel enthaltenen Informationen basieren auf der/den englischsprachigen Produktversion(en). Die Richtigkeit dieser Informationen in Zusammenhang mit anderssprachigen Produktversionen wurde im Rahmen dieser Übersetzung nicht getestet. Microsoft stellt diese Informationen ohne Gewähr für Richtigkeit bzw. Funktionalität zur Verfügung und übernimmt auch keine Gewährleistung bezüglich der Vollständigkeit oder Richtigkeit der Übersetzung.

Auf dieser Seite

- ↳ Zusammenfassung
- ↳ Bekannte Probleme
- ↳ Schritte, die eventuell helfen
 - ↳ Änderungen an der HTML-Hilfe durch Sicherheitsupdate 896358
 - ↳ Ansätze zum Umgehen von Kompatibilitätsproblemen in Sicherheitsupdate 896358
 - ↳ Einige Beispiele für die Arbeit mit Sicherheitsupdate 896358
 - ↳ Beispiel für einen konservativen Ansatz
 - ↳ Beispiel für einen weniger konservativen Ansatz
 - ↳ Registrierungswerte
 - ↳ Internet Explorer-Sicherheitszonen
 - ↳ Gruppenrichtlinie
 - ↳ Technische Unterstützung für x64-Versionen von Microsoft Windows

Zusammenfassung

Microsoft hat das Security Bulletin MS05-026 veröffentlicht. Das Security Bulletin enthält alle wesentlichen Angaben zu dem Sicherheitsupdate, einschließlich Dateiinformationen und Informationen zur Bereitstellung des Updates. Das komplette Security Bulletin finden Sie auf den folgenden Microsoft-Websites:

- Heimanwender:
<http://www.microsoft.com/germany/athome/security/update/bulletins/default.aspx> (<http://www.microsoft.com/germany/athome/security/update/bulletins/default.aspx>)
- IT-Profis:
<http://www.microsoft.com/germany/technet/sicherheit/bulletins/ms05-026.aspx> (<http://www.microsoft.com/germany/technet/sicherheit/bulletins/ms05-026.aspx>)

Bekannte Probleme

- Bestimmte webbasierte Anwendungen funktionieren möglicherweise nicht mehr einwandfrei, nachdem Sie das Sicherheitsupdate 896358 installiert haben. Zum Beispiel wird das Inhaltsverzeichnis der HTML-Hilfe möglicherweise nicht mehr angezeigt. Außerdem funktionieren bestimmte Funktionen der HTML-Hilfe (beispielsweise "Verwandte Themen") möglicherweise nicht mehr, wenn Sie eine CHM-Datei von einem Remotestandort öffnen. Weitere Informationen zu diesem Problem finden Sie im folgenden Artikel der Microsoft Knowledge Base:
[892675](http://support.microsoft.com/kb/892675/DE/) (<http://support.microsoft.com/kb/892675/DE/>) Nach der Installation des Sicherheitsupdates 896358 oder des Sicherheitsupdates 896358 funktionieren bestimmte HTML-Hilfefunktionen in einigen Websites nicht

- Nach der Installation des Sicherheitsupdates 896358 sind die Funktionen bestimmter Webanwendungen nicht mehr verfügbar. Zum Beispiel wird möglicherweise ein Thema nicht angezeigt, wenn Sie auf die entsprechende Verknüpfung klicken. Außerdem werden Themen in der CHM-Datei möglicherweise nicht angezeigt, wenn Sie einen UNC-Pfad (UNC = Universal Naming Convention) verwenden, um eine CHM-Datei zu öffnen, die sich in einem freigegebenen Netzwerkordner befindet. Weitere Informationen zu diesem Problem finden Sie im folgenden Artikel der Microsoft Knowledge Base:

896054 (<http://support.microsoft.com/kb/896054/DE/>) Sie können keine Remoteinhalte mit dem Protokoll "InfoTech" öffnen, nachdem Sie das Sicherheitsupdate 896358, das Windows Server 2003 Service Pack 1, oder das Sicherheitsupdate 840315 installiert haben

- Nach der Installation des Sicherheitsupdates 896358 funktionieren Webanwendungen möglicherweise nicht mehr, die das ActiveX-Steuerelement der HTML-Hilfe (HHCTRL) verwenden, um die Frame-übergreifende Navigation zu aktivieren. Weitere Informationen zu diesem Problem finden Sie im folgenden Artikel der Microsoft Knowledge Base:

896905 (<http://support.microsoft.com/kb/896905/DE/>) Nach Installation von Sicherheitsupdate 896358 werden Inhalte, die in einem anderen Frame angezeigt werden sollten, in dem Frame angezeigt, der das ActiveX-Steuerelement der HTML-Hilfe enthält

- Nach der Installation des Sicherheitsupdates 896358 gibt es möglicherweise Probleme beim Öffnen einer HTML-Hilfedatei mithilfe eines Hyperlinks im Internet Explorer. Weitere Informationen zu diesem Problem finden Sie im folgenden Artikel der Microsoft Knowledge Base:

902225 (<http://support.microsoft.com/kb/902225/DE/>) Nach der Installation des Sicherheitsupdates 896358 oder Windows Server 2003 Service Pack 1 können Hilfe-Dateien im HTML-Format nicht mehr mit Internet Explorer geöffnet werden

- Nach der Installation des Sicherheitsupdates 896358 akzeptiert das ActiveX-Steuerelement für die HTML-Hilfe bestimmte URLs in Parametern nicht mehr. Weitere Informationen zu diesem Problem finden Sie im folgenden Artikel der Microsoft Knowledge Base:

905215 (<http://support.microsoft.com/kb/905215/DE/>) Bestimmte URL-Schemas werden ignoriert, wenn Sie sie nach dem Installieren des Sicherheitsupdates 896258 in den Parametern eines ActiveX-Steuerelements für die HTML-Hilfe verwenden

Weitere Informationen zum neuesten Service Pack für Windows Server 2003 finden Sie im folgenden Artikel der Microsoft Knowledge Base:

889100 (<http://support.microsoft.com/kb/889100/DE/>) So erhalten Sie das neueste Service Pack für Windows Server 2003

Schritte, die eventuell helfen

Änderungen an der HTML-Hilfe durch Sicherheitsupdate 896358

Achtung: Dieser Artikel bietet Informationen darüber, wie Sie Probleme umgehen können, die durch die Bereitstellung des Sicherheitsupdates 896358 verursacht werden. Microsoft gibt jedoch keine Empfehlung dazu ab, welche Registrierungsschlüssel und -werte speziell für Ihr Unternehmen geeignet sind. Die IT-Abteilung Ihres Unternehmens kann die Vorteile dieser Workarounds am besten gegen die Risiken ihrer Verwendung abwägen. Am sichersten vermeiden Sie Probleme, indem Sie keine Workarounds mit Bezug zur Registrierung anwenden.

Im Folgenden finden Sie kurze Beschreibungen zu den möglichen Folgen des Updates 896358 auf Webanwendungen.

Problem	Verhalten vor Sicherheitsupdate 896358	Verhalten nach Sicherheitsupdate 896358	Artikel in der Microsoft Knowledge Base mit weiteren Informationen und Umgehungsmöglichkeiten
Der Zugriff auf Remoteinhalt durch das Protokoll "InfoTech" ist blockiert.	Das Protokoll "InfoTech" kann generell Remote-Inhalte anzeigen, es sei denn, Sie verwenden Windows Server 2003 Service Pack 1 (SP1), wo diese Funktion deaktiviert ist.	Die Verwendung des Protokolls "InfoTech" zum Anzeigen von Remoteinhalt ist für alle Betriebssysteme blockiert.	896054 (http://support.microsoft.com/kb/896054/DE/) Sie können keine Remoteinhalte mit dem Protokoll "InfoTech" öffnen, nachdem Sie das Sicherheitsupdate 896358, das Sicherheitsupdate 840315 oder das Windows

<p>Die Verwendung des ActiveX-Steuerlements der HTML-Hilfe ist in Remoteinhalt blockiert.</p>	<p>Das Sicherheitsupdate 890175 blockiert die Verwendung des ActiveX-Steuerlements der HTML-Hilfe in Remoteinhalt, der in einer anderen Anwendung als der HTML-Hilfe angezeigt wird. Das Steuerlement ist beispielsweise in Internet Explorer blockiert.</p>	<p>Das ActiveX-Steuerlement der HTML-Hilfe ist nun auch innerhalb der HTML-Hilfe blockiert.</p>	<p>Server 2003 Service Pack 1 installiert haben</p> <p>892675 (http://support.microsoft.com/kb/892675/DE/) Nach der Installation des Sicherheitsupdates 896358 oder des Sicherheitsupdates 896358 funktionieren bestimmte HTML-Hilfefunktionen in einigen Websites nicht</p>
<p>Die Verwendung des ActiveX-Steuerlements für die HTML-Hilfe zum Anzeigen von Inhalten in einem anderen Frame ist blockiert.</p>	<p>Die Verwendung des ActiveX-Steuerlements der HTML-Hilfe in Remoteinhalten, die in einer anderen Anwendung als der HTML-Hilfe angezeigt werden, wurde durch das Sicherheitsupdate 890175 blockiert. Beispielsweise wird das Steuerlement in Internet Explorer blockiert.</p>	<p>Webanwendungen, die das ActiveX-Steuerlement der HTML-Hilfe verwenden, um die Frame-übergreifende Navigation zu aktivieren, funktionieren nicht ordnungsgemäß. Der Inhalt, der in einem anderen Frame angezeigt werden sollte, erscheint in dem Frame, der das ActiveX-Steuerlement der HTML-Hilfe enthält.</p>	<p>896905 (http://support.microsoft.com/kb/896905/DE/) Nach Installation von Sicherheitsupdate 896358 werden Inhalte, die in einem anderen Frame angezeigt werden sollten, in dem Frame angezeigt, der das ActiveX-Steuerlement der HTML-Hilfe enthält</p>
<p>CHM-Dateien können nicht über den Internet Explorer geöffnet werden.</p>	<p>Kein Problem.</p>	<p>Wenn Sie Internet Explorer verwenden, um eine CHM-Datei zu öffnen, wird das Thema nicht angezeigt.</p> <p>Nachdem Sie eine CHM-Datei mithilfe des Internet Explorers gespeichert haben, treten aufgrund von Schutzmechanismen im Anlagen-Manager möglicherweise Probleme beim Öffnen auf.</p>	<p>902225 (http://support.microsoft.com/kb/902225/DE/) Nach der Installation des Sicherheitsupdates 896358 oder Windows Server 2003 Service Pack 1 können Hilfe-Dateien im HTML-Format nicht mehr mit Internet Explorer geöffnet werden</p>
<p>Manche URL-Schemas werden ignoriert, wenn Sie sie in den Parametern eines ActiveX-Steuerlements für die HTML-Hilfe verwenden.</p>	<p>In den Parametern des ActiveX-Steuerlements für die HTML-Hilfe waren alle Schemas gestattet.</p>	<p>Nur die folgenden Schemas werden nicht vom ActiveX-Steuerlement für die HTML-Hilfe ignoriert: file, http, https, ftp, its, ms-its, mk:@msitstore, Hcp.</p>	<p>905215 (http://support.microsoft.com/kb/905215/DE/) Bestimmte URL-Schemas werden ignoriert, wenn Sie sie nach dem Installieren des Sicherheitsupdates 896258 in den Parametern eines ActiveX-Steuerlements für die HTML-Hilfe verwenden</p>

Ansätze zum Umgehen von Kompatibilitätsproblemen in Sicherheitsupdate 896358

Das Sicherheitsupdate 896358 unterstützt einige Registrierungsschlüssel und Registrierungswerte, die Sie verwenden können, um Probleme mit der Anwendungscompatibilität zu umgehen. Beantworten Sie folgende Fragen, um zu entscheiden, welche Registrierungsänderungen vorzunehmen sind:

- Gibt es Anwendungen oder Szenarien, die von den in diesem Artikel beschriebenen Änderungen betroffen sind?

- Wie viele Anwendungen sind von diesen Änderungen betroffen? Wie wichtig sind diese Anwendungen?
- Wie schwerwiegend ist das Problem, das durch die Änderungen verursacht wird?
- Ist es möglich, die Programme so zu bearbeiten, dass sie diese Funktion der HTML-Hilfe nicht benötigen? Können Ihre Mitarbeiter beispielsweise CHM-Dateien herunterladen statt sie von einer Dateifreigabe auszuführen? Kann eine Webanwendung ein DHTML-Inhaltsverzeichnis anstelle des ActiveX-Steuerlements der HTML-Hilfe verwenden?
- Welche Sicherheitsanforderungen und -funktionen gelten in Ihrem Unternehmen?
 - Was ist wichtiger: das Verwenden der Funktion der HTML-Hilfe oder das Sicherstellen der maximalen Sicherheit.
 - Möchten Sie die HTML-Hilfefunktionen (wie in den folgenden Beispielen) eventuell auch in Ihrem Intranet verwenden. Falls ja, sind die externen Sicherheitsmaßnahmen, beispielsweise die Unternehmensfirewall, ausreichend? Vertrauen Sie Ihren Angestellten ausreichend, sodass Sie sich keine Sorgen darüber machen, dass ein System innerhalb Ihres Unternehmens verwendet werden kann, um ein anderes System anzugreifen?

Einige Beispiele für die Arbeit mit Sicherheitsupdate 896358

Achtung: Am sichersten vermeiden Sie Probleme, indem Sie keine Workarounds mit Bezug zur Registrierung anwenden. Falls Sie Workarounds mit Auswirkungen auf die Registrierung verwenden müssen, sollten Sie sie so konservativ wie möglich konfigurieren. Wenden Sie beispielsweise die folgenden Methoden an:

- Anstelle des Registrierungseintrags "MaxAllowedZone" könnten Sie den Registrierungseintrag "UrlAllowList" verwenden. Dabei sollte "UrlAllowList" so wenige Sites wie möglich erlauben.
- Wenn Sie den Wert "MaxAllowedZone" verwenden müssen, setzen Sie ihn nicht höher als nötig. Falls Sie den Wert von "MaxAllowedZone" auf 3 oder höher setzen, sind Ihre Systeme vor Internetattacken nur mangelhaft geschützt.

Nachdem Sie die Informationen über die Verwendung der HTML-Hilfe in Ihrem Unternehmen zusammengetragen haben, überlegen Sie, ob Sie anhand eines der folgenden Beispiele eine Strategie zur Verwendung bei der Anwendung des Sicherheitsupdates 896358 in Ihrem Unternehmen entwickeln können.

Beispiel für einen konservativen Ansatz

Ein konservativer Ansatz könnte erfolgreich sein, wenn die folgenden Bedingungen für Ihr Unternehmen zutreffen:

- Es sind keine Webanwendungen bekannt, die die Technologie der HTML-Hilfe verwenden.
- Das Sicherstellen der maximalen Sicherheit ist wichtiger als der Einsatz bestimmter Anwendungen und Szenarien, die die HTML-Hilfe erfordern, um ordnungsgemäß zu funktionieren.
- Sie verfügen über Webanwendungen, die die Technologie der HTML-Hilfe verwenden, aber die Besitzer dieser Anwendungen können diese Anwendungen schnell auf die Verwendung anderer Technologien umstellen.
- Sie können schnell die Anwendungsserver und Dateifreigaben ermitteln, auf denen die Anwendungen und Szenarien bereitgestellt werden, die die Technologie der HTML-Hilfe erfordern. Außerdem können Sie einen ausreichenden Schutz für diese Anwendungsserver und Dateifreigaben bieten.
- Niemand muss CHM-Dateien von Remotestandorten, zum Beispiel Dateifreigaben, öffnen.

Die folgende Methode ist ein Beispiel für einen konservativen Ansatz:

1. Wenden Sie das Sicherheitsupdate 896358 an, und erzwingen Sie Einschränkungen durch die Verwendung eines Gruppenrichtlinienobjekts.

Wenn Sie bei der Installation des Sicherheitsupdates 896358 nicht einen oder mehrere der Registrierungswerte anwenden, werden die Sicherheitseinschränkungen in Sicherheitsupdate 896358 standardmäßig so restriktiv wie möglich sein. Sie können jedoch ein Gruppenrichtlinienobjekt verwenden, um zu verhindern, dass einzelne Benutzer die Einschränkungen selbst lockern.

Die folgende Registrierungsdatei macht die Sicherheitseinschränkungen in Sicherheitsupdate 896358 so restriktiv wie möglich:

```
REGEDIT4 [HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\HTMLHelp] [HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\HTMLHelp\1.x\HHRestrictions] "MaxAllowedZone"=dword:00000000 "UrlAllowList"="" [HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\HTMLHelp\1.x\ItssRestrictions] "MaxAllowedZone"=dword:00000000 "UrlAllowList"=""
```

Wenn Sie wissen, dass Ihr Unternehmen über keine Webanwendungen verfügt, die die HTML-Hilfe erfordern, und die Benutzer in Ihrem Unternehmen nicht auf Remote-CHM-Dateien zugreifen müssen, können Sie den Vorgang hier beenden.

2. Untersuchen Sie die Verwendung der HTML-Hilfe durch Webanwendungen. Möglicherweise werden Benutzer berichten, dass einige interne Webanwendungen von dem Update betroffen sind. Fragen Sie die Besitzer dieser Webanwendungen, ob die Funktionen, die die Technologie der HTML-Hilfe erfordern, umprogrammiert werden können. Wenn die Webanwendungen ohne die Technologie der HTML-Hilfe auskommen, können Sie den Vorgang hier beenden.
3. Aktivieren Sie die Webanwendungen einzeln nacheinander. Wenn Sie feststellen, dass einige der Webanwendungen die Funktionalität der HTML-Hilfe erfordern, können Sie den Zugriff auf die Server, die diese Anwendungen hosten, einzeln nacheinander aktivieren. Das folgende Beispiel einer Registrierungsdatei aktiviert das ActiveX-Steuerelement der HTML-Hilfe und das Protokoll "InfoTech" für eine bestimmte Site. Dieses Beispiel einer Registrierungsdatei aktiviert auch die Frame-übergreifende Navigation durch das Active X-Steuerelement der HTML-Hilfe erneut.

```
REGEDIT4 [HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\HTMLHelp] [HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\HTMLHelp\1.x\HHRestrictions] "MaxAllowedZone"=dword:00000000 "UrlAllowList"="http://contoso/salesapp/" "EnableFrameNavigationInSafeMode"=dword:00000001 [HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\HTMLHelp\1.x\ItssRestrictions] "MaxAllowedZone"=dword:00000000 "UrlAllowList"="http://contoso/salesapp/"
```

Hinweis: Anwender werden möglicherweise immer noch nicht in der Lage sein, CHM-Dateien direkt über einen Weblink auf einer Webseite zu öffnen. Weitere Informationen zu diesem Problem und möglichen Workarounds finden Sie im folgenden Artikel der Microsoft Knowledge Base:

[902225](http://support.microsoft.com/kb/902225/DE/) (http://support.microsoft.com/kb/902225/DE/) Nach der Installation des Sicherheitsupdates 896358 oder Windows Server 2003 Service Pack 1 können Hilfe-Dateien im HTML-Format nicht mehr mit Internet Explorer geöffnet werden

Beispiel für einen weniger konservativen Ansatz

Dieser Ansatz könnte erfolgreich sein, wenn die folgenden Bedingungen vorliegen:

- Sie sind bereit, zusätzliche Risiken in Kauf zu nehmen, um zu vermeiden, dass das Sicherheitsupdate 896358 sich negativ auf Ihre Anwendungen auswirkt.
- Sie können nicht umgehend alle Anwendungen und Szenarien feststellen, die die Technologie der HTML-Hilfe erfordern.
- Sie verfügen über Webanwendungen, die die Technologie der HTML-Hilfe verwenden, und die sehr wichtig für Ihren Geschäftsbereich sind. Außerdem können Sie diese Anwendungen nicht schnell auf die Verwendung anderer Technologien umstellen.

Die folgende Methode ist ein Beispiel für einen weniger konservativen Ansatz:

1. Wenden Sie das Sicherheitsupdate 896358 an, und erzwingen Sie Einschränkungen durch die Verwendung eines Gruppenrichtlinienobjekts.

Das folgende Beispiel einer Registrierungsdatei ermöglicht allen Systemen in Ihrem Intranet, das ActiveX-Steuerelement der HTML-Hilfe und den Inhalt durch Verwendung des Protokolls "InfoTech" bereitzustellen. Dieses Beispiel einer Registrierungsdatei aktiviert auch die Frame-übergreifende Navigation durch das Active X-Steuerelement der HTML-Hilfe erneut.

```
REGEDIT4 [HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\HTMLHelp] [HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\HTMLHelp\1.x\HHRestrictions] "MaxAllowedZone"=dword:00000001 "EnableFrameNavigationInSafeMode"=dword:00000001 [HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\HTMLHelp\1.x\ItssRestrictions] "MaxAllowedZone"=dword:00000001
```

Hinweis: Anwender werden möglicherweise immer noch nicht in der Lage sein, CHM-Dateien direkt über einen Weblink auf einer Webseite zu öffnen. Weitere Informationen zu diesem Problem und möglichen Workarounds finden Sie im folgenden Artikel der Microsoft Knowledge Base:

[902225](http://support.microsoft.com/kb/902225/DE/) (http://support.microsoft.com/kb/902225/DE/) Nach der Installation des Sicherheitsupdates 896358 oder Windows Server 2003 Service Pack 1 können Hilfe-Dateien im HTML-Format nicht mehr mit Internet Explorer geöffnet werden

2. Untersuchen Sie die Verwendung der HTML-Hilfe durch Webanwendungen. Ermitteln Sie, welche Webanwendungen die Technologie der HTML-Hilfe erfordern. Fragen Sie die Besitzer dieser Webanwendungen, ob die Funktionen, die die Technologie der HTML-Hilfe erfordern, umprogrammiert werden können.
3. Wählen Sie die Einstellungen der HTML-Hilfe basierend auf den Ergebnissen Ihrer Nachforschungen. Wenn Ihre Untersuchungen ergeben, dass die Webanwendungen die Technologie der HTML-Hilfe nicht mehr

erfordern, können Sie die folgende Registrierungsdatei bereitstellen, um die maximalen Einschränkungen zu verwenden, die von Sicherheitsupdate 896358 unterstützt werden:

```
REGEDIT4 [HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\HTMLHelp] [HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\HTMLHelp\1.x\HHRestrictions] "MaxAllowedZone"=dword:00000000
"UrlAllowList"="" [HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\HTMLHelp\1.x\ItssRestrictions]
"MaxAllowedZone"=dword:00000000 "UrlAllowList"=""
```

Wenn Sie feststellen, dass einige Webanwendungen die Funktionalität der HTML-Hilfe erfordern, können Sie eine eingeschränkte Aktivierung der HTML-Hilfe nur für diese Systeme festlegen. Das folgende Beispiel einer Registrierungsdatei schränkt die Verwendung des ActiveX-Steuerelements der HTML-Hilfe und des Protokolls "InfoTech" für bestimmte Intranetsites ein. Dieses Beispiel einer Registrierungsdatei lässt auch weiterhin eine Frame-übergreifende Navigation durch das Active X-Steuerelement der HTML-Hilfe zu.

```
REGEDIT4 [HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\HTMLHelp] [HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\HTMLHelp\1.x\HHRestrictions] "MaxAllowedZone"=dword:00000000
"UrlAllowList"="http://wingtip toys/catalog/;\\wingtip toys\help\helpfiles;"
"EnableFrameNavigationInSafeMode"=dword:00000001 [HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\HTMLHelp\1.x\ItssRestrictions]
"MaxAllowedZone"=dword:00000000 "UrlAllowList"="http://wingtip toys/catalog/;\\wingtip toys\help\helpfiles;file://\\wingtip toys\help\helpfiles"
```

Registrierungswerte

Die folgende Tabelle listet die Registrierungswerte für die HTML-Hilfe auf, die in diesem Artikel beschrieben werden. Sie listet außerdem die Microsoft Knowledge Base-Artikel auf, in denen Sie weitere Informationen finden.

Wert	Microsoft Knowledge Base-Artikel
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\HTMLHelp\1.x\HHRestrictions\MaxAllowedZone	892675 (http://support.microsoft.com/kb/892675/DE/) Nach der Installation des Sicherheitsupdates 896358 oder des Sicherheitsupdates 896358 funktionieren bestimmte HTML-Hilfefunktionen in einigen Websites nicht
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\HTMLHelp\1.x\HHRestrictions\UrlAllowList	892675 (http://support.microsoft.com/kb/892675/DE/) Nach der Installation des Sicherheitsupdates 896358 oder des Sicherheitsupdates 896358 funktionieren bestimmte HTML-Hilfefunktionen in einigen Websites nicht
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\HTMLHelp\1.x\HHRestrictions\EnableFrameNavigationInSafeMode	896905 (http://support.microsoft.com/kb/896905/DE/) Nach Installation von Sicherheitsupdate 896358 werden Inhalte, die in einem anderen Frame angezeigt

	werden sollten, in dem Frame angezeigt, der das ActiveX-Steurelement der HTML-Hilfe enthält
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\HTMLHelp\1.x\ItssRestrictions\MaxAllowedZone	896054 (http://support.microsoft.com/kb/896054/DE/) Sie können keine Remoteinhalte mit dem Protokoll "InfoTech" öffnen, nachdem Sie das Sicherheitsupdate 896358, das Sicherheitsupdate 840315 oder das Windows Server 2003 Service Pack 1 installiert haben
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\HTMLHelp\1.x\ItssRestrictions\UrlAllowList	896054 (http://support.microsoft.com/kb/896054/DE/) Sie können keine Remoteinhalte mit dem Protokoll "InfoTech" öffnen, nachdem Sie das Sicherheitsupdate 896358, das Sicherheitsupdate 840315 oder das Windows Server 2003 Service Pack 1 installiert haben

Internet Explorer-Sicherheitszonen

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

[174360](http://support.microsoft.com/kb/174360/DE/) (http://support.microsoft.com/kb/174360/DE/) 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.msp#> (<http://technet2.microsoft.com/windowsserver/en/library/6d7cb788-b31d-4d17-9f1e-b5ddaa6deecd1033.mspx>)

- Editor für Gruppenrichtlinienobjekte

<http://technet2.microsoft.com/windowsserver/en/library/47ba1311-6cca-414f-98c9-2d7f99fca8a31033.msp#> (<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.msp#> (<http://technet2.microsoft.com/windowsserver/en/library/e926577a-5619-4912-b5d9-e73d4bdc94911033.mspx>)

Die Verwendung der hier aufgeführten Informationen, Makro- oder Programmcodes geschieht auf Ihre eigene Verantwortung. Microsoft stellt Ihnen diese Informationen sowie Makro- und Programmlistings ohne Gewähr auf Richtigkeit, Vollständigkeit und/oder Funktionalität sowie ohne Anspruch auf Support zur Verfügung. In diesem Artikel wird vorausgesetzt, dass Sie mit der in den Beispielen verwendeten Programmiersprache und mit den zum Erstellen und Debuggen von Prozeduren verwendeten Tools vertraut sind. Die Spezialisten von Microsoft Product Support Services können bei der Erläuterung der Funktionalität bestimmter Prozeduren helfen, jedoch werden sie diese Beispiele nicht in Bezug auf eine erweiterte Funktionalität verändern, noch werden sie Prozeduren entwickeln, die auf Ihre besonderen Bedürfnisse zugeschnitten sind.

Technische Unterstützung für x64-Versionen von Microsoft Windows

Falls Sie Microsoft Windows in einer x64-Version verwenden, sollten Sie die Anweisungen aus dem Abschnitt "Lösungsansätze" 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 im folgenden Artikel der Microsoft Knowledge Base:

[896459](http://support.microsoft.com/kb/896459/DE/) (<http://support.microsoft.com/kb/896459/DE/>) Registrierungsänderungen in von Windows XP Professional x 64 mal 64-basierten Versionen von Windows Server 2003 und in Edition

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 installierte Software bieten.

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

<http://www.microsoft.com/germany/windows/windowsxp/64bit/default.msp#> (<http://www.microsoft.com/germany/windows/windowsxp/64bit/default.mspx>)

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

<http://www.microsoft.com/germany/windowsserver2003/editionen/64bit/default.msp#> (<http://www.microsoft.com/germany/windowsserver2003/editionen/64bit/default.mspx>)

Die Informationen in diesem Artikel beziehen sich auf:

- Microsoft Windows Server 2003 Service Pack 1, wenn verwendet mit:
 - Microsoft Windows Server 2003, Standard Edition (32-bit x86)
 - Microsoft Windows Server 2003, Enterprise Edition (32-bit x86)
 - Microsoft Windows Server 2003, Datacenter Edition (32-bit x86)
 - Microsoft Windows Server 2003, Web Edition
 - Microsoft Windows Server 2003, Enterprise Edition for Itanium-based Systems
 - Microsoft Windows Server 2003, Datacenter Edition for Itanium-Based Systems
- Microsoft Windows Server 2003, Standard x64 Edition

- Microsoft Windows Server 2003, Enterprise x64 Edition
- Microsoft Windows Server 2003, Datacenter x64 Edition
- Microsoft Windows XP for Itanium-based Systems Version 2003
- Microsoft Windows XP Professional 64-Bit Edition (Itanium)
- Microsoft Windows XP Professional x64 Edition
- Microsoft Windows XP Service Pack 1
- Microsoft Windows 2000 Advanced Server
- Microsoft Windows 2000 Datacenter Server
- Microsoft Windows 2000 Professional Edition
- Microsoft Windows 2000 Service Pack 4
- Microsoft Windows 2000 Service Pack 3
- Microsoft Windows Millennium Edition
- Microsoft Windows 98 Second Edition
- Microsoft Windows 98 Standard Edition

Keywords: kbbug kbfix kbsecvulnerability kbqfe kbsecurity kbwinnt400presp7fix kbsecbulletin kbwinxppresp2fix kbpubtypekc kbwin2000presp5fix kbwinserv2003presp1fix kbhotfixserver kbwinserv2003sp2fix KB896358

Microsoft stellt Ihnen die in der Knowledge Base angebotenen Artikel und Informationen als Service-Leistung zur Verfügung. Microsoft übernimmt keinerlei Gewährleistung dafür, dass die angebotenen Artikel und Informationen auch in Ihrer Einsatzumgebung die erwünschten Ergebnisse erzielen. Die Entscheidung darüber, ob und in welcher Form Sie die angebotenen Artikel und Informationen nutzen, liegt daher allein bei Ihnen. Mit Ausnahme der gesetzlichen Haftung für Vorsatz ist jede Haftung von Microsoft im Zusammenhang mit Ihrer Nutzung dieser Artikel oder Informationen ausgeschlossen.

Help and Support

©2008 Microsoft