SICHER o INFORMIERT
Extraausgabe vom 19.01.2010

Weitere Anwendungen betroffen

# Kritische Sicherheitsluecke im Internet Explorer

Von der am 15.01.2010 im Buerger-CERT berichteten Schwachstelle im Internet Explorer sind noch weitere Anwendungen betroffen. Die Schwachstelle beruht auf einem Fehler in der Microsoft HTML-Bibliothek mshtml.dll und betrifft potenziell alle Anwendungen, die darauf zugreifen.

Zusaetzlich zum Internet Explorer sind nach Erkenntnissen des BSI insbesondere folgende Produkte verwundbar:

- Microsoft Outlook (bis einschliesslich Outlook 2003)
- Microsoft Outlook Express
- Microsoft Windows Mail
- Microsoft Windows Live Mail
- Microsoft Hilfesystem
- Microsoft Sidebar

Das BSI empfiehlt in Ergaenzung zu den bereits veroeffentlichten Massnahmen fuer den Internet Explorer allen Nutzern, die eines der oben genannten Produkte verwenden, die nachfolgenden Massnahmen zu ergreifen.

o Microsoft Outlook Express, Microsoft Windows Mail, Microsoft Windows Live Mail:
Die Nutzung der "Eingeschraenkten Zone" und nicht der "Internet-Zone" zur Anzeige von E-Mails wird dringend empfohlen. In der eingeschraenkten Zone ist die Ausfuehrung von Active Scripting zu unterbinden (Standardeinstellung). Zusaetzlich sollte die Anzeige von HTML-E-Mails deaktiviert werden.

In Windows Live Mail druecken Sie "Alt" + "m", waehlen den Menuepunkt "Sicherheitsoptionen..." aus, gehen anschliessend auf den Reiter "Sicherheit" und waehlen dort die "Zone fuer eingeschraenkte Sites" aus. Folgen Sie nicht der Empfehlung von Windows Live Mail, dass die "Internetzone" zweckmaessiger sei.

o Microsoft Outlook:
Die Nutzung der "Eingeschraenkten Zone" zur Anzeige von E-Mails wird dringend empfohlen. In der eingeschraenkten Zone ist die Ausfuehrung von Active Scripting zu unterbinden (Standardeinstellung). Zusaetzlich sollte die Anzeige von HTML-E-Mails deaktiviert werden.

In Unternehmensnetzwerken in denen Outlook bis Version 2003 im Einsatz ist, sollten diese Einstellungen ueber Gruppenrichtlinien zentral vorgenommen werden.

o Microsoft Hilfesystem:
Es sollten keine Hilfedateien, insbesondere mit der Dateiendung ".chm", aus unsicheren Quellen geoeffnet werden.

o Microsoft Sidebar:
Angriffe ueber die Sidebar sind schwieriger durchfuehrbar. Wer dieses Risiko vermeiden moechte, sollte bis zur Bereitstellung des Patches auf die Benutzung der Sidebar verzichten.

Die Luecke wird derzeit ausgenutzt. Microsoft arbeitet bereits an einem Patch, um die Sicherheitsluecke zu schliessen.  Sobald ein Patch seitens Microsoft verfuegbar ist, wird das BSI Sie darueber informieren.