COMPUTERWOCHE
VOICE OF DIGITAL

Link: https://www.computerwoche.de/a/alle-internet-explorer-versionen-unter-beschuss,1881798

Laut Microsoft

Alle Internet-Explorer-Versionen unter Beschuss

Datum: 15.12.2008
Autor(en): Uli Ries

Die in der letzten Woche bekannt gewordene Zero-Day-Attacke betrifft nicht nur den Internet Explorer 7, sondern sämtliche Varianten des Browsers. Noch ist kein Patch für die Browser verfügbar, aber die Redmonder geben Ratschläge, wie sich Administratoren und Nutzer gegen Angriffe schützen können. Gleichzeitig tauchen immer mehr Webseiten auf, die die Lücke anzugreifen versuchen.

Im Visier: Cyber-Kriminelle nutzen eine Lücke im Internet Explorer aus, um PCs mit Malware zu infizieren.
Foto:

Die jüngste Version eines inzwischen mehrfach überarbeiteten **Microsoft-Dokuments**[1] bestätigt, dass die vor kurzem aufgetauchte **Browser-Lücke**[2] nicht nur den **Internet Explorer 7**[3] betrifft, sondern alle Versionen – einschließlich der brandneuen **Beta 2**[4] des **IE8**[5]. Auch die Beschränkung auf **Windows XP**[6] und **Windows Vista**[7] ist gefallen: Egal unter welcher Windows-Version der Browser läuft, die Attacke ist prinzipiell möglich.

Noch immer gibt es keinen Patch von **Microsoft**[8], so dass die Sicherheitsexperten des Softwareherstellers eine **Liste**[9] mit inzwischen neun Anweisungen zusammen gestellt haben, wie Administratoren und Endanwender einer **Malware**[10]-Infektion entgehen können. Einige der Ratschläge sind technisch jedoch so komplex, dass auch überdurchschnittlich begabte Endanwender mit den knappen Hinweisen nicht zurecht kommen. Der Rat, Scripting zu deaktivieren, ist zudem praxisfremd, da ein derartig eingeschränkter Browser kaum eine Webseite fehlerfrei anzeigt. Insofern sollten Anwender wenn möglich auf alternative Browser wie **Firefox**[11] oder **Chrome**[12] ausweichen.

Das perfide an der Attacke ist, dass ohne Zutun des Users Malware auf seinen Rechner gespielt wird. Der Aufruf einer infizierten Web-Site genügt (Drive by Infection). Wie die Anti-Viren-Experten von **Trend Micro**[13] berichten, nutzen die Angreifer inzwischen automatisierte SQL-Injections, um neue Webseiten mit bösartigen JavaScripts zu infizieren. Die Skripte sorgen beim Aufruf der Seiten dann für den Malware-Download. Eine – nicht vollständige – Liste mit infizierten Sites findet sich bei **Shadowserver**[14].

Links im Artikel:

[1] **http://http//www.microsoft.com/technet/security/advisory/961051.mspx**
[2] **https://www.computerwoche.de/knowledge_center/web/1881574/**
[3] **https://www.computerwoche.de/schwerpunkt/i/IE7.html**
[4] **https://www.computerwoche.de/knowledge_center/web/1872387/**
[5] **https://www.computerwoche.de/schwerpunkt/i/IE8.html**
[6] **https://www.computerwoche.de/schwerpunkt/x/XP.html**
[7] **https://www.computerwoche.de/schwerpunkt/v/Vista.html**
[8] **https://www.computerwoche.de/knowledge_center/security/1881037/**

[9] **http://http//blogs.technet.com/swi/archive/2008/12/12/Clarification-on-the-various-workarounds-from-the-recent-IE-advisory.aspx**

[10] **https://www.computerwoche.de/schwerpunkt/m/Malware.html**

[11] **http://www.firefox.com/**

[12] **http://www.google.de/chrome**

[13] **http://http//blog.trendmicro.com/ie-zero-day-follow-up-now-featuring-mass-sql-injections/**

[14] **http://www.shadowserver.org/wiki/pmwiki.php?n=Calendar.20081210**
