

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 böartigen 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.msp>

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://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://blog.trendmicro.com/ie-zero-day-follow-up-now-featuring-mass-sql-injections/>
- ¹⁴ <http://www.shadowserver.org/wiki/pmwiki.php?n=Calendar.20081210>
-

IDG Tech Media GmbH

Alle Rechte vorbehalten. Jegliche Vervielfältigung oder Weiterverbreitung in jedem Medium in Teilen oder als Ganzes bedarf der schriftlichen Zustimmung der IDG Tech Media GmbH. dpa-Texte und Bilder sind urheberrechtlich geschützt und dürfen weder reproduziert noch wiederverwendet oder für gewerbliche Zwecke verwendet werden. Für den Fall, dass auf dieser Webseite unzutreffende Informationen veröffentlicht oder in Programmen oder Datenbanken Fehler enthalten sein sollten, kommt eine Haftung nur bei grober Fahrlässigkeit des Verlages oder seiner Mitarbeiter in Betracht. Die Redaktion übernimmt keine Haftung für unverlangt eingesandte Manuskripte, Fotos und Illustrationen. Für Inhalte externer Seiten, auf die von dieser Webseite aus gelinkt wird, übernimmt die IDG Tech Media GmbH keine Verantwortung.