GIF-Bug im Internet Explorer 6 - proof-of-concept

Warum ein proof-of-concept?

Vor einiger Zeit schon habe ich diesen, meiner Meinung nach problematischen Bug im Internet Explorer 6 von Microsoft, gefunden. Ich habe darauf, wie es sich gehört, mit Microsoft Kontakt aufzunehmen versucht, doch ich bekam entweder ein Standardmail zurück oder sonst eine weitere Adresse, an die ich mich wenden sollte. Doch nun ist es genug und ich werde den Bug hier präsentieren.

Um was geht es bei diesem Bug?

Es handelt sich um eine Fehlbehandlung von Bildern im GIF-Format. Es ist möglich, Code, der vom Internet Explorer interpretiert werden kann, direkt auszuführen, so z.B. Javascript.

Welche Systeme sind betroffen?

Leider habe ich nicht die Möglichkeiten, den Bug auf sehr vielen Systemen zu testen. Auf jeden Fall kann ich zumindest bestätigen, dass die Sicherheitslücke zu hundert Prozent bei Maschinen mit WindowsXP (Professional), ServicePack 2, Internet Explorer 6, sowie den neusten Patches von Microsoft vorhanden ist.

Was kann man mit dem Bug erreichen?

Grundsätzlich, kann man damit nicht mehr machen, als mit einer ganz normalen Datei, die in einer webkonformen Sprache geschrieben ist. Es gibt allerdings einen grossen Unterschied. Die Bilder, in die der Code eingebaut worden ist, behalten die Endung *.gif sowie ihren Header. Dies hat zur Folge, dass sehr viele teilweise renommierte Webapplikationen einen Upload der Dateien zulassen, zum Beispiel in eine Bildergalerie, als Avatar oder sonst etwas. Somit haben wir damit unser eigenes Script auf dem Webserver und können dieses auch nutzen. Als Beispiel könnte man hier verschiedene Cross-Site Scripting Attacken nennen aber auch etwas, für das dieser Bug wohl am besten geeignet ist: Cookies. Denn wenn wir zum Beispiel ein Script in das Bild einarbeiten, dass die Cookies eines Users in einem Forum ausliest, können wir uns unberechtigter Weise darauf Zugriff verschaffen.

Proof-of-concept

So nun will ich nicht weiter irgendwelchen Text schreiben, sondern werde in einem ganz simplen Beispiel, das Ausnützen der Sicherheitslücke erläutern.

Als erstes, benötigen wir einen Webserver (das ganze funktioniert nicht lokal ausser ein Apache läuft!!!), auf den wir unsere Datei(en) später uploaden können.

So nun zur Modifikation der Datei. Man nehme eine leere Datei und dann schreiben wir folgendes in diese hinein:

```
<GIF89aŸ  8  ÷™fÿ™™>

<html>
<head>

<script>
alert("Kleines Beispiel");
</script>

</head>
<body>
</body>
</html>
```

Nun speichern wir die Datei ab unter irgendeinname.gif. Wir sehen, es muss nichts weiter getan werden, als ein HTML-konforme Datei erstellt werden, welche den Header <GIF89aŸ 8 ÷™fÿ™™> enthält und den Namen *.gif trägt.

Jetzt kann die Datei auf den Anfangs erwähnten Webserver geladen werden und los geht's.

Kleine Info: Die Datei muss direkt angewählt werden, d.h. http://www.domain.com/bild.gif funktioniert aber nicht wenn das Bild irgendwo auf einer Website inmitten von anderem HTML-Code steht (→ Image-Tag).

So nun hoffe ich, dass nicht zu viel Unsinn damit getrieben wird.

Vielen Dank für das lesen dieses kleinen Papers.

Sollten Sie Fragen oder Anregungen haben, stehe ich Ihnen gerne zur Verfügung.

admin@disenchant.ch
http://www.disenchant.ch

Mit freundlichen Grüssen
Sven Vetsch